Gefahren aus dem Internet

Ein Leitprogramm für die Sekundarstufen I und II über das richtige Verhalten im Internet

Autor: Peter Skrotzky
Simulation: Christoph Bucher

Vorwort

Dieses Leitprogramm bietet einen Einblick in die Gefahren, denen eine Benutzerin im Internet begegnen kann. Der grösste Teil des Leitprogramms kann ab der Sekundarstufe I eingesetzt werden. Die vertiefenden Kapitel 7 und 8 verlangen weiter gehende Kenntnisse, insbesondere sollten die Studierenden über Grundkenntnisse in HTML und einer Programmiersprache verfügen.

Die einzelnen Kapitel des Leitprogramms sind grösstenteils unabhängig voneinander. Somit können auch nur Teile des Leitprogramms im Unterricht verwendet werden.

Im Text werden abwechselnd weibliche und männliche Nomen verwendet. Das andere Geschlecht ist jeweils mitgemeint.

Die Benützung des Leitprogramms, der Simulation und der dem Leitprogramm beiliegenden Dateien und Programme ist für Schulen kostenlos.

Ich möchte mich bei Prof. Carlos Rieder von der Hochschule Luzern für die Realisierung der Simulationssoftware bedanken. Einen besonderen Dank möchte ich an die Hasler Stiftung und das BKS des Kantons Aargau ausrichten, ohne deren finanzielle Unterstützung die Realisierung dieses Leitprogramms nicht möglich gewesen wäre. Ausserdem möchte ich mich bei Anton Lagger, Jacqueline Peter (WBZ CPS), Daniel Graf (ISB), Franz Zingg (ISB) und Thomas Müller (KS Sargans) für ihre Unterstützung und fachliche Beratung bedanken.

Inhaltsverzeichnis

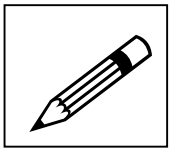
Einführung

Immer mehr Computer sind heutzutage permanent über schnelle Leitungen mit dem Internet verbunden. Wir nutzen das Internet tagtäglich zur Informationsbeschaffung, Kommunikation mit Freunden und Bekannten und vermehrt auch zur Selbstdarstellung. Dass es auch viele Personen gibt, die das Internet aus welchen Gründen auch immer missbrauchen, ist weitgehend bekannt.
Es liegt in der Natur der Sache, dass sich die Aktivitäten der Programme und Methoden, die von diesen Personen benutzt werden, meistens im Versteckten abspielen. Als Benutzer des Internets können wir uns einerseits mit technischen Hilfsmitteln wie Antivirenprogrammen, Firewalls etc. vor solchen Angriffen schützen, eine wichtige Rolle spielt aber auch, wie wir uns im Internet verhalten.
Ziel dieses Leitprogramms ist es, Schülerinnen und Schülern bewusst zu machen, welche Gefahren im Internet lauern und wo man als Benutzer besonders auf der Hut sein muss. Mit Hilfe einer Simulationsumgebung können die Schülerinnen und Schüler praktisch erleben, welche Auswirkungen unerwünschte Programme auf einem Computer haben können.
Nach Absolvierung dieses Leitprogramms sollten Schülerinnen und Schüler in der Lage sein, zu beurteilen, in welchen Situationen die Benützung des Internets (fast) gefahrlos ist und welche Aktionen potenziell gefährlich sein können.

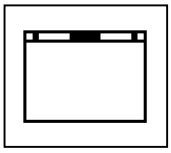
Wenn ein Computer gut geschützt ist und ein Benutzer sich im Internet richtig verhält, so ist die Gefahr einer Infektion verhältnismässig klein. Einen 100% Schutz gibt es aber leider nie.

Verwendete Symbole

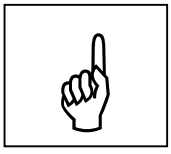
In diesem Leitprogramm werden für verschiedene Aktivitäten Symbole verwendet.



Beantworten Sie Fragen, die mit diesem Symbol gekennzeichnet sind, auf Papier.

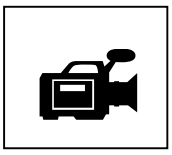


Dieses Symbol bedeutet, dass Sie für diesen Teil mit der Simulation arbeiten sollen.



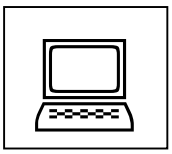
Neben diesem Symbol stehen wichtige Informationen, wie Sie Gefahren aus dem Weg gehen können.

Neben diesem Symbol stehen Aufgaben, die Sie nicht in der Schule sondern zuhause an Ihrem Computer lösen sollen.



Neben diesem Symbol steht jeweils ein Link auf einen Film zum Thema.

Neben diesem Symbol folgen Informationen oder Aufgaben, für die Sie das Internet benützen sollen.



Dieses Symbol bedeutet, dass Sie für die Aufgabe den Computer benützen sollen.

Die Simulationsumgebung

Sie gelangen zur Simulationsumgebung, indem Sie in einem Webbrowser den Link http://virtualab.ch/ eingeben. Dort finden Sie auch eine kurze Bedienungsanleitung.

Um mit der Umgebung zu arbeiten, müssen Sie Ihren Namen und Ihre Klasse eingeben.

Von Viren, Würmern und anderen Tieren

Unter dem Sammelbegriff *Malware* (von *Malicious Software*, *bösartiger Software*) versteht man Software, die ohne Wissen des Benutzers auf einen Computer gelangt und auf eine schädliche oder ärgerliche Art aktiv wird. Dazu gehören Viren, Würmer, Trojanische Pferde (kurz Trojaner), Spyware, Crimeware und andere Arten unerwünschter Software. Im Wesentlichen kann Malware auf drei verschiedene Arten Schaden anrichten. Es können Dateien auf dem infizierten Computer verändert oder gelöscht werden, ein Angreifer kann Zugang zum Computer erhalten und beliebige Aktivitäten manuell oder automatisch ausführen oder der infizierte Computer schickt Informationen an einen Angreifer, beispielsweise welche Webseiten ein Benutzer besucht, Passwörter, und so weiter.

Im letzten Jahrtausend wurden viele Viren und Würmer aus Experimentierfreude oder als (böse) Scherze geschrieben. Vorwiegend jungen Programmierern ging es oft vor allem darum, Sicherheitslücken zu finden oder eine möglichst grosse Verbreitung zu erreichen. Der Schaden, der von diesen Programmen ausging, war eher zweitrangig oder sogar unbeabsichtigt. Im 21. Jahrhundert wurde Malware immer gezielter dafür eingesetzt, Daten oder Webseiten zu beschädigen. Auch begannen kriminelle Organisationen damit, Malware einzusetzen, um an sensible Daten wie Passwörter für Bankkonten oder Online Shops zu gelangen oder einen infizierten Computer zur Speicherung von illegalen Inhalten zu benützen.
Als kriminelle Organisationen, die vor allem zu Geld kommen wollen, das Internet zu nutzen begannen, bildeten sich zwei weitere Gefahrenquellen, Spam und Phishing, heraus. Dabei geht es vor allem darum, dass Internetnutzer via E-Mail oder gefälschte Webseiten private Informationen wie Passwörter zu Online-Konten, Kreditkartennummern und ähnliches preisgeben oder zum Kauf von Produkten von zweifelhafter Herkunft überredet werden.

1 – Grundwissen

Voraussetzungen

- Sie haben das Internet bereits zuhause oder an der Schule genutzt.
- Sie wissen, was ein Provider ist.
- Sie wissen, was eine URL ist.

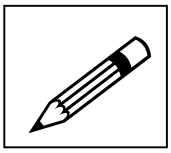
Lernziele

- Sie wissen, was es braucht, damit sich ein Computer mit dem Internet verbinden kann.
- Sie können die Bedeutung einiger grundlegender Begriffe grob erklären.

Einführung

Damit Sie auf einem Computer das Internet nutzen können, muss der Computer natürlich ans Internet angeschlossen sein. Vielleicht haben Sie Ihre Computer zuhause selbst ans Internet angeschlossen oder sich bereits Gedanken darüber gemacht, wie Ihre Computer zuhause oder an der Schule mit dem Internet verbunden sind.

In diesem Kapitel lernen Sie, welche Voraussetzungen nötig sind, damit Sie mit Ihrem Computer das Internet nutzen können. Dabei kommen einige Begriffe vor, die Sie vielleicht schon gehört haben oder sogar wissen, was sie bedeuten.



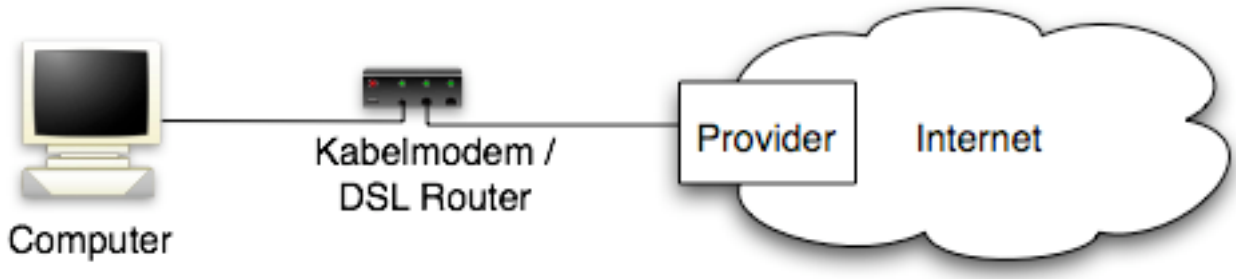
Lesen Sie die folgenden Begriffe. Unterscheiden Sie dabei zwischen Begriffen, die Ihnen fremd sind, die Sie schon gehört haben und solchen, von denen Sie wissen, was sie bedeuten. Notieren Sie die Bedeutung in zwei bis drei Sätzen.

- Kabelmodem
- DSL-Router
- WLAN
- TCP/IP
- IP-Adresse
- Domain Name
- DNS
- DHCP
- Port

Einen Computer ans Internet anschliessen

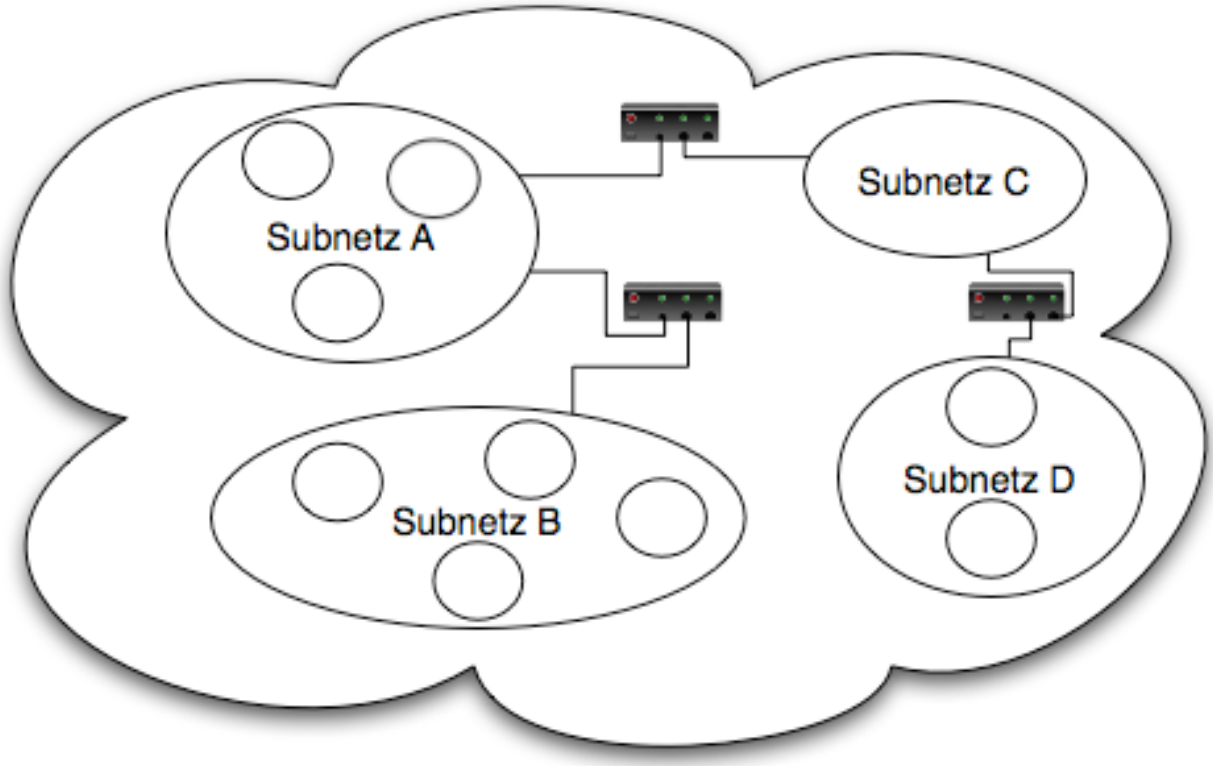
Ähnlich wie Sie zum Telefonieren ein Telefon benötigen, das die Verbindung zu einer Telefongesellschaft aufnehmen kann, brauchen Sie eine spezielle Hardware, um über einen Internet Service Provider ins Internet zu gelangen. In der heutigen Zeit ist diese Hardware in den meisten Fällen entweder ein Kabelmodem oder ein DSL-Router (DSL steht für *Digital Subscriber Line*). Möchten Sie an ein Kabelmodem mehrere Computer

anschliessen, benötigen Sie einen separaten Router. An einen DSL Router können Computer entweder über Kabel (*Ethernet-Router*) oder Funk (*WLAN-Router*) angeschlossen werden.



Logischer Aufbau des Internets

Wie der Name schon ausdrückt, ist das Internet ein Zusammenschluss von verschiedenen Netzwerken (Subnetzen). Jedes dieser Subnetze kann wiederum mehrere Subnetze enthalten und so weiter. Subnetze sind untereinander über Router verbunden. Auch das Netzwerk an Ihrer Schule ist ein solches Subnetz. Ebenso bilden Ihre Computer zuhause ein kleines Subnetz.



Wenn sich Ihr Computer mit dem Internet verbindet, wird er in ein Subnetz Ihres Providers eingebunden und somit selbst ein Teil des Internets.

Da sich im Internet Millionen von Computern und anderen Geräten von verschiedenen Herstellern befinden, ist es wichtig, dass nicht nur die technischen Spezifikationen der Geräte klar geregelt sind, sondern auch die Kommunikation zwischen den Geräten muss nach streng geregelten Abläufen geschehen. Diese Abläufe werden häufig *Protokolle*

genannt. Wenn Ihr Computer im Internet kommuniziert, so hält er sich an die Protokolle der TCP/IP Protokoll Suite (*Transmission Control Protocol / Internet Protocol*).

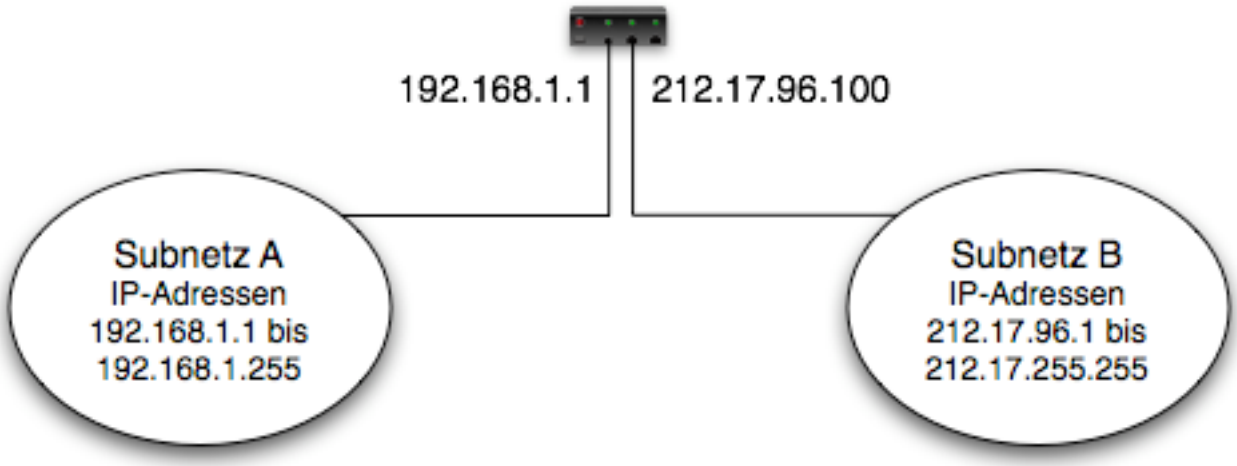
IP-Adressen

IP-Adressen haben eine gewisse Ähnlichkeit mit Telefonnummern. Sie dienen dazu, Geräte im Internet eindeutig zu identifizieren. Sie dürfen deshalb, von wenigen Ausnahmen abgesehen, nur einmal vergeben werden. Eine IP-Adresse besteht aus vier jeweils durch einen Punkt getrennte Zahlen zwischen 0 und 255, beispielsweise 192.168.1.86.

Wie können Sie nun herausfinden, welche IP-Adresse Sie benützen dürfen?

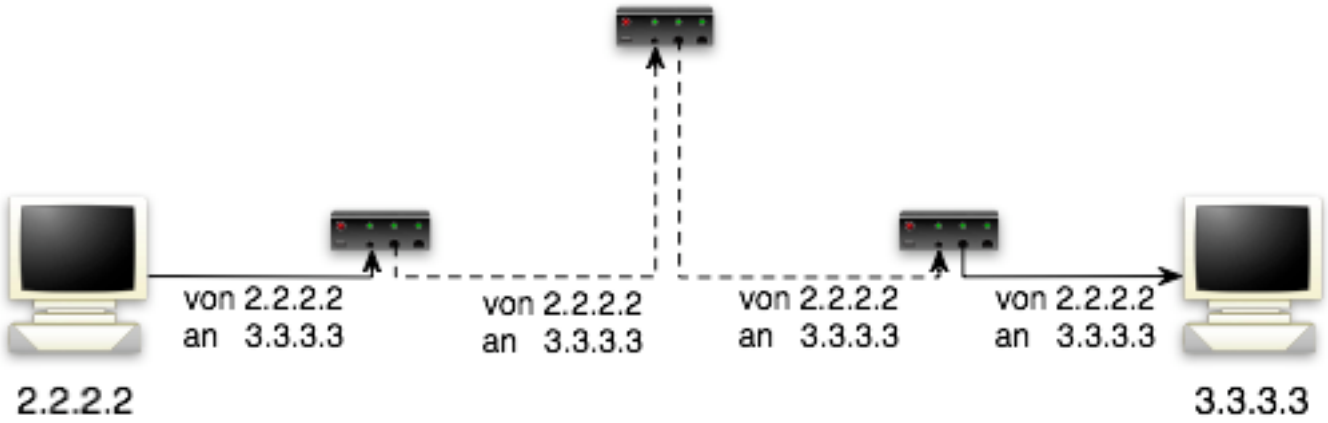
Die Antwort auf diese Frage ist einfach: Sie müssen sich nicht darum kümmern. Ihr Provider verfügt über einen Vorrat von IP-Adressen, von denen er Ihnen eine zuweist. Wenn Ihr Computer direkt an einem Kabelmodem angeschlossen ist, so bekommt Ihr Computer diese IP-Adresse. Wenn der Computer über einen (DSL-)Router mit dem Provider verbunden ist, bekommt der Router die IP-Adresse. Ihr Computer befindet sich dann in einem lokalen Netzwerk.

Wie bereits erwähnt, dient ein Router dazu, zwei Subnetze miteinander zu verbinden. Aus diesem Grund hat ein Router immer zwei IP-Adressen.



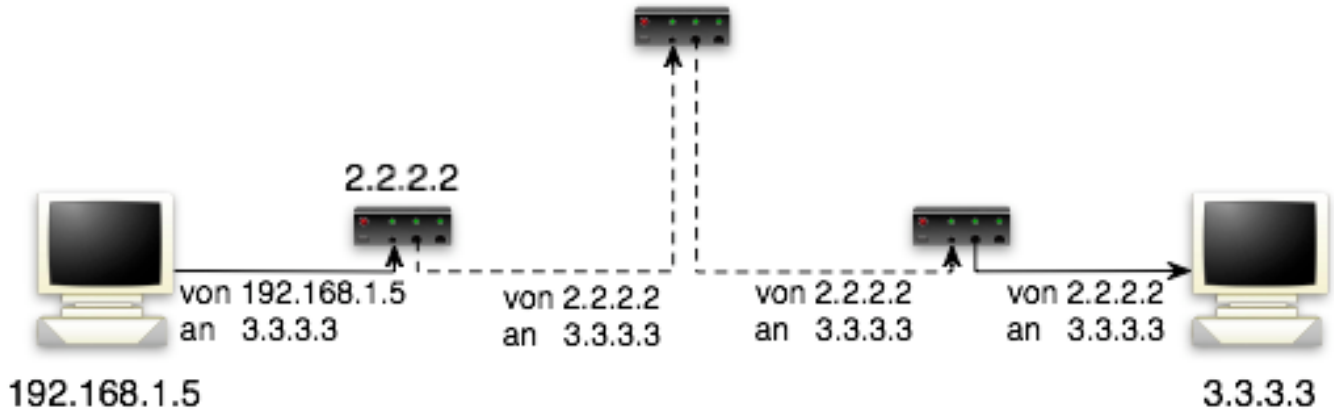
Lokale IP-Adressen

Wenn Ihr Computer mit einem anderen kommuniziert, müssen beide wissen, welche IP-Adresse der andere hat. Diese Informationen müssen also von den Routern dazwischen weitergegeben werden.



Es gibt nun drei Bereiche von IP-Adressen, die für lokale Netzwerke vorgesehen sind. Diese IP-Adressen werden von einem Router nicht weitergegeben. Stattdessen verwendet der Router seine eigene IP-Adresse. Diese Bereiche sind

- Alle IP-Adressen, deren erste Zahl 10 ist, also alle IP-Adressen zwischen 10.0.0.0 und 10.255.255.255. Dieser Bereich ist für sehr grosse lokale Netzwerke gedacht.
- Alle IP-Adressen, deren erste Zahl 172 und deren zweite Zahl mindestens 16 und höchstens 31 ist, also alle IP-Adressen zwischen 172.16.0.0 und 172.31.255.255.
- Alle IP-Adressen, die mit 192.168 beginnen, also von 192.168.0.0 bis 192.168.255.255. Diese IP-Adressen werden am häufigsten bei privaten lokalen Netzwerken verwendet.

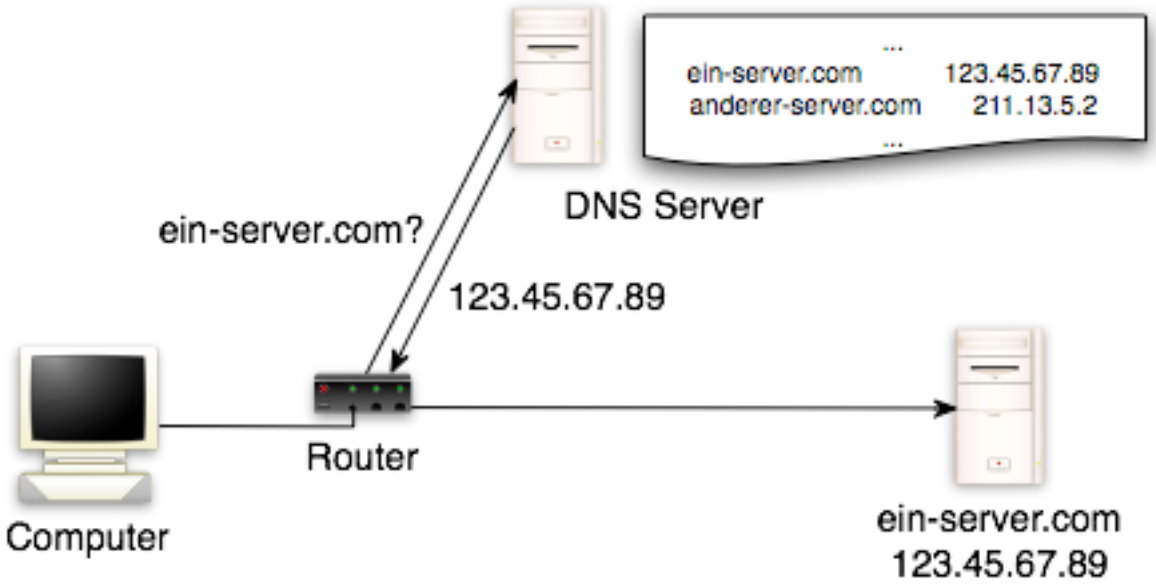


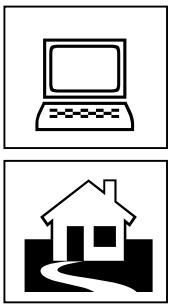
Es ist die Aufgabe des Routers, zu wissen, welcher Computer im lokalen Netz an der Kommunikation beteiligt ist.

Domain Namen

Wenn Sie das Internet benutzen, so geben Sie in der Regel keine IP-Adressen ein, sondern einen Domain Namen, beispielsweise *www.meine-schule.ch*. Computer und andere Netzwerkgeräte arbeiten jedoch mit den IP-Adressen. Deshalb gibt es spezielle Server, so genannte DNS-Server (*Domain Name System*-Server), auf denen Tabellen verwaltet werden, die einem oder mehreren Domain Namen eine entsprechende IP-Adresse zuordnen. Wenn sich also Ihr Computer mit dem Server *ein-server.com* verbinden möchte,

so schaut er zuerst auf einem DNS-Server nach, wie die entsprechende IP-Adresse lautet und ruft anschliessend diese Adresse auf.





Finden Sie heraus, wie der Computer, an dem Sie gerade sitzen und Ihr Computer zuhause mit dem Internet verbunden sind. Das heisst, finden Sie die IP-Adressen des Computers, des Routers und, falls möglich, der Name Server. Achtung: Vielleicht haben Sie auf den Computern Ihrer Schule nicht die nötigen Zugriffsrechte, um zu diesen Informationen zu gelangen.

DHCP

Wie wir in den vorherigen Abschnitten gesehen haben, muss Ihr Computer zur Benützung des Internets

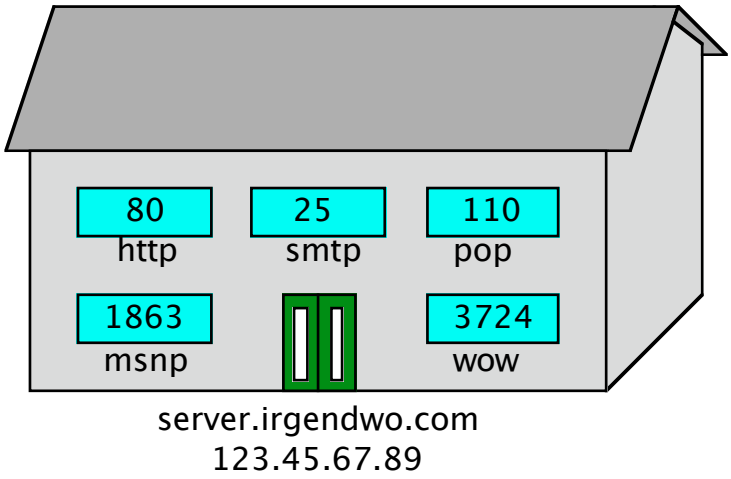
- eine (eindeutige) IP-Adresse haben
- die IP-Adresse des Routers kennen
- die IP-Adresse von mindestens einem DNS-Server kennen

Normalerweise werden diese Daten automatisch von Ihrem Router oder von Ihrem Provider geliefert. Dazu wird in der Regel das DHCP (*Dynamic Host Configuration Protocol*) verwendet.

Ports

Wenn Ihr Computer mit dem Internet verbunden ist, so möchten Sie das Internet natürlich auch nutzen. Genauer gesagt, Sie möchten einzelne Dienste davon nutzen, beispielsweise E-Mail, WWW, Chats, Online-Spiele etc. Hinter all diesen Diensten stehen Programme,

die auf Computern laufen. Sobald ein Computer einen Dienst anbietet, wird er als Server bezeichnet. Obwohl in der Regel spezielle Computer für Serverdienste verwendet werden, könnte grundsätzlich jeder Computer zum Server werden. Damit sich die einzelnen Dienste, die ein Server anbietet, nicht in die Quere kommen, benützt jeder Dienst einen oder mehrere so genannte *Ports*. Ist nun auf einem Server ein Dienst installiert und aktiviert, so horcht dieser seinen Port ab, ob eine Anfrage vorliegt. Ist das der Fall, so reagiert er auf die Anfrage.
Sie können sich einen Server ungefähr wie ein Geschäftshaus vorstellen, in dem es verschiedene Bürozimmer (= Ports) gibt. Je nach dem, welches Anliegen ein Kunde hat, muss dieser sich an das entsprechende Büro wenden.



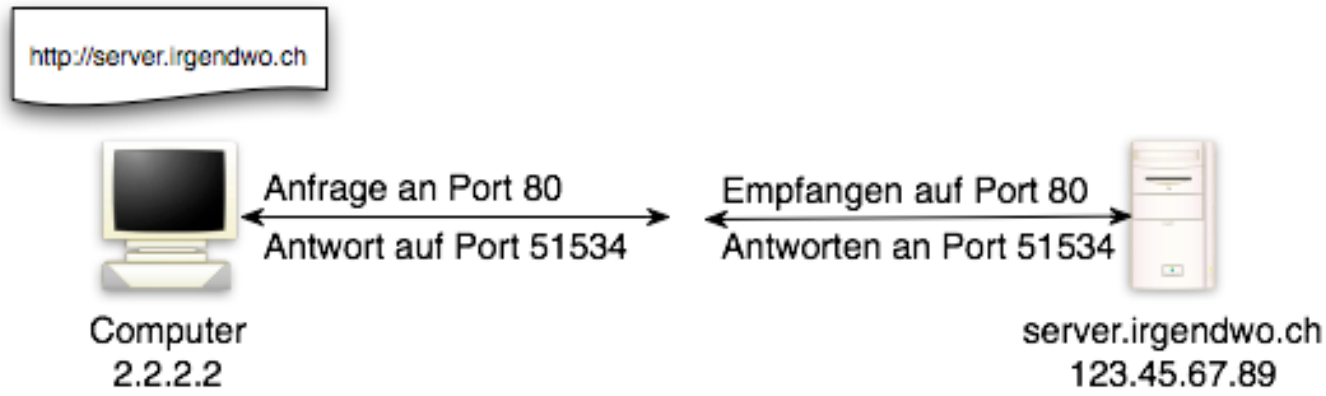
Sie haben sicher schon bemerkt, dass beim Surfen mit einem Internet Browser vor der URL in der Regel *http://* steht, beispielsweise *http://google.ch*. HTTP (*HyperText Transfer Protocol*) ist das Protokoll, das zur Übermittlung von Webseiten verwendet wird. In der oben abgebildeten Skizze sehen Sie, dass für dieses Protokoll der Port 80 verwendet wird.
Die übrigen abgebildeten Ports werden für folgende Dienste gebraucht:

- Port 25 SMTP *Simple Mail Transfer Protocol* Verschicken von E-Mails
- Port 110 POP *Post Office Protocol* Empfangen von E-Mails
- Port 1863 MSNP *MSN Protocol* MSN
- Port 3724 WOW *World Of Warcraft* Online-Spiel

Port Nummern gehen von 0 bis 65535.

Möchte der Kunde eine Webseite vom Server abrufen, so muss er dazu ins Bürozimmer 80 (also, die Anfrage über Port 80 senden). Möchte er dagegen eine E-Mail verschicken, so muss er sich an das Büro 25 wenden (also den Port 25 benutzen). Die meisten Programme, die auf einen Dienst eines Servers zugreifen, sind so eingestellt, dass sie den jeweiligen Standardport eines Dienstes automatisch benutzen. Somit ist es selten nötig, dass Sie sich mit Porteinstellungen beschäftigen müssen.

Wenn nun Ihr Computer eine Webseite auf dem Server *server.irgendwo.ch* aufrufen möchte, so richtet er an den Server eine entsprechende Anfrage auf dem Port 80. Um die Antwort des Servers zu empfangen, muss Ihr Computer ebenfalls einen Port öffnen. Da Ihr Computer nicht selbst ein Webserver ist, sondern nur ein Kunde eines Webservers, kann er für die Antwort nicht den Port 80 verwenden. Er wählt stattdessen zufällig einen unregistrierten Port. Das sind diejenigen mit den Nummern grösser als 49151.



Kontrollfragen

1) Was ist der wesentliche Unterschied zwischen IP-Adressen von lokalen Netzen, beispielsweise 192.168.1.5, und einer globalen IP-Adresse, beispielsweise 212.117.92.35?

2) Was ist die Aufgabe eines DNS Servers?

3) Was benötigen Sie, damit Sie sich mit Ihrem Computer von zuhause aus mit dem Internet verbinden können?

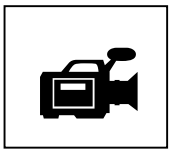
4) Können Sie auf einen Server, beispielsweise einen Webserver, auch zugreifen, ohne dass Sie dessen Domain Namen kennen?

2 – Malware

Lernziele

- Sie kennen die Bedeutung einiger wichtiger Begriffe im Zusammenhang mit Malware
- Sie kennen einige typische Arten von Malware und wissen grob, welchen Schaden sie anrichten können

Es gibt heute über zwei Millionen bekannte Schädlinge, die Windows-PCs befallen können und es werden täglich mehr. Bei dieser Anzahl erstaunt es nicht, dass die Wege, wie ein bösartiges Programm auf unseren Computer gelangen kann, die Möglichkeiten, wo es sich auf unserem Computer einnistet und welche Wirkungen es entfaltet, äusserst vielfältig sind. Natürlich ist nicht jedes dieser Programme vollständig neu und so versucht man, die Schädlinge in Kategorien einzuteilen. Im Folgenden werden Sie einige dieser Kategorien und typische Auswirkungen kennen lernen.



Das deutsche Bundesamt für Sicherheit in der Informationstechnik stellt einen sechsminütigen Lehrfilm über verschiedene Arten von Malware unter folgender Adresse zur Verfügung:
https://www.bsi-fuer-buerger.de/cln_174/BSIFB/DE/ITSicherheit/AbzockerUndSpione/BotNetze/botnetze_node.html

Arten von Malware

Viele bösartige Programme, die heute unsere Computer bedrohen, können nicht mehr unbedingt einer bestimmten Kategorie zugeordnet werden, sondern enthalten mehrere Komponenten. So ist es möglich, dass ein Adware Programm zusätzlich den Benutzer ausspioniert und somit auch ein Spyware Programm ist, oder dass ein Computerwurm auch einen Trojaner installiert und so weiter.

Trojaner

Trojaner sind mit über einer Million Varianten die mit Abstand am häufigsten auftretende Malware. Der Begriff stammt aus der griechischen Mythologie, als die Griechen die Stadt Troja belagerten. Nach über 10 Jahren ohne Erfolg bauten sie ein hölzernes Pferd, in dem sich einige Krieger versteckten. Die übrigen zogen sich auf ihre Schiffe zurück und taten so, als würden sie die Belagerung aufgeben und absegeln. Die Trojaner betrachteten das Pferd als Kriegsbeute und zogen es in die Stadt. In der Nacht schlichen sich die versteckten Krieger aus dem Pferd, öffneten die Tore Trojas und ermöglichten so den inzwischen zurückgekehrten Griechen, in die Stadt einzudringen und die Trojaner zu besiegen.
Ein Trojaner bezeichnet deshalb ein bösartiges Programm, das sich als nützliches oder sogar notwendiges Programm tarnt, beispielsweise zum Abspielen eines Videos, aber in Realität eine “Hintertür” zum Internet auf unserem Computer öffnet, die einem Angreifer Zugriff auf ihn ermöglicht.

Würmer

Würmer sind Programme, die sich selbständig über das Internet verbreiten. Typischerweise nutzen sie dazu Schwachstellen von Betriebssystemen oder Programmen aus. Viele Würmer wurden so programmiert, dass sie sich nur verbreiten und der einzige Schaden darin besteht, dass sie das Internet "langsamer machen". Es gibt aber auch Würmer, die beispielsweise ähnlich wie ein Trojaner auf einem infizierten Computer eine Hintertür öffnen oder E-Mails von unserem Computer verschicken und so weiter.

Viren

Oftmals verwendet man im Alltag den Begriff Computervirus synonym für jede Art bösartiger Programme. Ein Computervirus im eigentlichen Sinn ist ein Programm, das sich selbst reproduzieren kann und sich oftmals im Programmcode eines seriösen Programms (einem "Wirtprogramm") einnistet und auch so übertragen wird. Der Schaden, den ein Virus anrichtet, reicht von harmlosen, eher lästigen Meldungen auf dem Bildschirm bis zum Löschen von wichtigen Dateien oder Systemabstürzen.

Rootkits

Rootkits bestehen aus einem oder mehreren Programmen, die sich sehr tief im Betriebssystem einnisten, beispielsweise als Gerätetreiber. Dadurch können sie wichtige Teile des Betriebssystems verändern oder in die Abläufe eingreifen, vielfach mit dem Ziel, ihre Präsenz zu verbergen. So kann ein installierter Rootkit beispielsweise das Betriebssystem so manipulieren, dass er von einem Antivirenprogramm nicht gefunden wird, oder dass er unbemerkt aufs Internet zugreifen kann.

Spyware

Unter diesem Begriff werden Programme zusammengefasst, die ohne sein Wissen Informationen über einen Benutzer sammeln. Beispielsweise so genannte Keylogger, Programme, die aufzeichnen, welche Tasten ein Benutzer gedrückt hat. Auch könnte ein Spyware Programm aufzeichnen, welche Webseiten eine Benutzerin besucht und sie sogar auf ungewünschte Webseiten umlenken.

Adware

Adware bezeichnet Programme, die eine Benutzerin mit unerwünschter Werbung eindecken. Obwohl Adware an und für sich keinen Schaden anrichtet, ist sie für einen Benutzer lästig, weil plötzlich erscheinende Fenster und ähnliches die Arbeit am Computer erschweren.

Spam

Bei diesem Begriff handelt es sich nicht um Malware, vielmehr bezeichnet man damit E-Mails, die mehr oder weniger wahllos an viele Empfänger geschickt werden. Der Inhalt der E-Mails kann von Werbung für diverse Produkte, meist von zwielichtigen Anbietern,

bis zur Verbreitung von Malware reichen. Gemäss Statistiken von Organisationen, die den Mailverkehr beobachten, macht Spam ca. 90% des gesamten E-Mail Verkehrs aus.
Der Name *Spam* ist übrigens keine Abkürzung, sondern stammt aus einem Sketch der englischen Komikertruppe *Monty Python* aus dem Jahre 1970 und bezeichnet eine Art Dosenfleisch.

Auswirkungen

Wie bereits oben erwähnt, kann Malware auf unserem Computer dazu führen, dass wir in unserer Arbeit am Computer behindert werden, dass Dateien verändert oder gelöscht werden oder dass unsere Internetverbindung plötzlich sehr langsam wird. Ebenfalls erwähnt wurde, dass private Informationen von unserem Computer gesammelt und an einen Angreifer übermittelt werden können. Während diese Gefahren direkt die Benutzerin des Computers betreffen, können andere weiter reichende Auswirkungen haben. Sobald es einem Angreifer gelingt, ein bösartiges Programm auf unserem Computer zu platzieren, das eine Hintertür zum Internet öffnet, hat der Angreifer eine gewisse, wenn nicht gar die volle Kontrolle über unseren Computer. Eine mögliche Folge davon ist, dass er unseren Computer in ein von ihm kontrolliertes *Botnet* einbindet. Es können aber auch schwerwiegendere Folgen auftreten, beispielsweise, wenn ein Angreifer unseren Computer als Webserver für illegale Inhalte missbraucht.

Botnets

Wenn Ihr Computer einem Angreifer eine Hintertür öffnet, so kann er diese dazu nutzen, um einen so genannten *Bot* (Kurzversion für *Software Robot*) auf Ihrem Computer zu installieren. Dabei handelt es sich um kleine Programme, die eigenständig und automatisch im Hintergrund laufen und über die der Angreifer Ihren Computer nach belieben steuern kann. Ihr Computer wird so zu einem *Zombie Computer*. Das Ziel des Angreifers ist dabei in der Regel, so viele Computer wie möglich unter seine Kontrolle zu bringen. Der Angreifer, *Bot Master*, kann nun sein Botnet gezielt einsetzen. Er kann beispielsweise allen Bots befehlen, Spam E-Mails zu verschicken oder gleichzeitig alle Bots auf denselben Webserver zugreifen zu lassen und diesen so blockieren (*Denial of Service* Angriff).
Botnets können einige Tausend bis mehrere Millionen Computer umfassen. Beispielsweise wurde Anfang 2010 in Spanien eine Hackergruppe verhaftet, die ein Botnet von 13 Millionen Computern primär für Angriffe auf grosse Unternehmen benutzt haben.

Kontrollfragen

1) Daniel meint, dass es ihm egal sei, wenn er Malware auf seinem Computer hat. Er habe nichts darauf gespeichert, was für einen Angreifer interessant sein könnte. Deshalb gebe er sein Geld lieber für andere Dinge als Virenschutz und ähnliches aus.

   Welche Argumente könnten Sie anführen, um Daniel zu überzeugen, dass auch er seinen Computer schützen sollte?

2) Warum ist es heute oft schwierig, ein Malware Programm einer bestimmten Kategorie zuzuordnen?

3) Welche Anzeichen könnten darauf hindeuten, dass Ihr Computer von einer Malware infiziert wurde?

3 – E-Mail

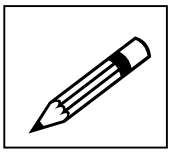
Voraussetzungen

- Sie haben eine eigene E-Mail Adresse und benützen diese regelmässig.
- Sie kennen den Unterschied zwischen einem Mail Client und einem Webmailer.

Lernziele

- Sie können einschätzen, ob eine bestimmte E-Mail potenziell gefährlich ist oder nicht.
- Sie kennen Kriterien, um die Seriosität/Echtheit einer E-Mail einzustufen.
- Sie erkennen, welche Auswirkungen ein schädliches Programm auf ihren Computer haben kann.
- Sie wissen, welchen Schutz ein Virenscanner erbringt.

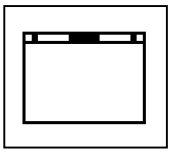
Praxis



Haben Sie schon E-Mails erhalten, die Sie ungeöffnet gelöscht haben? Falls Ja: Begründen Sie, warum Sie sich entschieden haben, die E-Mails zu löschen. Falls Nein: Haben Sie schon E-Mails geöffnet, deren Absender oder Inhalt Ihnen im nachhinein komisch vorkam?

Wissen Sie, ob die E-Mails, die Sie erhalten, auf Viren geprüft werden? Geschieht diese Prüfung durch Ihren Provider oder durch Ihr Virenprogramm?

Verfügt Ihr Mailprogramm über einen Spam Filter? Haben Sie diesen selbst eingerichtet?



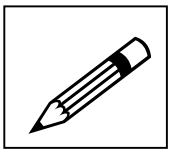
Wechseln Sie nun an den Computer.
Starten Sie die Simulation und melden Sie sich an. Wenn Sie angemeldet sind, starten Sie den Mail-Client, indem Sie auf das Icon Doppelklicken und klicken Sie anschliessend auf *Empfangen*. Sie erhalten einige E-Mails.

Bevor Sie die E-Mails öffnen, versuchen Sie die E-Mails in die drei Kategorien *wahrscheinlich ungefährlich*, *eventuell gefährlich/Spam* und *wahrscheinlich gefährlich/Spam* zu unterteilen.

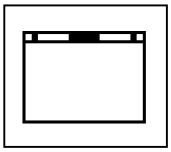
Öffnen Sie nun alle E-Mails und klicken Sie auch auf die Links bzw. die Anhänge. Beobachten Sie, was geschieht.

Welche E-Mails haben sich als gefährlich herausgestellt? Stimmen die Resultate mit Ihren Vermutungen von vorhin überein? Notieren Sie einige Merkmale durch die Sie gefährliche von ungefährlichen E-Mails unterscheiden können.

Sie haben nun einige Möglichkeiten gesehen, was passieren kann, wenn Sie jede eingehende Mail und jeden Anhang auf einem ungeschützten Computer öffnen. Mit einem aktuellen Virenscanner können Sie Ihren Computer schützen.



Welche der gefährlichen Mails, die Sie erhalten haben, entdeckt ein Virenscanner Ihrer Meinung nach?



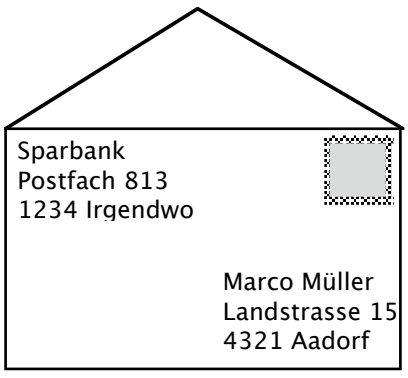
Starten Sie die Simulation und melden Sie sich an. Wenn Sie angemeldet sind, starten Sie das Virenschutzprogramm und anschliessend den Mail-Client und klicken Sie wiederum auf *Empfangen*.

Versuchen Sie wiederum, alle empfangenen E-Mails zu lesen und auch wieder auf die Links und Anhänge zu klicken.

Welche gefährlichen E-Mails erkennt der Virenschutz? Können Sie begründen, warum der Virenschutz gewisse gefährliche Inhalte nicht erkennt?

Hintergrundwissen

Wenn wir einen Brief erhalten, so interessiert uns in der Regel der Inhalt des Briefes und nicht der Umschlag. Dieser hat eigentlich nur den Zweck, dass der Brief bei uns ankommt (und dass er nicht von anderen Personen gelesen werden kann).
Insbesondere in "offiziellen" Briefen stehen der Absender und der Adressat nicht nur auf dem Umschlag sondern auch noch auf dem Brief selbst. Dabei kann es durchaus vorkommen, dass auf dem Umschlag ein *anderer* Absender als im Brief steht.



Sparbank
Patrizia Muster
Dorfweg 12
1111 Bestadt

Marco Müller
Landstrasse 15
4321 Aadorf

Sehr geehrter Herr Müller

...
...
...

Freundliche Grüsse
P. Muster

Ganz ähnlich ist die Situation bei einer E-Mail. Der "Umschlag", der eine E-Mail vom Absender zu den Adressaten verschickt, ist das SMTP Protokoll. Im Gegensatz zu einem

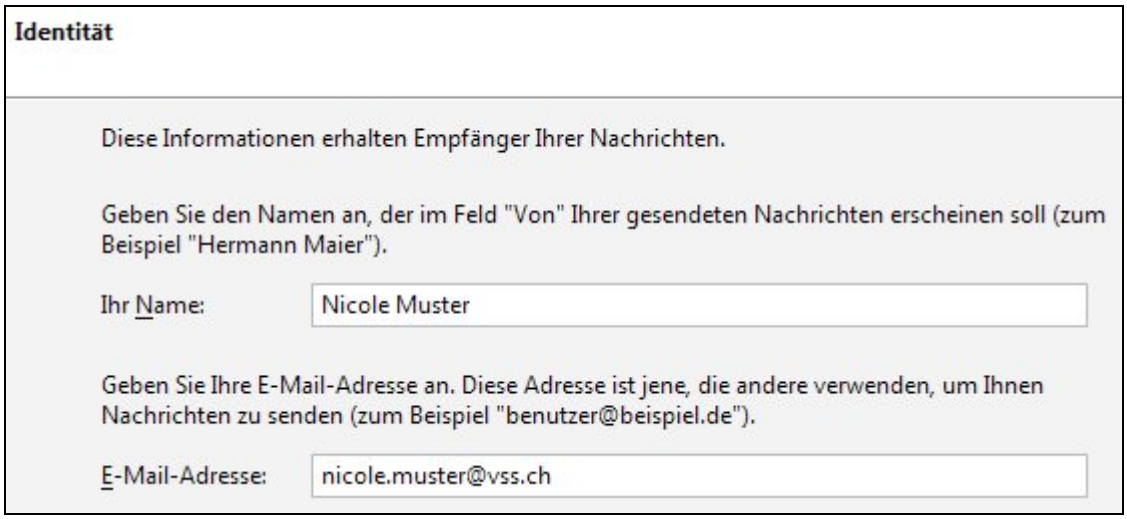
Brief wird der Umschlag jedoch “weggeworfen”, sobald die E-Mail im Postfach des Adressaten eingetroffen ist. Wenn wir E-Mails empfangen, erhalten wir also sozusagen den Brief ohne Umschlag.

Eine E-Mail besteht im Wesentlichen aus drei Teilen. Ein erster Teil, in dem verschiedene Informationen zur E-Mail stehen, beispielsweise der Absender, der oder die Adressaten, die Betreffzeile, Datum und Uhrzeit, von welchem Server die E-Mail geschickt wurde und so weiter. Der zweite Teil enthält den Text der E-Mail und der dritte Teil die Anhänge. Jeder dieser drei Teile kann falsche oder gefährliche Inhalte haben.

Informationsteil

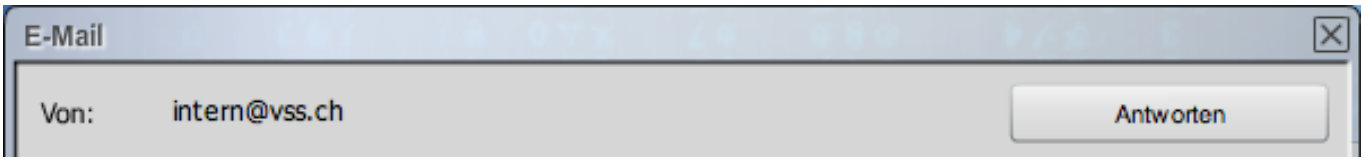
Dieser Teil enthält verschiedene Informationen über die E-Mail. Die meisten dieser Informationen werden von einem Mail Client normalerweise nicht angezeigt, weil sie für einen durchschnittlichen Benutzer wenig aussagekräftig sind. Für diejenigen, die sie trotzdem sehen wollen, bieten Mail Clients eine entsprechende Anzeigemöglichkeit, die je nach Mail Client *Rohdaten*, *Kopfzeilen* oder ähnlich heisst.
Die für uns wichtigsten Informationen dieses Teils bereitet ein Mail Client für uns auf. Es sind der Absender, die Betreffzeile sowie die Adressaten der E-Mail.
Der Absender einer E-Mail gibt uns eine erste Auskunft darüber, wie vorsichtig wir mit dem Inhalt der E-Mail umgehen sollten.

Der Absender enthält die E-Mail Adresse des Absenders und meistens auch noch dessen Namen. Wenn Sie einen Mail Client einrichten, so werden Sie unter anderem aufgefordert, eine E-Mail-Antwortadresse und einen Namen einzugeben.

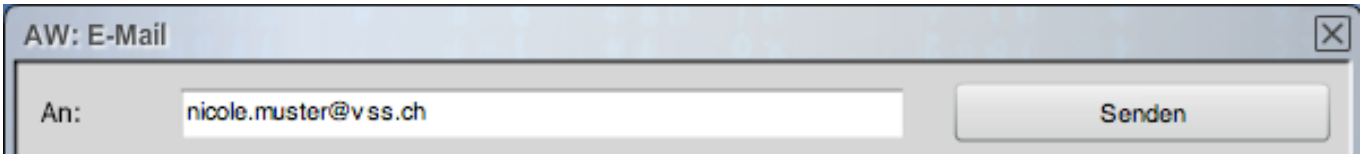


Diese Angaben werden bei jeder E-Mail, die Sie verschicken, in den Informationsteil der E-Mail geschrieben. Obwohl es in der Regel sinnvoll ist, korrekte Angaben zu machen, ist es vom technischen Standpunkt her nicht zwingend.
Es können auch tatsächlich Situationen auftreten, in denen es zweckmässiger ist, beispielsweise eine andere E-Mail Adresse anzugeben. Ein Beispiel dazu:

Nicoles Schule bietet die Möglichkeit, über eine interne Webseite E-Mails an mehrere oder alle Schülerinnen und Schüler zu verschicken. Nicole möchte dieses Angebot nutzen und ruft die entsprechende Webseite auf. Nachdem Sie die Nachricht geschrieben hat, schickt sie sie ab. Weil Nicole die Nachricht nicht von ihrem E-Mail Konto aus verschickt hat, ist der Absender eine allgemeine E-Mail Adresse, in diesem Beispiel *intern@vss*, Antworten sollen aber an das E-Mail Konto von Nicole gelangen. Beim Empfänger sieht die Nachricht so aus:

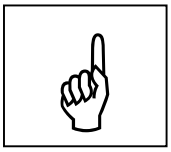


Antwortet ein Empfänger auf diese Mail, so ist Nicole die Adressatin.



Spammer nutzen diese Möglichkeiten gezielt, einerseits, weil sie damit den Eindruck erwecken können, die E-Mail stamme von einem seriösen Absender und andererseits, um die Herkunft der E-Mails zu verbergen.

Somit sollten Sie folgendermassen vorgehen:



Achten Sie auf den Absender von E-Mails. Wenn Ihnen der Name unbekannt ist, so heisst das noch nicht unbedingt, dass die E-Mail gefährlich ist. Sie sollten dann aber die Betreffzeile genau betrachten. Wenn deren Inhalt nichts mit Ihnen zu tun hat, so stammt die E-Mail mit grosser Wahrscheinlichkeit nicht von einem seriösen Absender.

Können Sie nun daraus folgern, dass E-Mails, deren Absender Ihnen bekannt ist, grundsätzlich harmlos sind?

Leider ist die Antwort Nein.

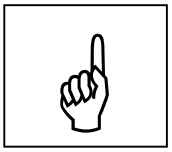
Bei allgemein bekannten Absendern wie beispielsweise *Facebook*, *MySpace* oder *msn* ist diese Antwort eigentlich noch leicht einzusehen. Verwirrender ist es, wenn es sich um E-Mails aus Ihrem Bekanntenkreis handelt. Auch hier lohnt es sich, die Betreffzeile genauer anzuschauen. Wenn Ihnen Ihr Mathematiklehrer eine E-Mail mit dem Betreff "*Hey, schau mal was ich Cooles gefunden habe*" schickt, oder Ihre beste Freundin Ihnen Software zu Billigstpreisen verkaufen will, sollten Sie stutzig werden.
Aber wie kann das passieren? Wollen Ihnen Ihre Lehrer und Freunde plötzlich Viren unterjubeln? Woher kennt ein Übeltäter die Namen und E-Mail-Adressen Ihres Bekanntenkreises?
Eine mögliche Ursache kann der sorglose Umgang mit den Adressaten von E-Mails sein.

Wenn Sie eine E-Mail verfassen, so wissen Sie, dass es drei verschiedene Arten von Empfängern gibt. Diejenigen, an die sich die E-Mail direkt richtet (*An:*), diejenigen, die eine Kopie zur Kenntnis bekommen (*CC:*) und diejenigen, die eine versteckte Kopie bekommen (*BCC:*). Übrigens: *CC* steht für *Carbon Copy* und *BCC* für *Blind Carbon Copy*.

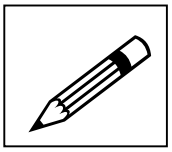
Während die ersten beiden Arten nur den Empfänger informieren, ob die E-Mail an ihn gerichtet ist, oder ob er sie einfach zur Kenntnisnahme erhält, so gibt es einen wesentlichen Unterschied zur dritten Art, *BCC*. Alle E-Mails, die an Empfänger, die unter *An:* oder *CC:* aufgelistet sind, enthalten alle Adressen dieser Empfänger. E-Mails, die an *BCC*-Empfänger gehen, enthalten nur die Adressen, die unter *An:* aufgelistet sind.

Stellen Sie sich vor, dass eine E-Mail an alle Schülerinnen und Schüler Ihrer Schule verschickt wird und alle Empfänger in der *An:*-Zeile aufgeführt sind. Für die Empfänger hat eine solche E-Mail drei unschöne Konsequenzen:

- Jeder Empfänger kennt nun die E-Mail Adresse der übrigen Empfänger. Dies kann aus der Sicht des Datenschutzes unter Umständen problematisch sein.
- Empfänger, die mit einem Webmailer arbeiten, müssen sich zuerst durch alle Empfänger scrollen, um zur eigentlichen Nachricht zu gelangen.
- Einige Würmer oder Trojaner durchsuchen auf einem infizierten Computer dessen Mailboxen nach E-Mail Adressen und senden diese an die Übeltäter. Wenn nun der Computer eines einzigen Empfängers infiziert ist, kennt der Übeltäter nun alle E-Mail Adressen der Empfänger und kann erst noch den Schluss daraus ziehen, dass sich diese untereinander vermutlich kennen.



Wenn Sie E-Mails an eine grössere Anzahl Empfänger versenden, listen Sie alle Empfänger unter *BCC:* auf. Weil Sie zum Versenden der E-Mail aber mindestens einen Empfänger unter *An:* angeben müssen, ist eine empfehlenswerte Praxis, dort die eigene E-Mail Adresse anzugeben. Vielleicht steht Ihnen aber auch ein Multi-Mailing-System zur Verfügung. Solche Systeme sind normalerweise so konfiguriert, dass sie dieses Problem automatisch lösen.



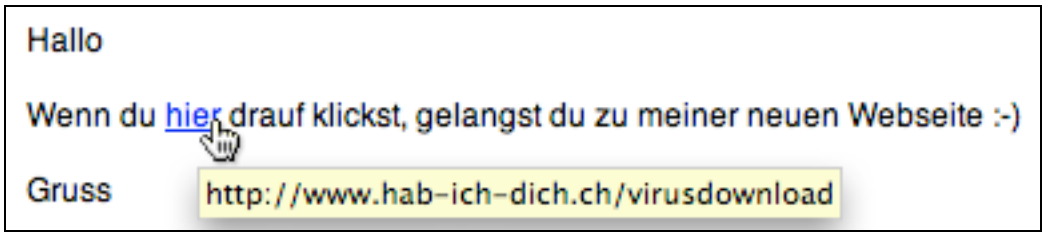
Welche der folgenden E-Mails erscheinen Ihnen seriös (können Sie wahrscheinlich ohne Bedenken öffnen), bei welchen sind Sie unsicher, ob sie Spam enthalten oder gefährlich sein könnten und welche E-Mails würden Sie ungelesen löschen, weil sie sicher unseriös sind?

@	Absender	Betreff	Datum
@	Englischlehrer	Aufgaben für nächsten Dienstag	
	Mahnung	Offene Rechnung	
	Lotterie Schweiz	Sie haben gewonnen!	
	Walter	Re:	
@	Patrick@vss.ch	Umfrage für unsere Maturarbeit	
@	Rita	Dein Bild auf Facebook	
	MySpace	Spaceman möchte dein Freund auf MySpa	
	Lea@vss.ch	I need your help	
@	Robbie	Fwd: Important!	

Der Mailinhalt

Eine Frage, die immer wieder gestellt wird, ist, ob man nur beim Öffnen von Anhängen vorsichtig sein muss, oder ob ein Computer bereits infiziert werden kann, wenn man eine E-Mail nur zum Lesen öffnet.

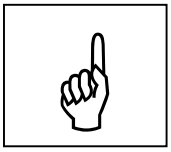
Bis Ende der Neunziger Jahre war es tatsächlich so, dass ein Computer nicht infiziert werden konnte, solange man keine Anhänge öffnete. Dies lag daran, dass Mail Clients den Inhalt einer Mail als reinen Text interpretierten. Mit dem Aufkommen des WWW wurden auch die Mail Clients so erweitert, dass sie in der Lage waren, den Inhalt einer E-Mail ähnlich wie ein Webbrowser zu interpretieren. Damit wurde es möglich, E-Mails zu versenden, die beispielsweise einen klickbaren Link oder Bilder enthalten oder sogar versuchen, Programme auf dem Computer zu installieren.
Diese Tatsache hat durchaus ihre praktische Seite. Zum Beispiel erhalten Sie bei vielen Internetforen bei der Registrierung eine E-Mail mit einem Link. Erst wenn Sie die Webseite, die mit diesem Link aufgerufen wird, besucht haben, ist die Registrierung abgeschlossen.
Diese Erweiterung der Mail Clients bringt leider auch Gefahren mit sich. Einerseits kann eine E-Mail Links enthalten, die zwar so erscheinen, als ob sie auf seriöse Webseiten verweisen, tatsächlich aber ein Programm herunterladen oder auf irgendeine Webseite führen, die jemandem gehört, der nichts Gutes im Schilde führt. Glücklicherweise haben Sie schon bevor Sie auf den Link klicken, die Möglichkeit, festzustellen, wohin der Link führt. Wenn Sie die Maus ohne zu klicken auf dem Link platzieren, zeigen die meisten E-Mail Clients an, wohin der Link führt.



Falls Ihr Mail Client das nicht tut, so gibt es andere Möglichkeiten festzustellen, wohin der Link führt. Sie können beispielsweise mit einem Rechtsklick den Link kopieren und in einen Editor einfügen.
Besonders heimtückisch sind Links, die bei flüchtigem Hinsehen auf einen seriösen Absender hinweisen, wie beispielsweise

http://www.microsoft.com.unsicher.ch/downloads/ieupdate?id=34Fcd26drg53ds3

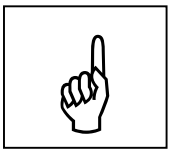
Hier erhält man den Eindruck, der Link führe zu Microsoft. Tatsächlich führt er aber zur Domain *unsicher.ch*, also zu einem ganz anderen Server.



Bevor Sie auf einen Link in einer E-Mail klicken, prüfen Sie genau, wohin Sie der Link führt. Dies gilt insbesondere, wenn Ihnen der Absender der E-Mail unbekannt ist, oder die E-Mail (scheinbar) von einem Online Dienst wie Facebook oder MySpace stammt. Verweist der Link auf eine Webseite, die nichts mit dem (scheinbaren) Absender zu tun hat, so sollten Sie den Link nicht anklicken.

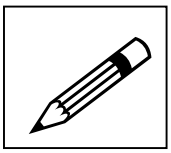
Noch gefährlicher sind E-Mails, die Code enthalten, der versucht, auf Ihrem Computer ein Programm zu installieren. Da dieser Code ausgeführt wird, sobald Sie eine E-Mail zum Lesen öffnen, kann heute bereits das Anklicken einer E-Mail auf einem ungeschützten Computer dazu führen, dass Ihr Computer infiziert wird. Gegen solche E-Mails können Sie sich nur schützen, indem Sie sie entweder gar nicht erst öffnen und ungelesen löschen oder einen aktuellen Virenscanner installiert haben, der E-Mails *vor* dem Öffnen prüft. Es kann auch sein, dass Sie von Ihrem Computer beim Öffnen einer E-Mail gefragt werden, ob Sie ein Programm (beispielsweise eine “fehlende” ActiveX-Komponente) installieren möchten. Solche Fragen sollten Sie *immer* ablehnen.

Eine weitere Variante von gefährlichen E-Mails sind solche, die Sie auffordern, gewisse Informationen wie Benutzernamen, Passwörter oder sogar Kreditkartennummern in einer Antwort-Mail mitzuteilen. Solche E-Mails erwecken in der Regel den Eindruck, als stammten sie von einer echten Organisation, beispielsweise einer Online Firma oder einem sozialen Netzwerk (Facebook etc.). Meist enthält der Mailinhalt die Schilderung irgendeines Problems, und fordert Sie auf, Ihre Benutzerdaten zu übermitteln, damit das Problem gelöst werden kann. Solche Mails sollten Sie immer ignorieren und löschen.



Seriöse Unternehmen werden Sie *niemals* auffordern, ihnen Passwörter, Kreditkartennummern oder ähnliches per E-Mail zuzusenden. Sollte ein

Unternehmen tatsächlich Probleme mit Ihrem Benutzerkonto haben, so läuft die Problembehebung immer über gesicherte Webseiten (Mehr zu gesicherten Webseiten im Kapitel WWW).



Welche der folgenden E-Mails erscheinen Ihnen seriös? Auf welche Links können Sie klicken und bei welchen sollten Sie vorsichtig sein? Begründen Sie Ihre Entscheidung.

Goldhamster würde gerne zu deinen MySpace-Freunden gehören.

Vollständiger Name:

Nachricht von Goldhamster:

Logg dich bei MySpace ein, um die Freundanfrage zu bestätigen oder abzulehnen:
http://collect.myspace.com/reloc.cfm?c=1&id=

Sieh dir das Profil von Goldhamster an:
http://www.myspace.com/ Goldhamster

Finde mehr Leute, die du kennen könntest:
http://www.myspace.com/index.cfm?fuseaction=peopleyoumayknow

Achtung - Wichtige Virenwarnung:

Nach Berichten des Bundesamts für Sicherheit in der Informationstechnik (BSI) ist derzeit ein besonders gefährlicher Virus/Trojaner im Umlauf.

Ihr PC ist ungeschützt und damit potentiell gefährdet. Bitte laden Sie unbedingt in Ihrem eigenen Interesse einen aktuellen Virenscanner herunter.

Die aktuellste Version erhalten Sie direkt hier:

http://www.Virenwarnung-sofort.info/

Mit freundlichen Grüßen
Ihr Virenwarndienst

Sie erhalten diese E-Mail, weil Sie sich beim Erweiterten MSN Angebot angemeldet haben. Microsoft respektiert Ihre Privatspäre. Wenn Sie künftig keine E-Mails über die Erweiterten MSN Angebote erhalten möchten, klicken Sie bitte unten auf den Link "Abbestellen". E-Mails von allfälligen Drittanbietern im Erweiterten MSN Angebot sind davon nicht betroffen. MSN lehnt jede Verantwortung bezüglich der angebotenen Produkte oder Dienstleistungen von Drittanbietern ab.

Abbestellen | Mehr Newsletter | Privatsphäre

Microsoft Corporation, One Microsoft Way, Redmond, WA 98052

Hallo zusammen

Hier was zur Aufheiterung für die kommende Matheprüfung ☺

http://www.youtube.com/watch?v=2yW6-zlu8AY

Mailanhänge

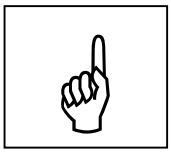
Bei Mailanhängen ist die Art des Anhangs ein wichtiges Entscheidungskriterium dafür, ob ein Anhang gefährlich ist oder nicht. Handelt es sich um einen Anhang, der ausführbaren Code enthält, so kann dieser Code unter Umständen Schaden anrichten. Sie können grundsätzlich zwischen vier Dateiarten unterscheiden.

- Dateien, die nur Daten enthalten. Solche Anhänge können Sie in der Regel ohne Gefahr öffnen. Dazu gehören beispielsweise Dateien mit den Erweiterungen “.jpg“, “.gif”, “.pdf”, “.txt”, “.mp3” und “.mov”.
- Dateien, die Daten und ausführbaren Code enthalten. Dazu gehören unter anderem Dokumente von Programmen, die Makrosprachen oder die Ausführung von Scripts unterstützen. Also beispielsweise Dateien mit den Erweiterungen “.doc”, “.xls” oder “.swf”.
- Komprimierte Dateien. Diese Dateien können einen beliebigen Inhalt haben. Möchte man einer E-Mail einen ganzen Ordner oder mehrere Dateien anhängen, so ist es oft einfacher, den Ordner oder die Dateien in einer einzigen Datei zusammenzufassen. Je nach Datei kann die Komprimierung auch eine erhebliche Verringerung der Datenmenge mit sich bringen. Da Sie nicht wissen, welche Dateien in einer komprimierten Datei enthalten sind, sollten Sie bei solchen Anhängen immer vorsichtig sein. Komprimierte Dateien verwenden oft die Erweiterung “.zip”.
- Programme und Skripte. Ist der Anhang ein Programm oder ein Skript, so ist es ziemlich offensichtlich, dass Sie hier vorsichtig sein müssen. Grundsätzlich wissen Sie nicht, ob das Programm auch tatsächlich das bewirkt, was es zu machen vorgibt.

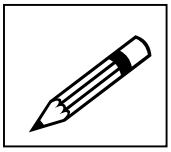
Programme haben beispielsweise die Erweiterungen “.exe”, “.com”, “.vbs”, “.app”, “.bat” oder “.scr”.

Achten Sie darauf, dass die Erweiterung immer zuhinterst steht. Ein Anhang mit dem Namen *Bitte_Lesen.txt.exe* ist kein Textdokument, sondern ein Programm.

Auch Dokumente, die nur Daten enthalten, beispielsweise Bilddateien, können unter Umständen gefährlich sein. Die Daten können so manipuliert sein, dass sie ein Fehlverhalten des Programms, das die Daten interpretiert, provozieren. Meist reagieren die Hersteller der Programme auf solche Gefahren, indem sie Updates zur Verfügung stellen. Regelmässiges Updaten verringert somit die Anfälligkeit der Programme, die Sie verwenden.



Grundsätzlich sollten Sie keinem Anhang blind vertrauen. Wenn Sie einen aktuellen Virenscanner benutzen und Ihre Software durch Installieren von Updates auf dem neusten Stand halten, so können Sie Dokumente, die nur Daten enthalten in der Regel ohne Bedenken öffnen, insbesondere wenn sie von einem bekannten Absender stammen.
Besondere Vorsicht ist geboten, wenn Ihnen der Absender unbekannt und der Anhang ein Dokument ist, das Code enthalten kann. Die Wahrscheinlichkeit ist in einem solchen Fall gross, dass der Anhang gefährlich ist.



Bei welchen der folgenden E-Mails können Sie die Anhänge ohne grosses Risiko öffnen, welche sollten Sie besser vorher mit einem Antivirenprogramm prüfen und welche Anhänge sollten Sie sicher nicht öffnen? Begründen Sie Ihre Antwort.

Sehr geehrte Damen und Herren!
Die Anzahlung Nr.629080883985 ist erfolgt
Es wurden 9520.00 EURO Ihrem Konto zu Last geschrieben.
Die Auflistung der Kosten finden Sie im Anhang in der Datei: Abrechnung.

Regel Inkasso GmbH & Co. KG
Kleinfeld Str. 21
22577 Bielefeld

Postfach 31 24 05
22577 Bielefeld

Tel.: 0521 93212-0
Fa x: 0521 92412-15

AG Bielefeld HRA 26315
Steuer-Nummer: 249/5749/1807

abrechnung.zip (19.2 KB)

Liebe Schülerinnen und Schüler der 4. Klassen Gymnasium

Ich schicke Ihnen Im Auftrag unseres Prorektors als Anhang den Brief mit der Urlaubsregelung für den Besuch von Universitäts-/ETH-Informationstagen.

Freundlicher Gruss

Edith Sager, Sekretariat

Brief Infotage Uni.pdf

Liebe Schülerinnen und Schüler

Da ich krank bin, fällt die Doppelstunde von morgen leider aus. Ich möchte Sie bitten, die Aufgaben im Anhang selbständig zu lösen.

Freundliche Grüsse

Bettina Huber, Ihre Französischlehrerin

Aufgaben.doc

Hinweise zu den Einstellungen in Mail-Clients und Antivirenprogrammen

Viele Anbieter von E-Mail Diensten prüfen bereits von sich aus alle E-Mails, die über ihre Server laufen, auf Spam und Malware. Trotzdem sollten Sie nicht auf eigene Schutzmassnahmen verzichten. Deshalb folgen hier ein paar Hinweise, wie Sie sich vor unangenehmen Überraschungen schützen können.

Finden Sie heraus, ob und welche E-Mails von Ihrem privaten E-Mail Konto von Ihrem Anbieter geprüft werden oder nicht.
Hinweis: Wenn Sie einen Webmailer benützen, steht meistens irgendwo, ob eine E-Mail geprüft wurde. Falls Sie mit einem Mail Client arbeiten, so finden Sie vielleicht auf der Homepage Ihres Providers Informationen.

Wenn Sie E-Mails ausschliesslich über einen Webmailer schreiben und lesen, dann betrifft Sie dieser Abschnitt weniger.

Kommerzielle Antivirenprogramme können so eingestellt werden, dass Sie E-Mails automatisch auf Malware überprüfen. Ob eine E-Mail bereits beim herunterladen oder wenn sie geöffnet wird oder sogar erst, wenn auf einen Anhang geklickt wird, vom Antivirenprogramm geprüft wird, hängt vom verwendeten Programm und eventuell von den Einstellungsmöglichkeiten ab. Grundsätzlich ist es am sichersten, wenn eine E-Mail möglichst früh geprüft wird.
Je nach Programm, haben Sie zudem die Möglichkeit, Anhänge in E-Mails, die Sie verschicken, ebenfalls auf Malware zu prüfen.

Achtung: Einige gratis Antivirenprogramme bieten keine Prüfung von E-Mails an. Falls Sie ein solches Programm verwenden, empfiehlt es sich, Anhänge vor dem Öffnen manuell vom Antivirenprogramm prüfen zu lassen, indem Sie beispielsweise den Anhang sichern, ohne ihn zu öffnen, und dann die Datei mit dem Antivirenprogramm prüfen.

Viele Hersteller kommerzieller Antivirenprogramme bieten zusätzlich Anti-Spam Programme an. Diese so zu konfigurieren, dass sie wirkungsvoll sind, aber keine seriösen Mails als Spam verloren gehen, ist jedoch nicht ganz so einfach.
Viele Anbieter von E-Mail Diensten prüfen einkommende Mails auf Spam. Falls eine E-Mail als Spam erkannt wird, so wird im Informationsteil der E-Mail ein entsprechender Eintrag hinzugefügt. Einige Mail Clients sind in der Lage, diese Information zu verarbeiten und als Spam gekennzeichnete Mails auch als solche zu interpretieren.

Kontrollfragen

1. Kommentieren Sie die folgenden Aussagen.

   Linda sagt: "*Ich halte das Antivirenprogramm auf meinem Computer immer auf dem neusten Stand, also kann ich jedes E-Mail und jeden Anhang auch ohne Bedenken Öffnen.*"

   Marco meint: "*Ich will auf keinen Fall ein gefährliches Programm auf meinem Computer. Deshalb lösche ich sofort jede E-Mail, deren Absender ich nicht kenne.*"

2. Sie arbeiten mit einer Klassenkollegin an einem Vortrag und sie schickt Ihnen ihre Unterlagen per E-Mail in Form einer angehängten Worddatei. Können Sie die Datei bedenkenlos öffnen? Begründen Sie Ihr Vorgehen.

3. Beim Öffnen einer E-Mail meldet Ihr Computer, dass ihm eine Softwarekomponente fehlt, um die Nachricht anzeigen zu können. Er fragt Sie, ob Sie die Komponente installieren wollen. Klicken Sie auf "Ok" oder auf "Abbrechen"? Begründen Sie Ihre Wahl.

4 – WWW

Voraussetzungen

- Sie können mit einem Webbrowser umgehen
- Sie kennen die Bedeutung der Begriffe URL, Cookie, Browser Plugin

Lernziele

- Sie kennen einige Strategien, die ein Angreifer anwendet, um Ihren Computer zu infizieren
- Sie können einschätzen, wann ein Dialog auf einen möglicherweise gefährlichen Download hinweist
- Sie kennen einige Möglichkeiten, wie Sie prüfen können, ob eine Aufforderung zum Download eines Programms wahrscheinlich echt ist oder nicht
- Sie erfahren an einem simulierten praktischen Beispiel einen möglichen Angriff auf Ihren Computer und seine Auswirkungen

Einführung

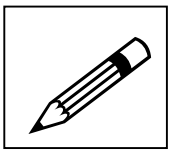
Viele Webseiten sind heute sehr komplex aufgebaut. Neben Texten und Bildern können wir auch Filme anschauen, Spiele spielen, Dateien herunterladen, uns mit anderen Benutzern unterhalten, einkaufen, uns selbst auf einer Webseite darstellen und so weiter. Um alle diese Aufgaben zu bewältigen, muss ein Webbrowser nicht nur Code, beispielsweise JavaScript, ausführen können. Er ist auch auf die Hilfe von Plugins angewiesen. Wenn Sie beispielsweise auf YouTube ein Video anschauen wollen, so benötigen Sie das Flash Player Plugin und Ihr Browser muss so eingestellt sein, dass er die Ausführung von JavaScript zulässt. Fehlt ein entsprechendes Plugin, so erscheint auf der Webseite eine Fehlermeldung und meistens auch ein Link darauf, wo Sie das Plugin herunterladen können.
Ein Angreifer hat grundsätzlich zwei Möglichkeiten, wie er schädliche Software auf Ihren Computer bringen kann. Er kann versuchen, Sie auf eine gefährliche Webseite zu locken, beispielsweise durch versenden von E-Mails mit entsprechenden Links, oder er kann versuchen, eine “normale” Webseite zu hacken und so zu verändern, dass sie gefährlich wird.
Man kann grob zwei Arten von gefährlichen Webseiten unterscheiden.

- Bösartige Webseiten, die von einem Angreifer selbst ins Internet gestellt werden.
- Gutartige Webseiten, die ungenügend geschützt sind, sodass ein Angreifer bösartigen Code darauf platzieren kann.

Aus dieser Aufzählung können Sie erkennen, dass nicht nur Ihre Surfgewohnheiten ausschlaggebend sind, ob Sie auf eine gefährliche Webseite gelangen. Ein wichtiger Punkt ist auch, ob die Betreiber von Webseiten ihre Seiten genügend sorgfältig aufgebaut haben und aktuelle Sicherheitsmassnahmen treffen. Diesen Punkt können Sie als Nutzer nicht beeinflussen.

Infizierte Webseiten verfolgen im Prinzip zwei Ziele. Entweder wird versucht, an vertrauliche Daten, wie Passwörter, Kreditkartennummern und so weiter, zu kommen oder Ihr Computer soll mit schädlicher Software infiziert werden.
Letzteres kann grundsätzlich auf zwei Arten passieren. Entweder versucht ein Angreifer, Sie zu überzeugen, auf Links in dieser Seite klicken, oder es wird bereits beim Aufruf der Seite automatisch, und möglicherweise sogar ohne, dass Sie etwas bemerken, ein schädliches Programm heruntergeladen.

Ihre Surfgewohnheiten



Zunächst sollen Sie sich ein paar Gedanken dazu machen, wofür Sie das Internet nutzen und wie Sie sich im Internet bewegen. Kreuzen Sie bei den folgenden Aussagen an, welche jeweils am ehesten auf sie zutrifft.

Das Internet als Informations- und Datenquelle

- ☐ Zur Informationssuche benutze ich Suchmaschinen wie Google oder Bing etc.
  - ☐ Die Links bei den angezeigten Suchresultaten halte ich grundsätzlich für unbedenklich.
- ☐ Ich lade Musik, Software, Spiele etc. herunter.
  - ☐ Ich informiere mich vorher darüber, ob die Webseite vertrauenswürdig ist.

Das Internet zur Unterhaltung

- ☐ Ich besuche Webseiten, die Bilder, Filme und ähnliches anbieten, beispielsweise YouTube oder Tillate.
- ☐ Ich nutze Webseiten, die gratis Online-Spiele anbieten.
- ☐ Ich höre Musik übers Internet.
- ☐ Ich habe schon selbst Bilder, Musik, Filme etc. auf eine entsprechende Webseite gepostet.

Das Internet als Soziales Netzwerk

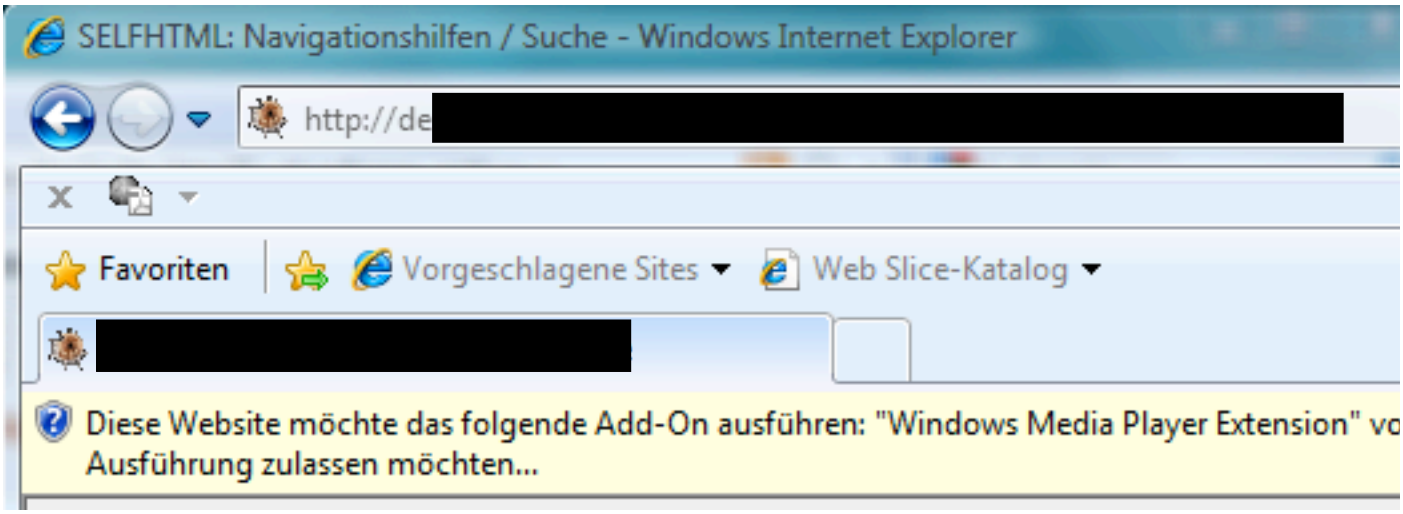
- ☐ Ich bin Mitglied in einem sozialen Netzwerk, beispielsweise Facebook, MySpace etc.
  - ☐ Ich kenne alle meine Freunde persönlich.
  - ☐ Wenn ich im Internet etwas Spannendes entdecke, teile ich den Link meinen Freunden mit.
  - ☐ Meine Freunde haben mir auch schon Links geschickt, die ich angeklickt habe
    - ☐ Ich habe diesen Links vertraut.
  - ☐ Ich habe auf meiner Seite Links auf externe Fotos, Musik, Filme oder Webseiten eingebaut.

☐ Ich nutze Anwendungen, die auf der Homepage des sozialen Netzwerks angeboten werden.

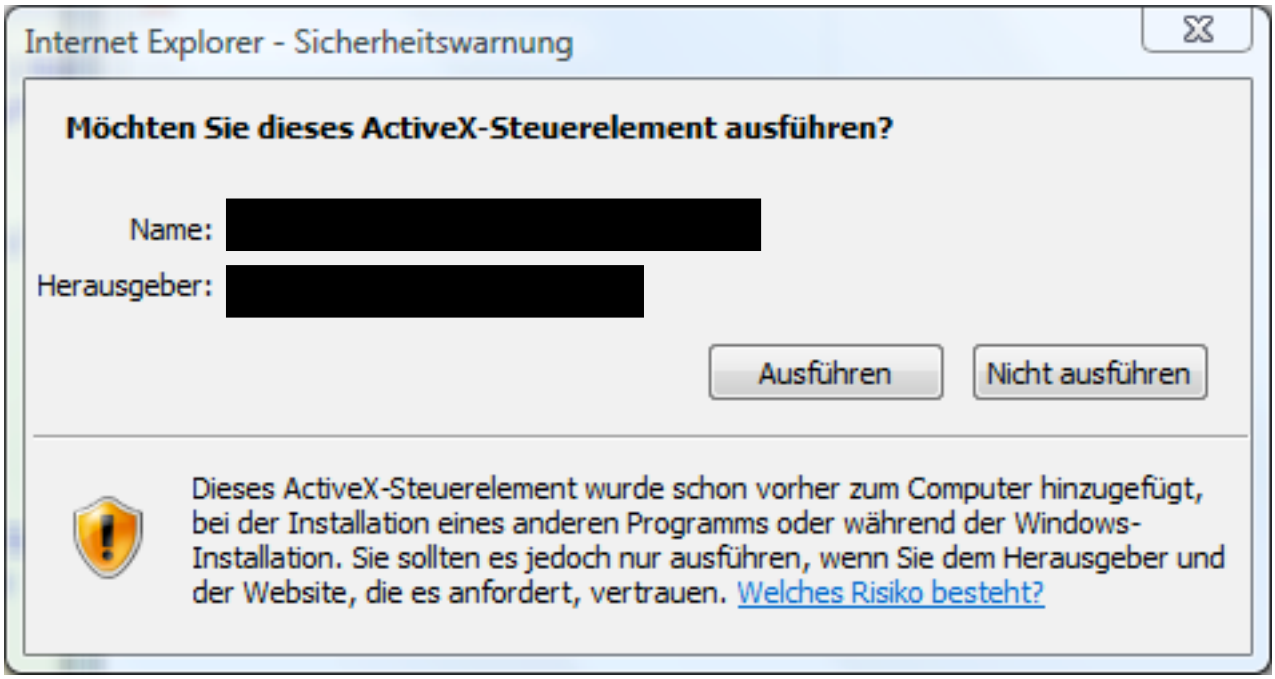
☐ Ich erkundige mich vor der Nutzung, ob die Anwendung als gefährlich bekannt ist.

Reaktionen auf Browsermitteilungen

☐ Ich bin beim Surfen auch schon auf Seiten gelangt, bei denen mein Browser etwas blockiert hat, beispielsweise ActiveX Elemente, Popup Fenster etc.



☐ Ich klicke jeweils auf den Balken und hebe die Blockade auf (Es erscheint darauf beispielsweise folgende Mitteilung.

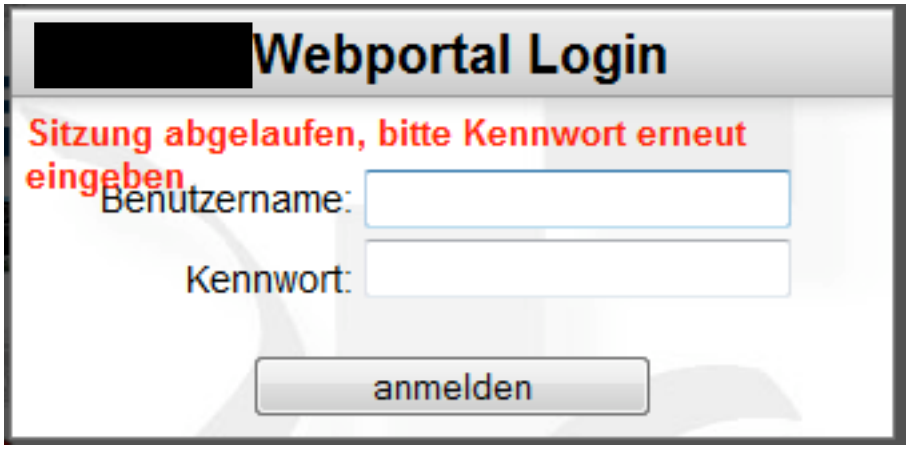


☐ Ich klicke in der Regel auf *Ausführen*.

☐ Ich bin beim Surfen auch schon auf Seiten gestossen, die mich aufgefordert haben, etwas zu installieren, damit die Seite vollständig angezeigt werden kann.

☐ Ich klicke jeweils auf den angegebenen Link und installiere die fehlende Software.

☐ Es ist schon vorgekommen, dass ich irgendwo eingeloggt war und plötzlich aufgefordert wurde, mich nochmals anzumelden.



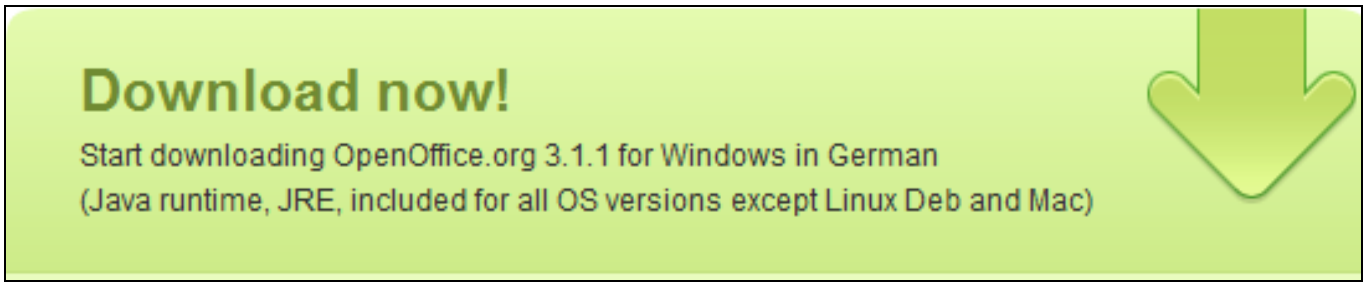
Keine dieser Aktivitäten führt grundsätzlich dazu, dass Ihr Computer sich mit bösartiger Software infiziert. Sie sollen Ihnen vielmehr in Erinnerung rufen, wie vielseitig wir heute das Internet nutzen. Dabei laufen wir auch Gefahr, auf Webseiten zu stossen, die unseren Computer angreifen wollen. Das heisst, dass im Gegensatz zu bösartigen E-Mail-Anhängen, die Ihnen von einem Angreifer zugeschickt werden, die Benutzer auf infizierte Webseiten gelockt werden und dann selbst bösartige Programme herunterladen oder vertrauliche Daten preisgeben.

Da wohl kaum jemand absichtlich auf eine infizierte Webseite zugreifen wird, drängt sich die Frage auf, wie ein Angreifer vorgeht, damit wir ihm “ins Netz” gehen.

Mitteilungsbedürftige Browser

Nicht nur seriöse Unternehmen analysieren das Surfverhalten der Internetnutzer. Auch für einen potenziellen Angreifer ist es interessant, möglichst viel über den Computer eines Benutzers zu erfahren und zu wissen, wie sich ein Benutzer im Internet verhält, wofür er es benutzt und welche Seiten er in letzter Zeit besucht hat.
Dass unser Computer so viele Informationen preisgibt, ist vielfach beabsichtigt. Ein Betreiber einer Website kann dadurch die Darstellung und den Inhalt der Seiten für den entsprechenden Browser und das verwendete Betriebssystem optimieren und so die Benutzung seiner Seite vereinfachen und allenfalls sinnvolle Fehlermeldungen und Hinweise zu deren Behebung anzeigen.

Beispiele



Der Server erkennt, welches Betriebssystem und welche Sprache wir verwenden und erleichtert uns so das Herunterladen der korrekten Programmversion.

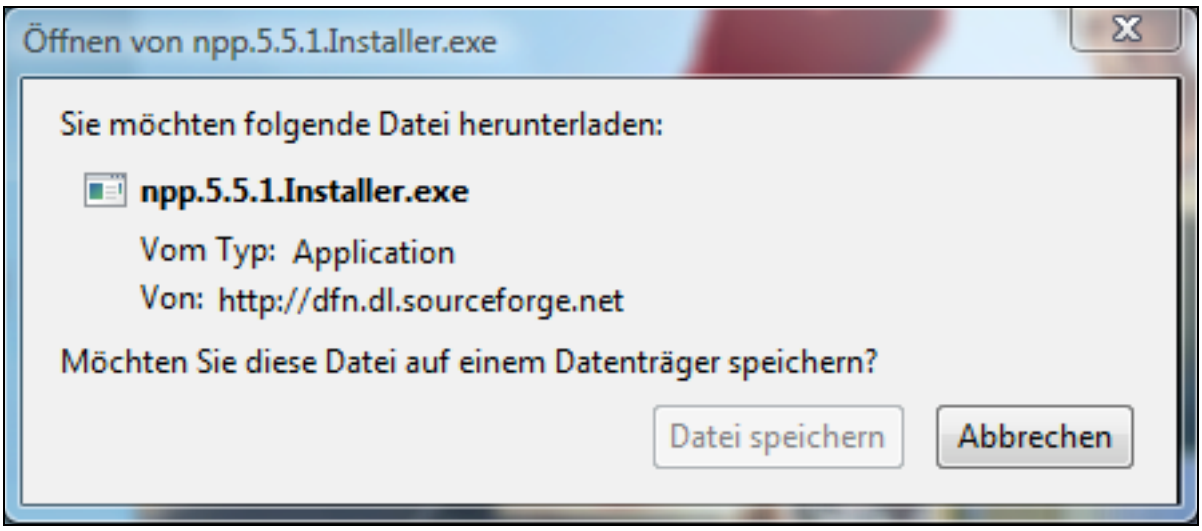
Der Server merkt, dass ein Element (hier ein Video) auf dem Computer des Benutzers nicht dargestellt werden kann, weil eine Einstellung im Browser deaktiviert ist (JavaScript) oder ein entsprechendes Plugin (Adobe Flash Player) fehlt oder zu alt ist und informiert den Benutzer auch, wie er das Problem lösen kann. Dass eine solche Antwort möglich ist, bedeutet, der Server kann herausfinden, wie unser Browser eingestellt ist und welche Plugins installiert sind.

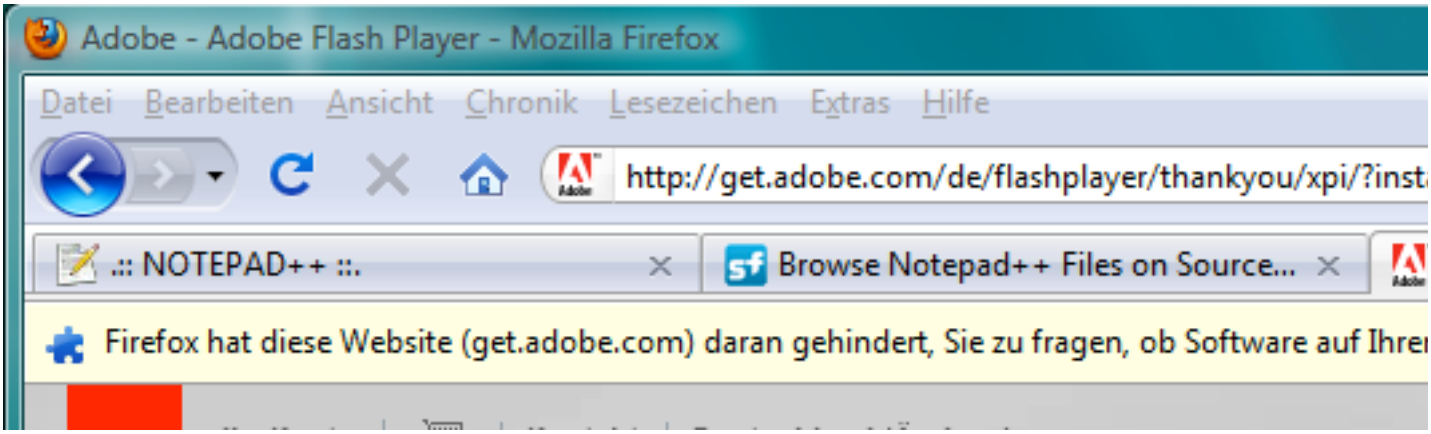
Es ist durchaus überraschend, wie viele Informationen ein Betreiber einer Webseite über unseren Computer herausfinden kann. Das reicht von relativ offensichtlichen

Informationen wie beispielsweise Art und Version des Browsers und installierte Plugins bis zu installierten Schriften und kürzlich besuchten Webseiten.

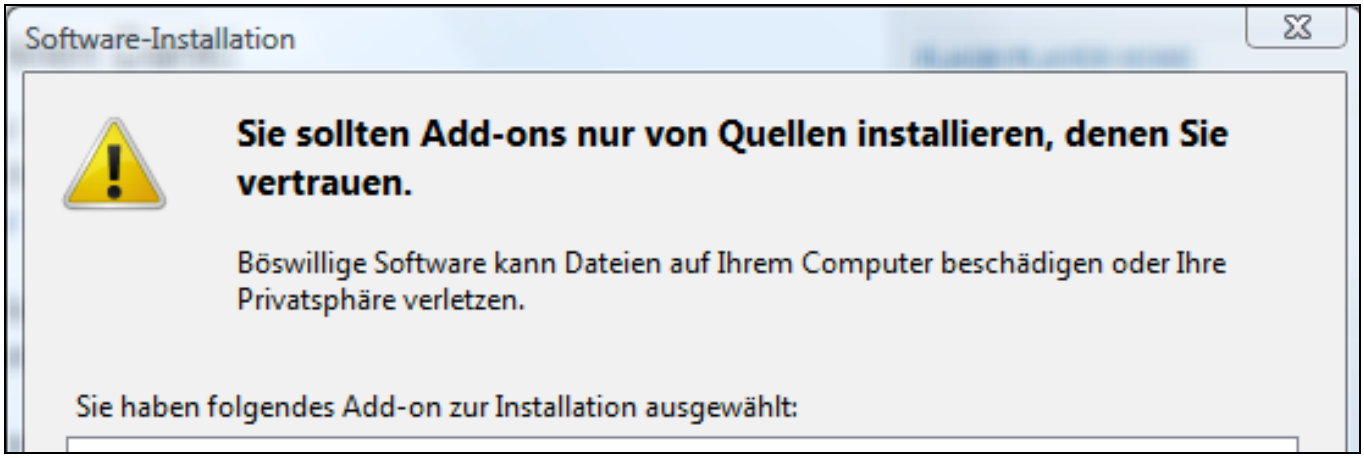
Diese Informationen können natürlich auch missbraucht werden. Wenn ein Server beispielsweise erkennt, dass ein Benutzer mit einer veralteten Version einer bestimmten Komponente arbeitet, die bekannte Sicherheitsmängel aufweist, so kann er die ausnützen.

Auch uns gegenüber zeigen sich Browser durchaus kommunikativ und fragen uns, was wir mit einer Datei, die heruntergeladen wird, anfangen wollen oder ob blockierte Elemente zugelassen werden sollen.



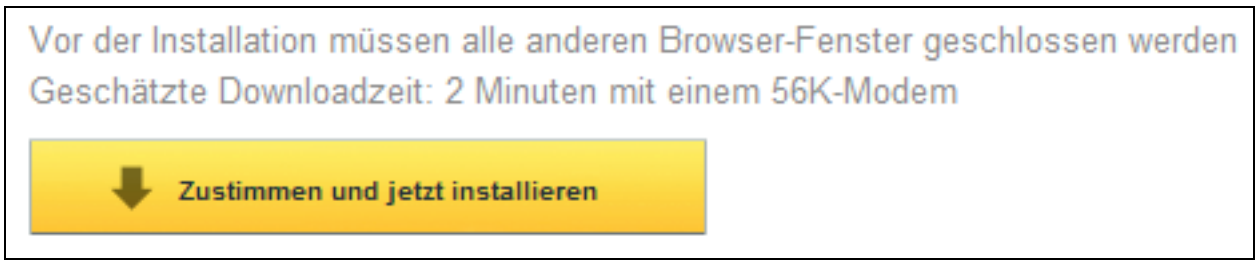


Dabei kann das Mitteilungsbedürfnis eines Browsers so gross werden, dass man sich als Benutzerin darüber ärgert und die Aktionen, ohne die Texte durchzulesen, akzeptiert. Ein solches Verhalten kann dadurch unterstützt werden, dass wir auch Warnungen erhalten, wenn wir seriöse Komponenten installieren.
Einem Angreifer ist dieses Verhalten durchaus bewusst.



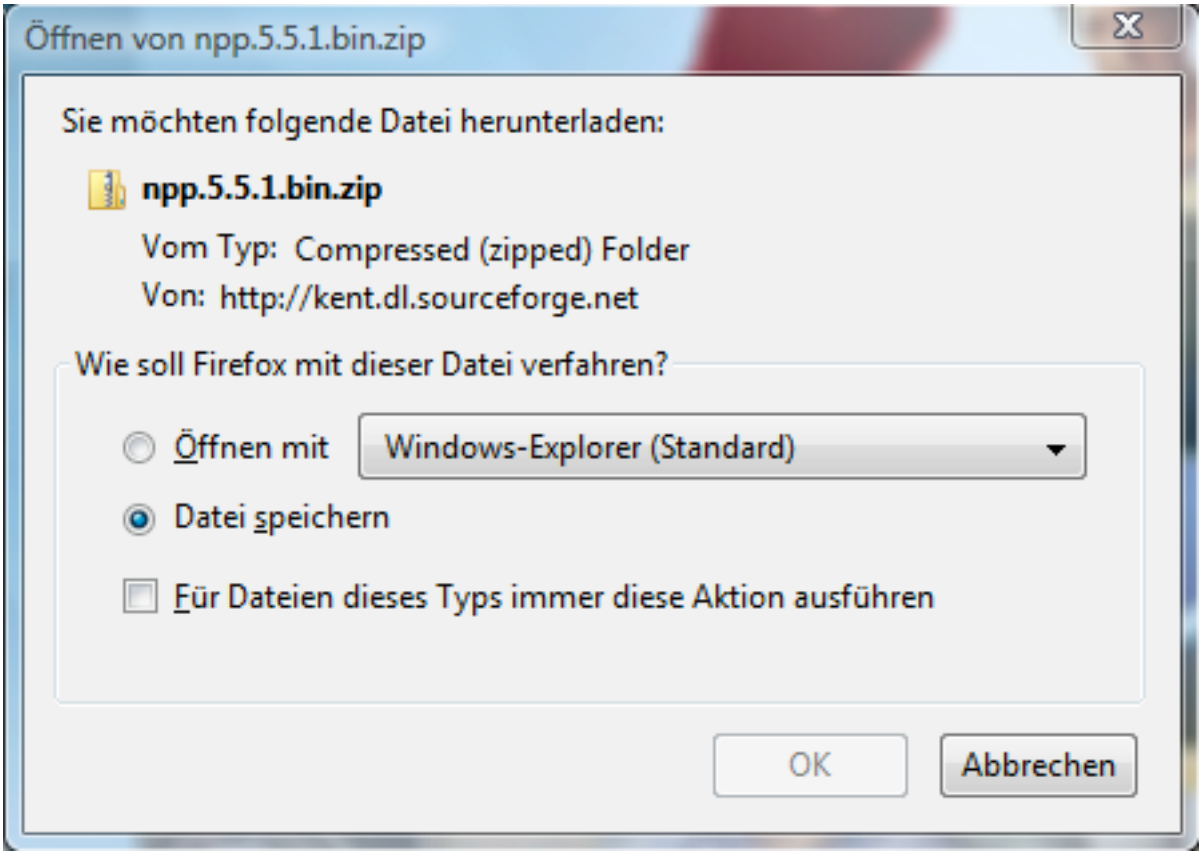
Automatische Downloads

Webseiten können so aufgebaut werden, dass eine Datei automatisch herunter geladen wird, wenn die Seite aufgerufen wird. Eine solche Technik verwenden viele Softwareanbieter. Dabei gelangen Sie meist zuerst auf eine Seite mit verschiedenen Hinweisen und können durch einen Klick auf einen Button den Download auslösen.



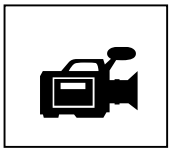
Ein Klick auf den Button löst nicht nur den Download aus, sondern führt auf eine nächste Seite, die weitere Informationen, beispielsweise Installationshinweise, enthalten kann.

Ein Angreifer kann eine “normale” Webseite so bearbeiten, dass sie diese Funktionalität aufweist. Sobald Sie diese Seite aufrufen, beginnt der Download, ohne dass Sie ihn bewusst ausgelöst haben. In der Regel werden Sie von Ihrem Browser gefragt, was Sie mit einer Datei, die herunter geladen wird, tun möchten.



Ein Angreifer kann deshalb zu Ihrer "Beruhigung" vorher noch ein eigenes Dialogfenster einblenden, das Sie darauf hinweist, dass für das Betrachten der Seite zunächst ein "wichtiges" oder "fehlendes" Programm installiert werden müsse.

Für einen Angreifer wäre es natürlich von Vorteil, wenn ein Download vollkommen automatisch geschieht, ohne dass ein Dialogfeld erscheint, in dem der Benutzer dem Download zustimmen muss. An und für sich sollte so etwas nicht möglich sein. Leider finden Angreifer immer wieder Softwarefehler, die sie genau für solche Zwecke nutzen können. Diese so genannten *Drive-By-Downloads* sind besonders gefährlich, weil es bereits genügt, eine infizierte Seite anzuklicken, damit das Herunterladen bösartiger Software ausgelöst wird ohne dass eine Benutzerin dies merkt, weil alles im Hintergrund abläuft.



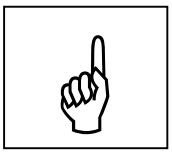
Folgender Link führt zu einem ca. 12 Minuten langen Film (in englisch), der demonstriert, was passiert, wenn ein Computer ohne dass es der Benutzer merkt, infiziert wird.
http://www.watchguard.com/education/video/play.asp?vid=dbd-cubecast

Webseiten, die Schaden anrichten

Damit ein Angreifer überhaupt die Gelegenheit hat, Ihren Computer zu infizieren, muss er Sie auf eine infizierte Webseite locken. Es gibt verschiedene Möglichkeiten, wie er dabei vorgehen kann.

Schnäppchenjäger

Im Internet gibt es viele Seiten, die kostenlose Downloads von Musik, Filmen, Spielen etc. anbieten. Die Motivationen, Produkte gratis zur Verfügung zu stellen, sind vielseitig. Als Internetnutzerin haben wir uns an solche Angebote gewöhnt. Dass wir dabei oft nichts über den Anbieter wissen, kümmert die wenigsten Benutzer.



Ein Angreifer kann Ihre Gutgläubigkeit ausnützen, indem er Sie mit einem Gratisangebot auf seine Seite lockt. Da Sie die Seite mit dem Zweck besuchen, Software herunterzuladen, werden Sie auch die Dialoge, ob Sie die Dateien herunterladen möchten, weniger kritisch durchlesen.

Falsche Freunde

Immer mehr Personen nützen heute soziale Netzwerke wie Facebook, MySpace und Ähnliches. Dabei ist der virtuelle "Freundeskreis" vieler Teilnehmer meist deutlich grösser als der reale Bekanntenkreis, das heisst, viele unserer "Freunde" kennen wir eigentlich gar nicht. Viele Nutzer und Nutzerinnen bringen ihren virtuellen Freunden grosses Vertrauen entgegen, insbesondere betrachten sie deren Benutzerprofile, unterhalten sich mit ihnen und folgen auch interessanten Links, die sie von ihren virtuellen Freunden mitgeteilt bekommen.
Für Angreifer sind soziale Netzwerke gerade deshalb besonders interessant, denn wenn es ihnen gelingt, die Identität einer Teilnehmerin oder eines Teilnehmers zu stehlen oder ihren Computer so zu infizieren, dass er an die Freunde des Teilnehmers Links zu infizierten Seiten schickt, so ist die Wahrscheinlichkeit, dass die Empfängerinnen diesen Links folgen, relativ hoch.
Da soziale Netzwerke in der Regel ihren Benutzern auch erlauben, selbst HTML Code in Ihren Profilen einzubauen (wenn auch in eingeschränktem Masse), kann ein Angreifer, der sich als Teilnehmer des Netzwerks ausgibt, versuchen, bösartigen HTML Code oder Links auf infizierte Seiten in seinem Profil einzubinden.
Ausserdem geben viele Benutzerinnen von sozialen Netzwerken bewusst oder unbewusst relativ viel über sich und ihre Lebensgewohnheiten preis. So können beispielsweise Blogeinträge, verlinkte Fotos, Gruppenmitgliedschaften, angezeigte Gemütszustände etc. unter Umständen ein sehr genaues Bild über eine Person liefern. Ein geschickter Angreifer kann diese Informationen gezielt nutzen und so rasch ein Vertrauensverhältnis aufbauen, das er anschliessend dazu missbraucht, um an vertrauliche Informationen wie Zugangsdaten zu kommen oder das Opfer zu bestimmten Aktionen zu bewegen. Eine solche Vorgehensweise gehört zum so genannten *Social Engineering*.

Manipulierte Webseiten

Eine ebenfalls äusserst beliebte Vorgehensweise von Angreifern ist, dass sie versuchen in seriöse Webseiten einzudringen und diese so abzuändern, dass beim Besuch der Seite entweder ein automatischer Download einer bösartigen Software ausgelöst wird, oder die Besucherin, ohne es zu merken, auf eine andere, vom Angreifer kontrollierte Seite umgelenkt wird. Diese Seite könnte beispielsweise gleich aussehen wie die Anmeldeseite der seriösen und ein Angreifer könnte so die Zugangsdaten eines Benutzers erlangen.

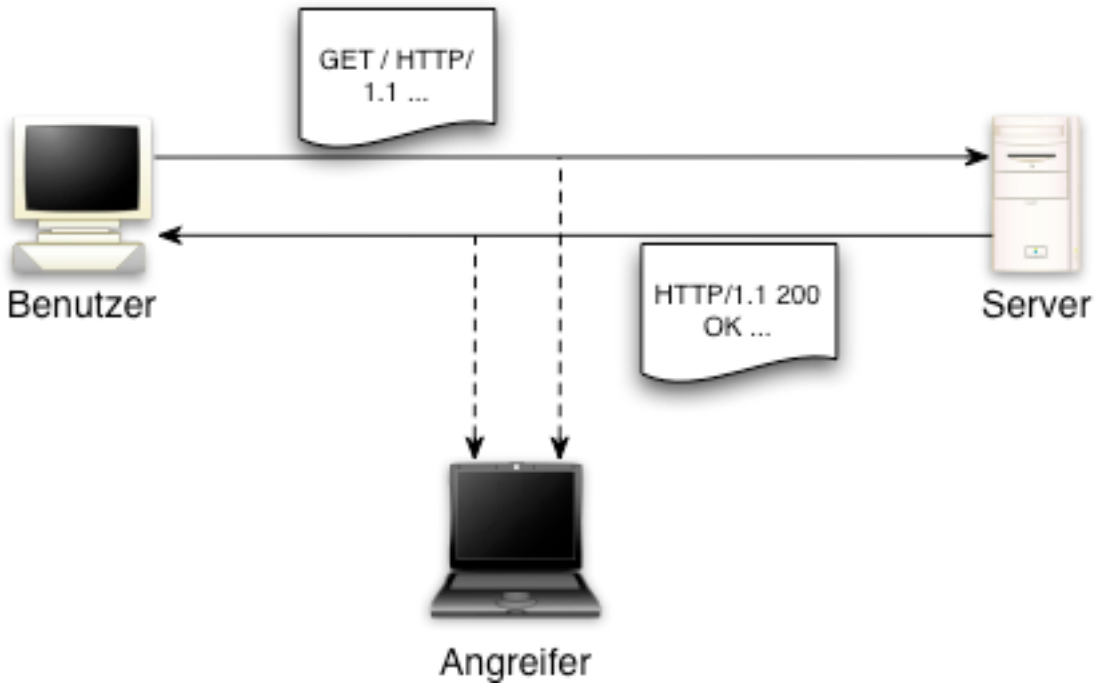
Es gibt mittlerweile Untergrundorganisationen, die Softwarepakete verkaufen, mit denen ungenügend geschützte Webserver auf einfache Weise infiziert werden können.

Böse Werbeüberraschung

Werbung auf Webseiten ist für viele Betreiber eine nicht unwesentliche Einnahmequelle. Dabei darf ein Drittanbieter auf der Webseite des Betreibers Code platzieren, der die Werbung anzeigt. Normalerweise handelt es sich bei diesen Drittanbietern um anerkannte Firmen, die auf Internetwerbung spezialisiert sind und denen der Betreiber vertraut. Es ist nun aber durchaus üblich, dass diese Firmen den Werbeplatz teilweise weitervermieten dürfen und so weiter. Das kann dazu führen, dass ein Angreifer die Gelegenheit erhält, seinen Code auf einer an und für sich seriösen Seite zu platzieren.

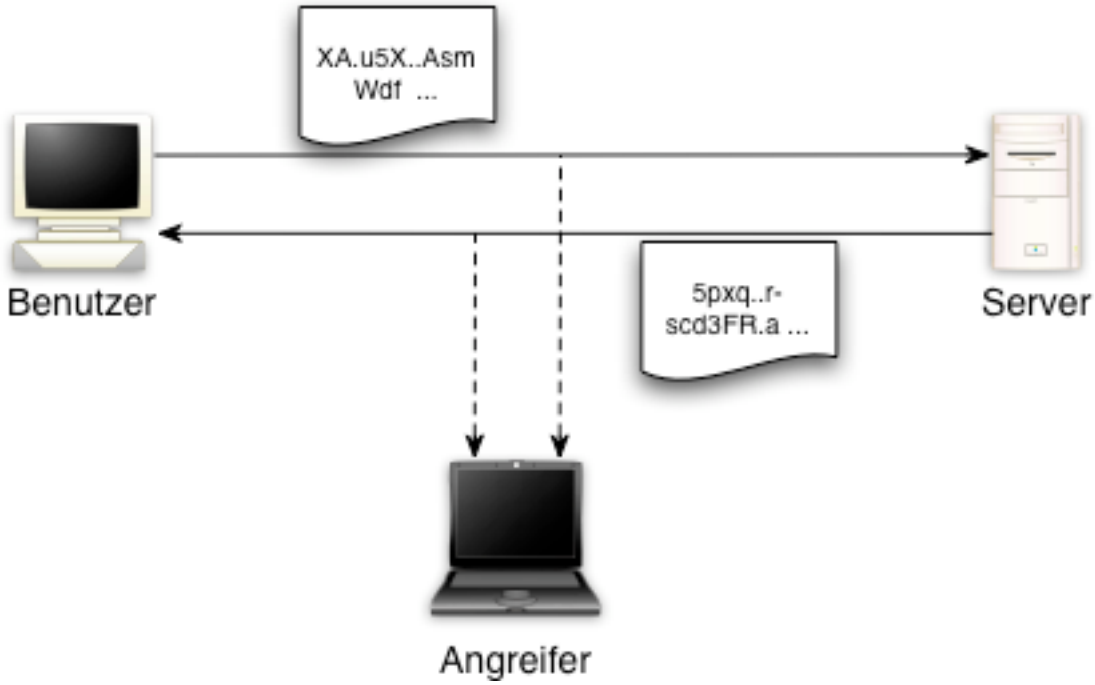
S wie Sicher

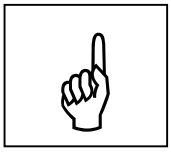
Wenn wir uns im Internet bewegen, wird in der Eingabezeile des Browsers die jeweils die URL der entsprechenden Seite angezeigt. In der Regel beginnt die URL mit “http://”. Vielleicht haben Sie auch schon Webseiten besucht, die stattdessen mit “https://” beginnen. Das “s” steht für *secure*.
Normalerweise wird der Inhalt einer Webseite in einer leicht lesbaren Form übermittelt. Das gilt auch für die Daten, die wir über ein Formular (beispielsweise wenn wir uns irgendwo anmelden) zu einem Webserver zurückschicken. Somit ist es für jeden, der die Verbindung abhören kann, leicht möglich, herauszufinden, welche Informationen hin und her geschickt werden.



Wenn wir uns beispielsweise bei GMail anmelden, möchten wir natürlich nicht, dass unser Benutzername und vor allem unser Kennwort einfach so gelesen werden können. Seriöse Organisationen, auf deren Webseiten man sich anmelden muss, verwenden deshalb

mindestens für die Anmeldung eine Verschlüsselung. Geschieht die Kommunikation zwischen Benutzerin und Webserver über eine verschlüsselte Verbindung, so wird dies in der Eingabezeile dadurch angezeigt, dass anstelle von “http://” “https://” steht. Ausserdem wird im Browserfenster auch noch irgendwo ein Schloss angezeigt (wo, ist browserabhängig, meistens entweder zuoberst, zuunterst oder in der Eingabezeile selbst). Sollte ein Angreifer bei der Kommunikation mithören, so würde er nur unverständliche Zeichen empfangen.

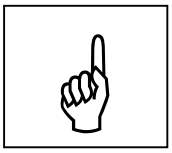




Bei manchen Webseiten ist es nicht so leicht zu erkennen, dass unsere Eingaben auch tatsächlich verschlüsselt übermittelt werden. Bei Facebook oder MySpace sind die Anmeldeseiten normale Webseiten. Wenn wir uns Einloggen, werden die Daten trotzdem über eine verschlüsselte Seite geschickt, von der ein Benutzer allerdings nichts mitbekommt. Nur wenn eine Benutzerin den Quelltext der Anmeldeseite ansieht, erkennt sie, dass die Anmeldedaten über eine verschlüsselte Seite verschickt werden.

Damit ein Webserver verschlüsselt kommunizieren kann, muss er ein Sicherheitszertifikat besitzen. Diese Zertifikate sind kostenpflichtig. Es gibt verschiedene Organisationen, die autorisiert sind, solche Zertifikate auszustellen. Bietet ein Webserver eine Verschlüsselung an, prüft der Browser der Benutzerin zunächst, ob es sich um ein autorisiertes Zertifikat handelt. Falls nicht, erscheint eine Warnung.

Diese Warnung muss noch nicht unbedingt heissen, dass Sie im Begriff sind, auf eine Webseite mit bösartigem Code zuzugreifen. Grundsätzlich kann jeder, der einen Webserver betreibt, selbst ein (kostenloses) Zertifikat erzeugen. Sie sollten aber trotzdem stutzig werden. Vor allem grössere Organisation oder Online-Shops verfügen immer über autorisierte Zertifikate. Eine solche Warnung kann deshalb bedeuten, dass die Webseite, auf die Sie zugreifen, nicht seriös ist. Wenn Ihr Computer beispielsweise bereits infiziert ist, sodass er auf einen bösartigen DNS Server zugreift, kann zwar die URL in der Eingabezeile korrekt sein, aber Sie landen trotzdem auf dem Server des Angreifers.

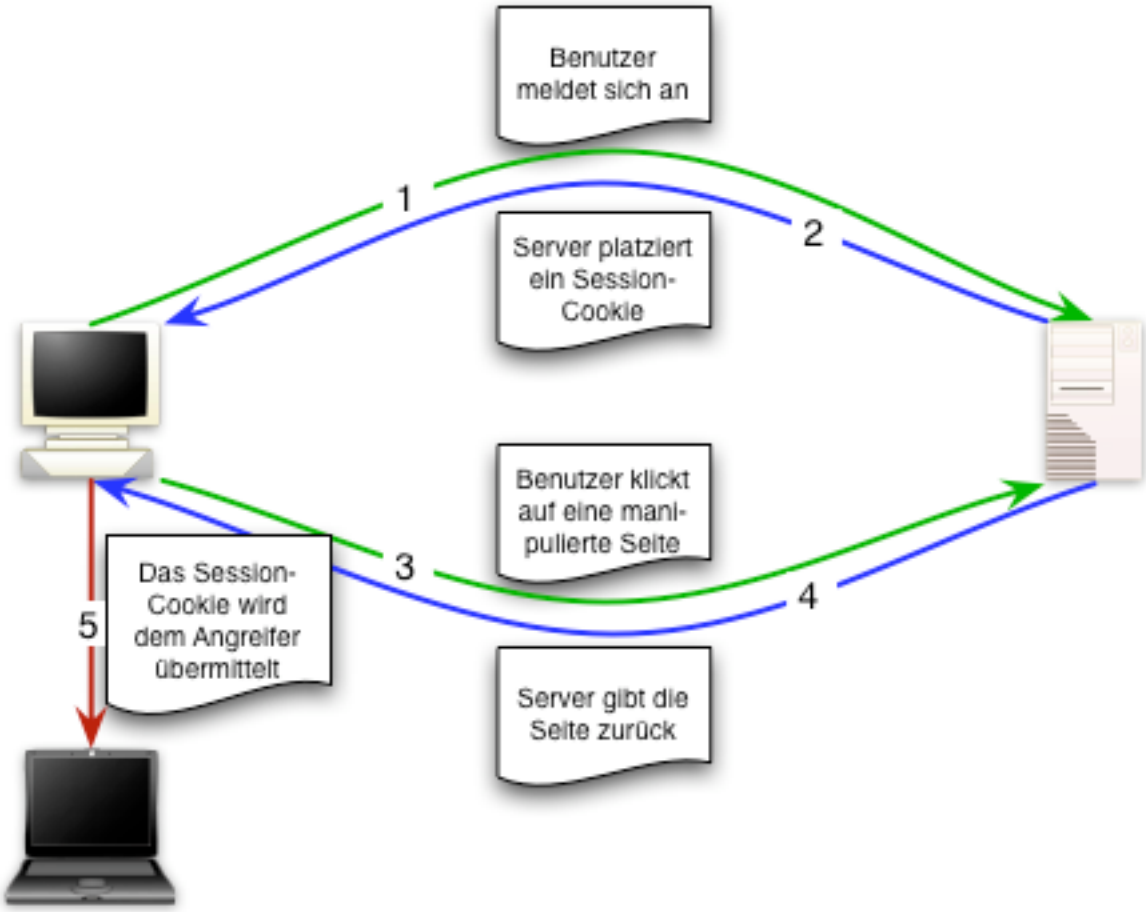


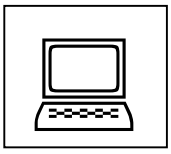
Falls eine Warnung über ein nicht verifizierbares Zertifikat erscheint, sollten Sie vorsichtig sein und eher auf Abbrechen klicken und vor allem keinesfalls sensible Informationen wie Kennwörter oder gar Kreditkartennummern eingeben.

Gestohlene Identitäten

Viele Webseiten platzieren so genannte Cookies auf den Computern der Benutzer. Cookies sind für einen Computer unschädlich. Sie können verschiedene Informationen über eine Besucherin einer Webseite enthalten, beispielsweise wie oft sie eine Webseite besucht hat, wann ihr letzter Besuch stattfand und so weiter. Cookies können auch zum Speichern von Benutzernamen verwendet werden, damit beim nächsten Besuch der Webseite ein Benutzer persönlich begrüsst werden kann oder bei der Anmeldung der Benutzername automatisch eingesetzt wird. Cookies haben immer eine bestimmte “Lebensdauer”. Diese kann von wenigen Minuten bis zu mehreren Jahren reichen, oder davon abhängen, wie lange ein Browserfenster geöffnet ist.
Webseiten, die es zulassen, dass Benutzer selbst Daten auf der Seite platzieren können, erlauben dies in der Regel nur registrierten und angemeldeten Benutzern. Ein Server muss sich merken können, ob sich ein Benutzer angemeldet hat oder nicht. Dies kann er beispielsweise tun, indem er nach der Anmeldung ein so genanntes Session-Cookie auf dem Computer des Benutzers platziert, das wieder gelöscht wird, wenn der Benutzer sich abmeldet oder die Seite schliesst. Ein Angreifer kann versuchen, ein Session-Cookie einer Benutzerin zu stehlen und sich so als diese auszugeben.

Ein solcher Angriff ist für einen Benutzer sehr schwierig zu entdecken, weil aus Sicht des Benutzers nichts Ungewöhnliches passiert. Auch Antivirenprogramme erkennen einen solchen Angriff nicht.





Starten Sie den Browser, den Sie üblicherweise benutzen, und schauen Sie nach, welche Programme Cookies auf Ihrem Computer platziert haben. Hinweis: Das Anzeigen von Cookies ist nicht bei allen Browsern gleich einfach. Bei Firefox sehen Sie die Cookies nur, wenn Sie über *Extras->Einstellungen->Datenschutz* auf *einzelne Cookies löschen* klicken. Beim Internet Explorer müssen Sie über *Extras->Internetoptionen->Allgemein* im Abschnitt *Browserverlauf* auf Einstellungen und anschliessend auf *Dateien anzeigen* klicken. Bei Safari können Sie über *Einstellungen->Sicherheit* auf *Cookies anzeigen* klicken.
Sie werden erstaunt sein, wie viele Cookies sich auf Ihrem Computer befinden...

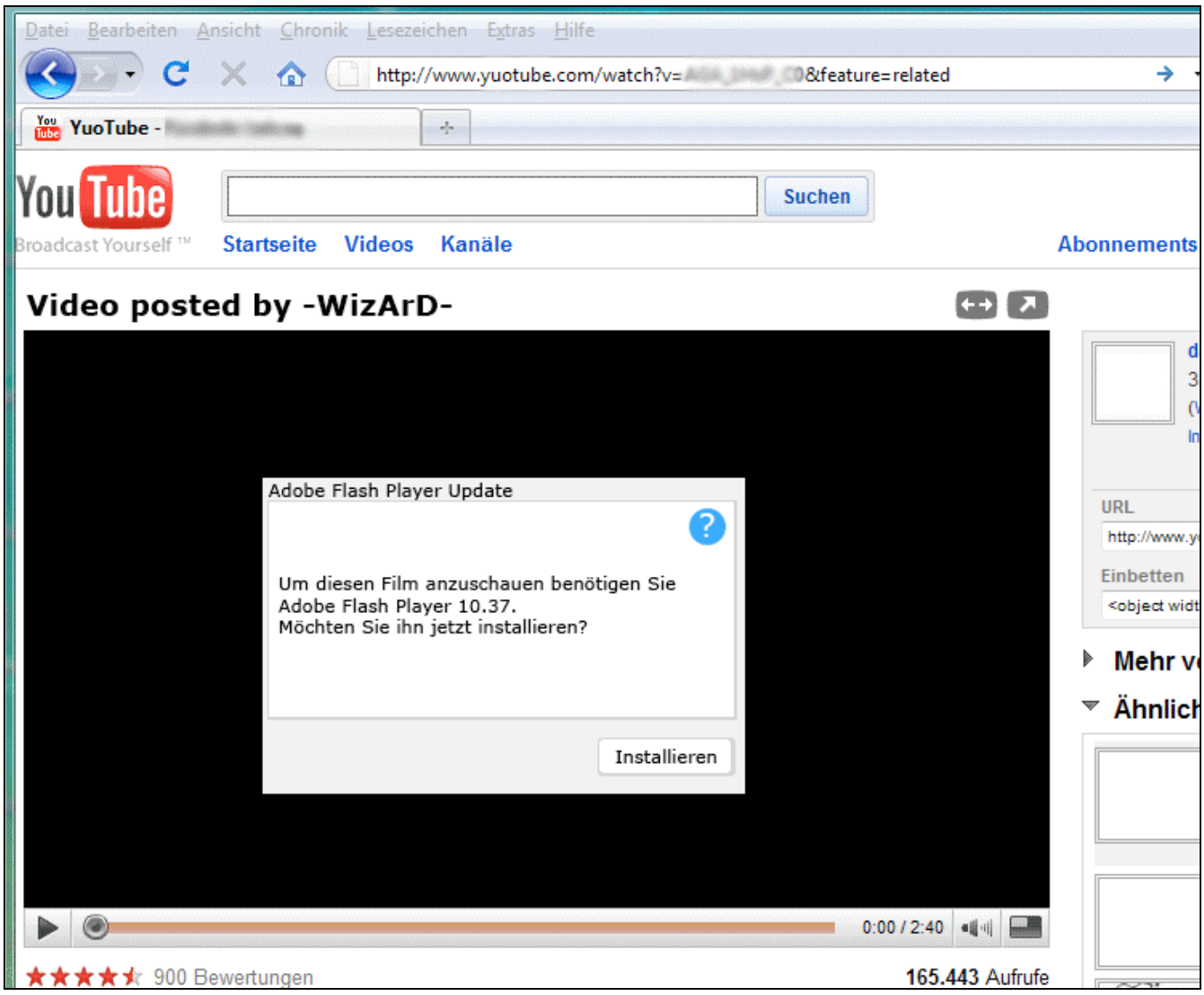
Tipps zur Erkennung gefährlicher Webseiten

Natürlich versucht ein Angreifer, seine Software möglichst unentdeckt auf die Computer seiner Opfer zu bringen. Oft ist es für ihn aber einfacher, wenn er uns "überzeugen" kann, dass wir dem Herunterladen der Software zustimmen oder das Herunterladen sogar selbst aktiv durchführen. Ein Angreifer wendet dabei Techniken aus dem Gebiet des *Social Engineering* an, indem er versucht, uns zu bestimmten Handlungen zu bringen. Die Strategien sind oft verhältnismässig einfache, wie *Einschüchtern* ("Ihr Computer ist

gefährdet/infiziert etc."), *Verwirren* (Fachbegriffe, die aber gar keinen Sinn ergeben), *Täuschen* (Angeblich fehlende Komponenten, ähnliche URLs etc.), *Beruhigen* (Angebliche Sicherheitszertifikate etc.) und *Gewöhnungseffekte* ("Schon wieder so eine Meldung..." etc.). Es folgen nun einige Szenarien, die darauf hinweisen könnten, dass Sie im Begriff sind, Ihren Computer zu infizieren.

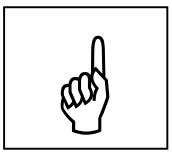
Installation fehlender Plugins

Beim Laden einer Seite wird Ihnen mitgeteilt, dass ein Plugin fehlt oder veraltet ist. Gleichzeitig werden Sie aufgefordert, das Plugin zu installieren.



Eine Webseite kann ziemlich einfach so gestaltet werden, dass sie einer "echten" Webseite täuschend ähnlich sieht. Dass Sie bei dieser Seite nicht auf *Installieren* klicken sollten, kann man anhand zweier Details merken. Erstens lautet die URL nicht *youtube.com* sondern *yuotube.com*. Angreifer locken Ihre Opfer gerne auf Webseiten, die fast gleich heissen, wie die echte. Das zweite Detail ist, dass Sie direkt aufgefordert werden, die Software zu installieren. Wenn eine seriöse Seite feststellt, dass auf Ihrem Computer ein Plugin fehlt oder veraltet ist, erhalten Sie einen Link auf die Webseite des

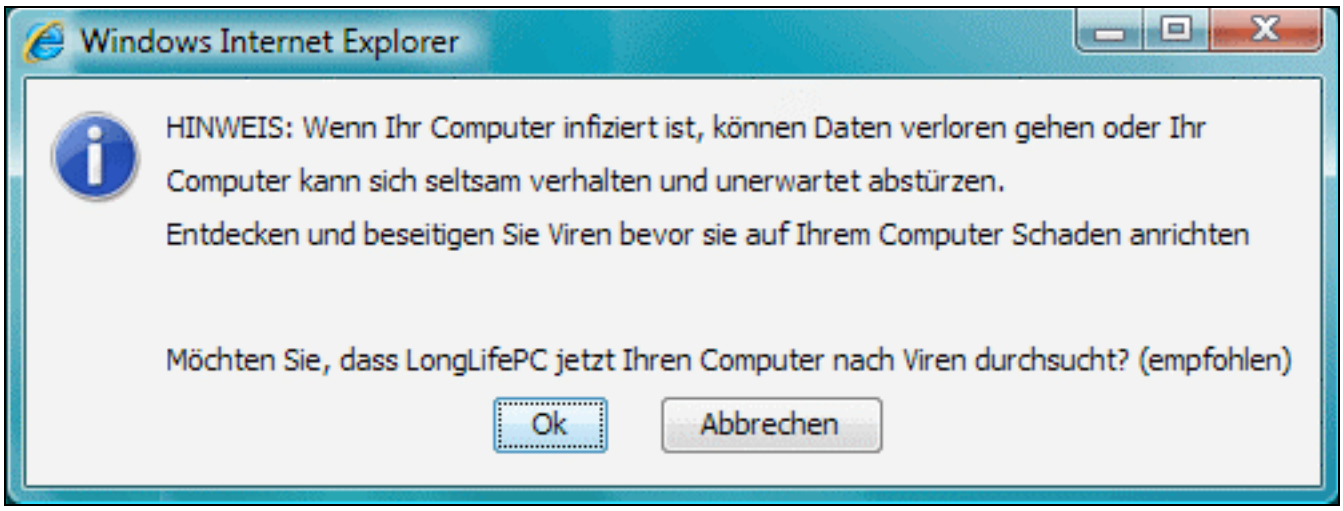
entsprechenden Herstellers. Dadurch müssen Sie zwar ein paar Klicks mehr ausführen, bis Sie das Plugin herunterladen können, Sie gehen dafür aber sicher, dass es auch echt ist.

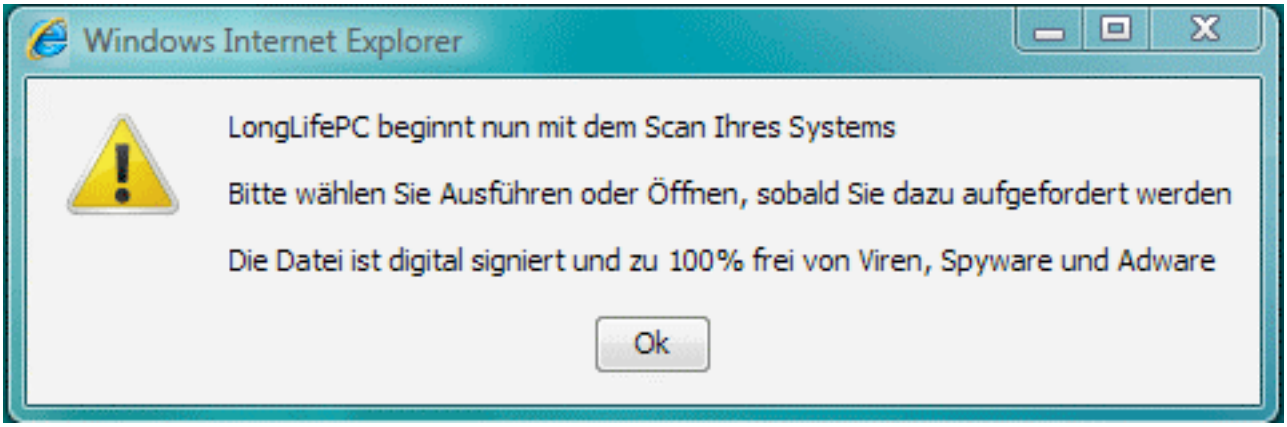


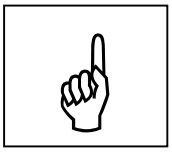
Generell ist es empfehlenswert, bei Meldungen über fehlende oder veraltete Plugins, zuerst zu kontrollieren, ob dies tatsächlich der Fall ist und wenn ja, direkt die URL des Herstellers einzugeben und so das Plugin herunter zu laden.

Seltsame (Viren-)meldungen

Wenn Sie eine (echte aber infizierte) Webseite laden, erscheint ein Dialog mit einer seltsamen Meldung, die Sie beispielsweise auffordert, Ihren Computer nach Viren zu durchsuchen und das auch gleich selbst tun will. Der Dialog kann Ihnen sogar die Auswahl geben, *Ok* oder *Abbrechen* zu wählen, aber das nützt Ihnen oft nichts, weil der "Scan" so oder so beginnt. Das Resultat des "Scans" ist natürlich, dass "Viren" gefunden werden und Sie werden aufgefordert, eine (fiktive) Antivirensoftware zu installieren. Installiert wird aber keine Antivirensoftware sondern ein bösartiges Programm.





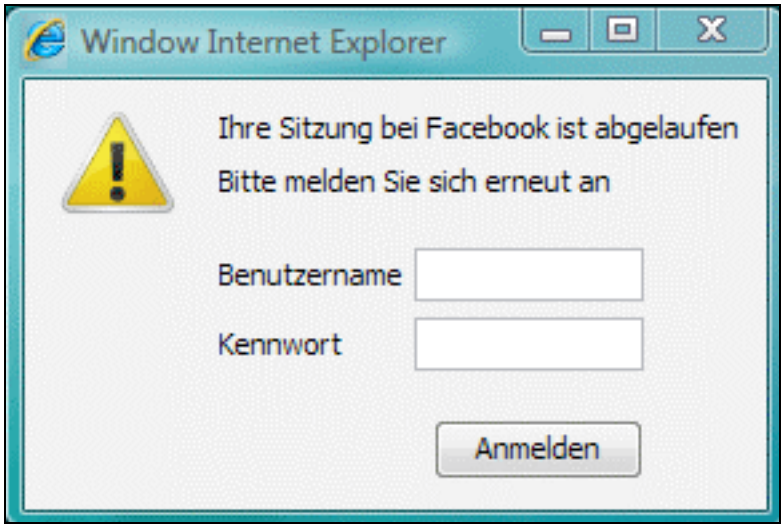


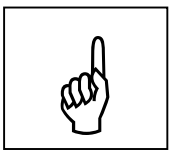
Heute gibt es viele Programme, die beim Start auf das Internet zugreifen und prüfen, ob ein Update vorhanden ist. Auch kann das Betriebssystem so eingestellt sein, dass periodisch Sicherheitswarnungen eingeblendet werden, die Sie beispielsweise auffordern, Ihren Computer zu überprüfen. Die meisten Benutzer haben sich an solche Mitteilungen gewöhnt und bestätigen

sie, ohne sie wirklich durchzulesen. Es empfiehlt sich auf alle Fälle, zu wissen, welches Programm die Meldung verursacht hat und welche Auswirkungen eine Bestätigung hat. Dies gilt insbesondere, wenn etwas aus dem Internet auf Ihren Computer geladen wird.

Unerwartete Aufforderung, sich Anzumelden

Bei einigen Webseiten, die eine Anmeldung erfordern, wird eine angemeldete Benutzerin nach einer gewissen Zeit der Inaktivität automatisch abgemeldet. Kehrt sie auf die Seite zurück, muss sie sich erneut anmelden. Wenn wir auf eine infizierte Webseite gelangen, ist es für einen Angreifer einfach, herauszufinden, ob wir kürzlich gewisse Seiten besucht haben, bei denen eine Anmeldung nötig ist, beispielsweise Facebook. Der Angreifer kann Ihnen dann eine falsche Webseite oder einen falschen Warnhinweis senden, etwa dass Sie sich erneut anmelden müssen, und so Ihre Zugangsdaten erfahren.

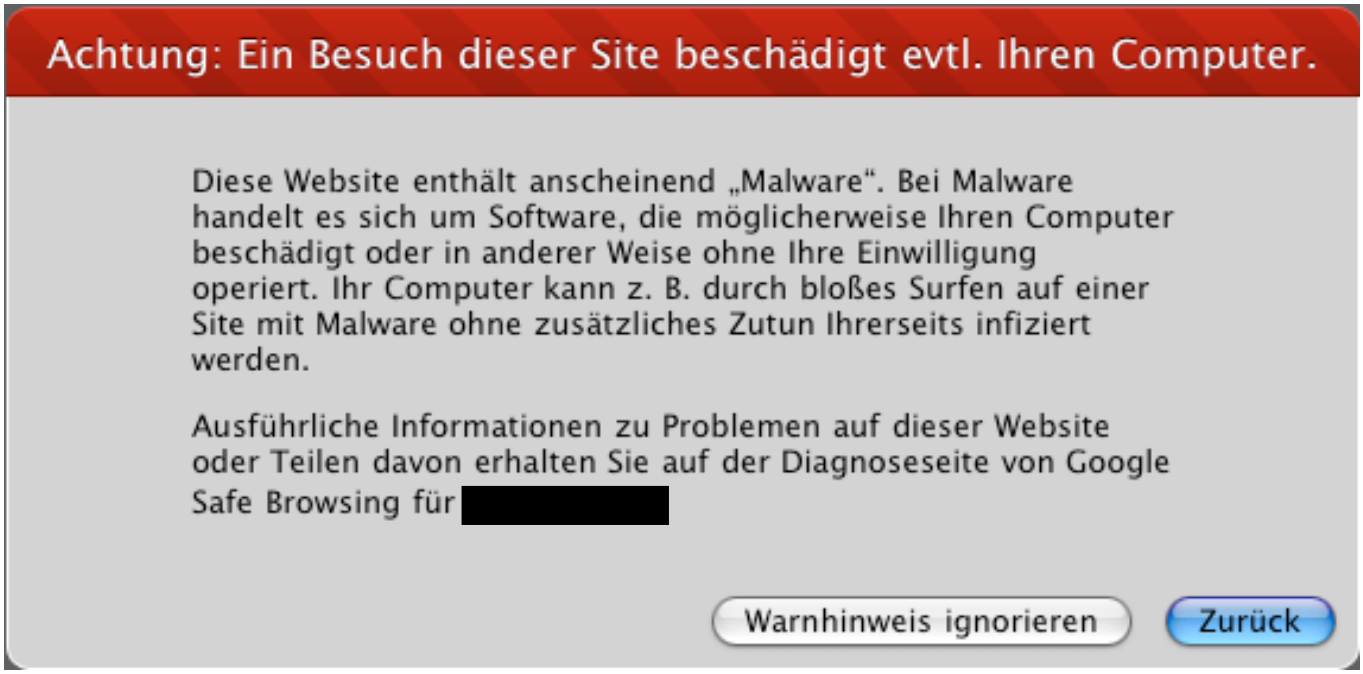




Hier empfiehlt es sich, die URL der Seite, die das erneute Anmelden verlangt, genau anzuschauen. Im Zweifelsfall lieber nicht anmelden sondern die echte URL eingeben und sich gegebenenfalls dort neu anmelden.

Warnungen des Browsers

Viele Browser stellen eine Einstellung zur Verfügung, die prüft, ob eine Webseite, die angezeigt werden soll, als bösartige Webseite bekannt und in einer entsprechenden “schwarzen Liste” aufgeführt ist.

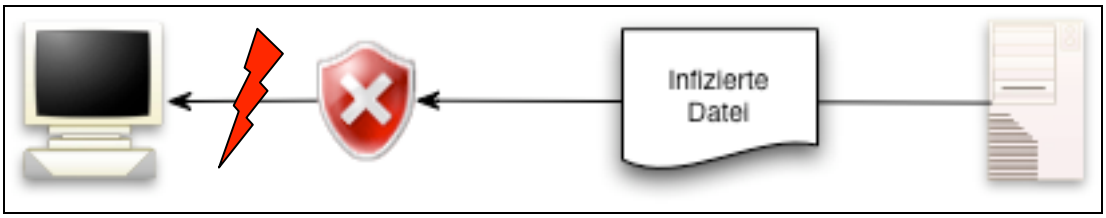


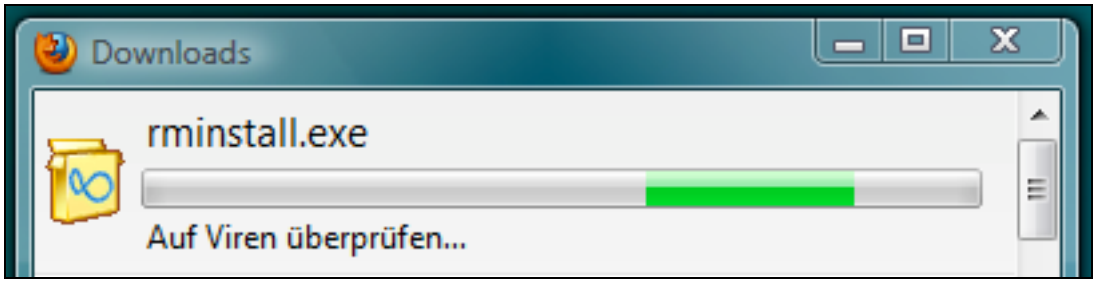
Was erkennt mein Antivirenprogramm?

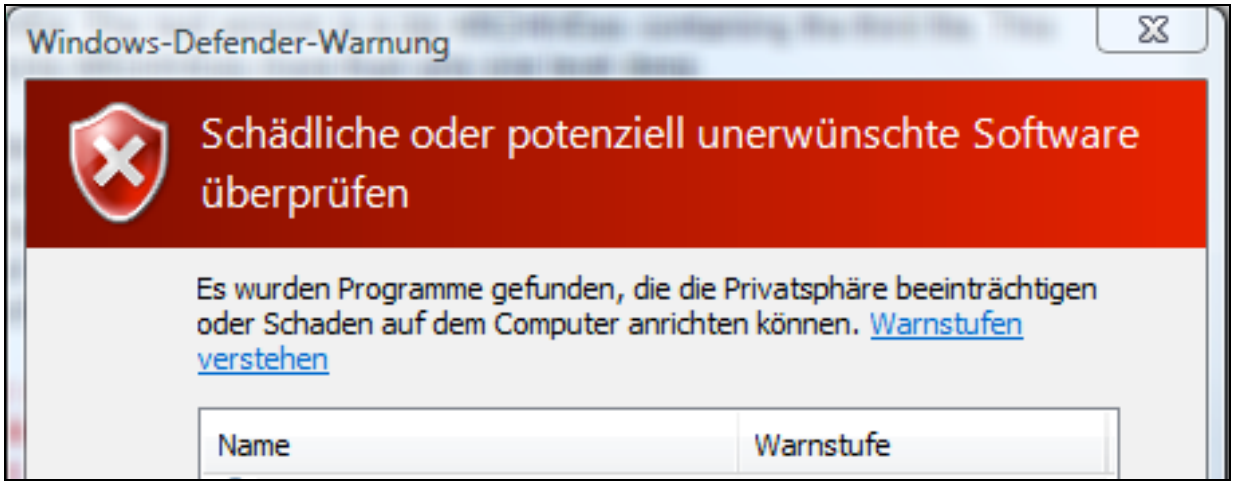
Es wäre natürlich beruhigend, wenn die Antwort auf diese Frage wäre: “Wenn ich mein Antivirenprogramm aktuell halte, ALLES.”. Leider ist das nicht so. Dafür gibt es technische und praktische Gründe.

Was ein Antivirenprogramm erkennen kann

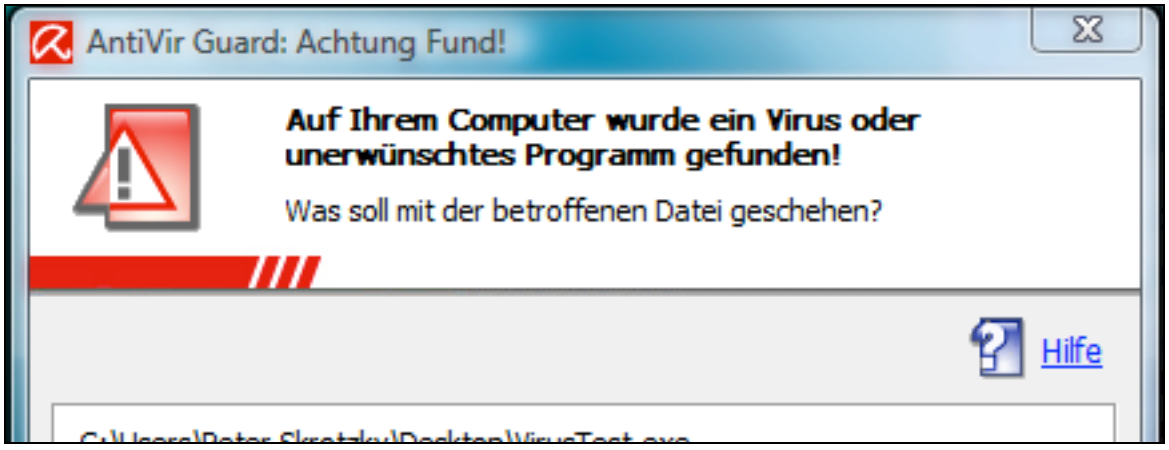
- Wenn wir beispielsweise mit unserem Browser versuchen, eine infizierte Datei herunter zu laden und unser Antivirenprogramm so eingestellt ist, dass es Downloads automatisch prüft.







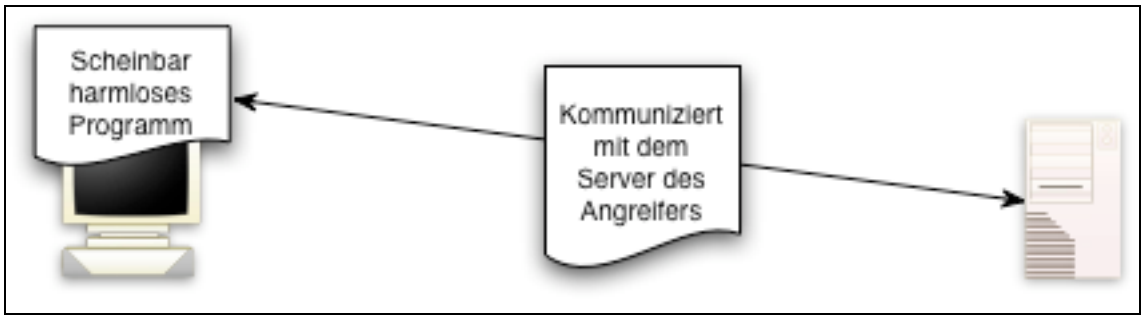
- Wenn ein (herunter geladenes) Programm versucht, eine bösartige ausführbare Datei, beispielsweise eine *.exe* Datei zu erzeugen.



Was ein Antivirenprogramm in der Regel nicht erkennt

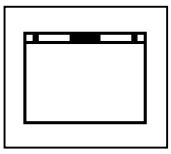
- Die meisten Benutzer konfigurieren ihre Antivirenprogramme so, dass nicht jede Datei, die auf dem Computer angelegt oder geändert wird, geprüft wird. Dies vor allem aus Gründen der Geschwindigkeit. Wenn ein Antivirenprogramm permanent alle Änderungen überprüfen würde, hätte das einen beträchtlichen Einfluss auf die Geschwindigkeit des Computers.

- Wenn ein herunter geladenes Programm selbst keinen bösartigen Code enthält, so gibt der Virenscanner keine Warnung aus. Ein Angreifer kann versuchen, diese Tatsache auszunützen. Er installiert ein “harmloses” Programm auf unserem Computer, das unbemerkt eine Internetverbindung zum Server des Angreifers herstellt. Das Programm kann nun beispielsweise versuchen, bösartige Software vom Server des Angreifers herunter zu laden.



Solche Programme sind oft schwierig zu entdecken, weil sie an sich nichts anderes tun als normale Programme, die aufs Internet zugreifen. Ein Antivirenprogramm kann erst eingreifen, wenn das Programm versucht, ausführbare Dateien zu erzeugen.

Praktische Übung



In dieser Übung mit der Simulationsumgebung sollen Sie erkennen, wie ein Angreifer Ihren infizierten Computer für seine Zwecke missbrauchen kann. Die Übung basiert auf einer real existierenden Malware, die 2009 unter dem Namen *Koobface* bekannt wurde und über soziale Netzwerke wie Facebook, MySpace, Twitter etc. verbreitet wurde. Sie arbeiten dazu in Zweiergruppen. Eine von Ihnen ist die Angreiferin, die andere das Opfer. Lesen Sie diesen Abschnitt und folgen Sie den Anweisungen.

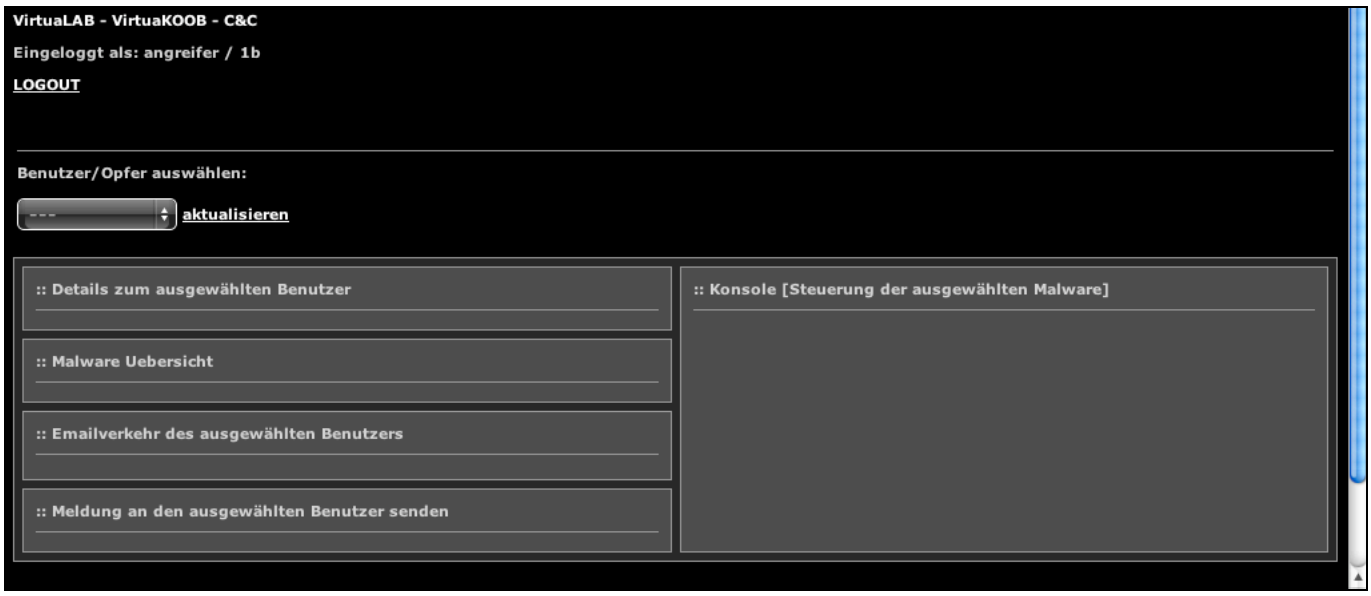
Ausgangslage

Das Opfer hat von einer infizierten Seite ein Programm namens *FlashPlayer Update.exe* herunter geladen. Das Programm gibt vor, dass es ein Update für den FlashPlayer installiert. Typischerweise könnte ein solches Programm auf zwei Arten auf Ihren Computer gelangen. Entweder erscheint in einer Webseite eine “Fehlermeldung”, dass ein Film nicht angezeigt werden konnte, mit der Aufforderung, das nötige Update durch einen Klick auf eine entsprechende Schaltfläche herunter zu laden, oder das Herunterladen findet automatisch im Hintergrund statt.
Das Programm selbst enthält keine eigentliche Malware, öffnet aber eine Verbindung zum Server des Angreifers, der dadurch nach Belieben verschiedene bösartige Software auf dem Computer platzieren kann.

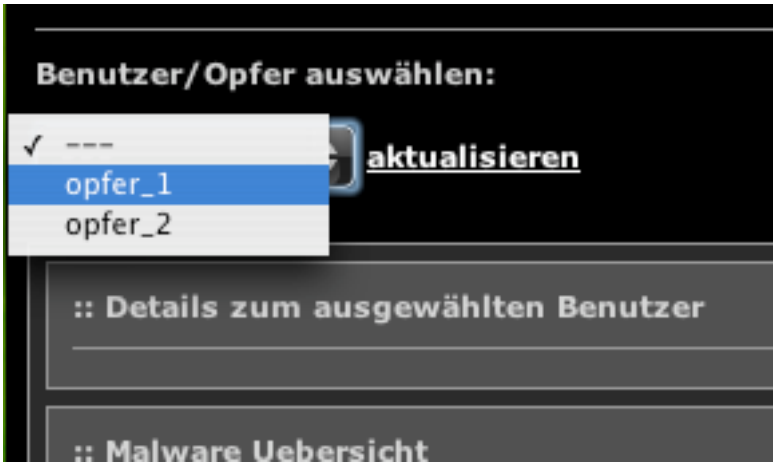
Wählen Sie nun, je nach Rolle als Opfer oder Angreifer, den entsprechenden Einstieg.

Der Bildschirm des Opfers

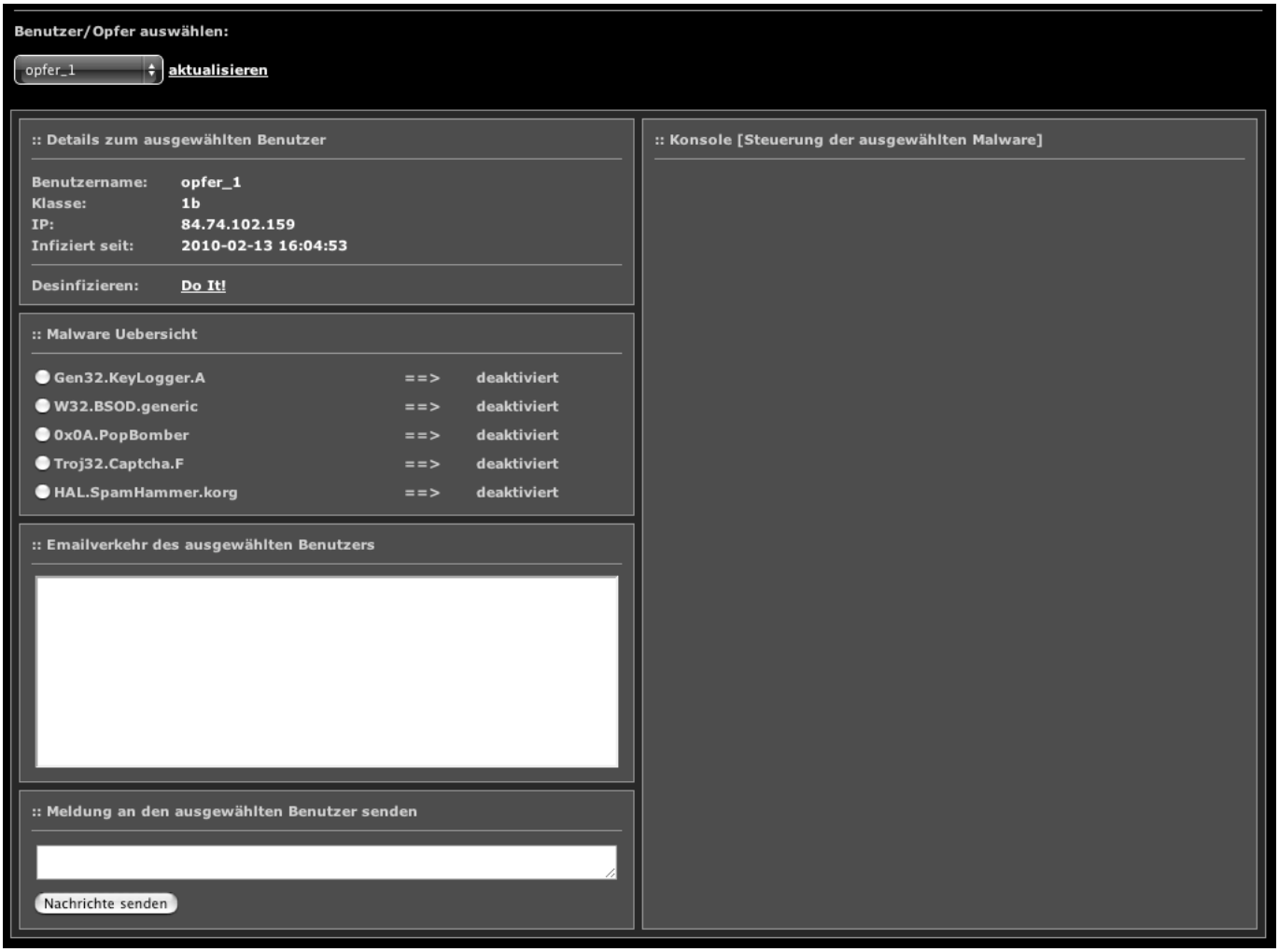
Der Bildschirm des Angreifers



Sobald ein Opfer das bösartige Programm gestartet hat, nimmt der Computer des Opfers mit dem Server des Angreifers Kontakt auf. Der Angreifer sieht in einer Liste die Computer, die er missbrauchen kann.



Er kann nun entscheiden, welche Malware er auf wie vielen und welchen Computern installieren möchte. In der Realität kann das so ablaufen, dass der Angreifer seinen (kriminellen) Kunden anbietet, gegen Geld gewisse Malware auf den Computern seiner Opfer zu platzieren. Das kann beispielsweise ein Programm sein, das Spam über das E-Mail Konto des Opfers verschickt. Natürlich kann der Angreifer die Identität eines Opfers auch benützen, um sein Programm an die Freunde des Opfers weiterzugeben und so noch mehr Computer infizieren.

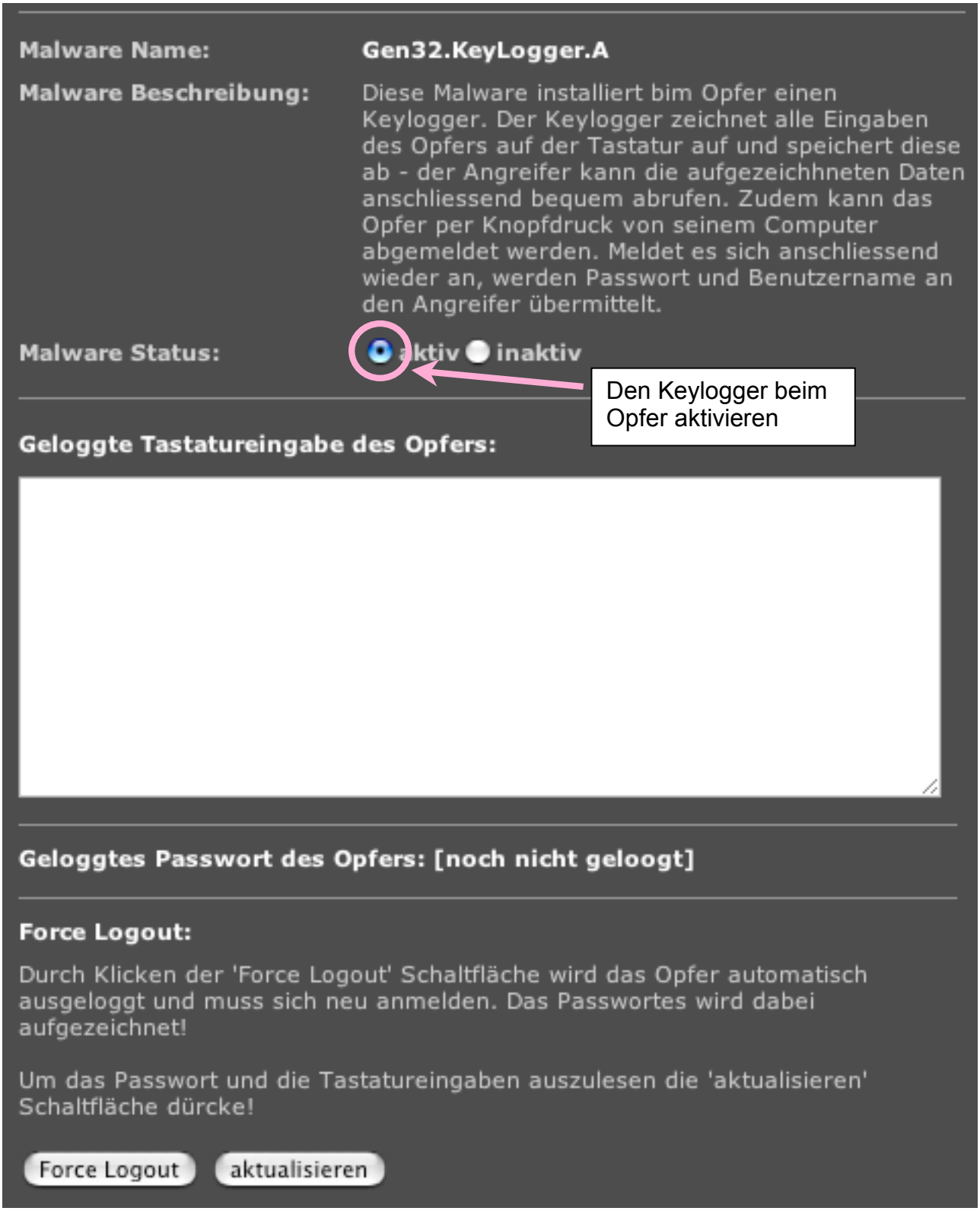


In der Simulation sind fünf Typen von Malware vorhanden, die Sie benützen können. In den folgenden Abschnitten werden diese Typen kurz erklärt. Lesen Sie die Erklärungen und probieren Sie die Malware aus. Beobachten Sie dabei, was auf den Computern des Opfers und des Angreifers geschieht. Achten Sie insbesondere darauf, welche Informationen der Angreifer erhält.

Gen32.KeyLogger.A

Keylogger sind Programme, die aufzeichnen, welche Tasten auf einem Computer gedrückt werden. Die Aufzeichnungen können entweder automatisch, oder wenn es der Angreifer will, an den Angreifer übermittelt werden. Ein Angreifer kann diese Daten nützen, um beispielsweise an Benutzernamen und Kennwörter des Opfers zu gelangen. Keylogger können auch so eingesetzt werden, dass sie ausser den Tasten, die gedrückt werden auch noch Screenshots übermitteln.

Beschliesst der Angreifer, auf dem Computer des Opfers einen Keylogger zu platzieren, so muss er in der Simulation den entsprechenden Eintrag auswählen und aktivieren. Mit einem Klick auf *aktualisieren* in der rechten unteren Ecke erhält der Angreifer die Tastenfolgen übermittelt, die das Opfer auf seinem Computer tippt. Ausserdem kann der Angreifer durch klicken auf *Force Logout* das Opfer von seinem Computer abmelden, und bei der Wiederanmeldung das Passwort aufzeichnen.



Um den Effekt der Malware zu erkennen, soll das Opfer den Editor starten und einen kurzen Text tippen.

W32.BSOD.generic

BSOD steht für "*Blue Screen of Death*". Eine solche Malware führt dazu, dass der Computer abstürzt oder ohne Zutun des Opfers herunterfährt. Das kann von einem Angreifer gezielt eingesetzt werden, beispielsweise weil ein Neustart des Computers des Opfers nötig ist, damit andere Malware eingesetzt werden kann. Es kann aber auch sein, dass die Malware einen Programmierfehler enthält, der zum Absturz führt.

0x0A.PopBomber

Diese Art Malware führt dazu, dass so genannte *Adware*, unerwünschte Werbebotschaften, auf dem Computer des Opfers erscheinen. Üblicherweise erscheinen diese Botschaften in unregelmässigen Abständen als Popup-Fenster.

Troj32.Captcha.F

Captcha werden die kleinen Bilder mit schwer lesbaren Zeichenfolgen genannt, die von vielen Websites bei der Registrierung und/oder Anmeldung verwendet werden, um zu verhindern, dass ein Angreifer den Anmelde- oder Registrierungsvorgang von einem Computerprogramm ausführen lassen kann.

Für einen Angreifer bieten soziale Netzwerke, gratis E-Mail Dienste, Foren und ähnliche Dienste eine ideale Ausgangsplattform, um bösartige Software zu verbreiten. Dazu muss er aber erst entsprechende Konten besitzen oder die Zugangsinformationen von existierenden Benutzern herausfinden respektive stehlen. Ein denkbares Szenario wäre, dass ein Angreifer die Zugangsinformationen eines Opfers kennt. Für seine Aktivitäten verwendet er ein Computerprogramm. Muss er beim Anmelden nicht nur Benutzernamen und Passwort des Opfers eingeben, sondern auch noch die (bei jedem Versuch andere) Zeichenfolge des angezeigten Captchas, so ergibt sich für den Angreifer ein Problem. Menschen haben keine Probleme, die angezeigte Zeichenfolge zu entziffern. Ein Computerprogramm allerdings tut sich damit schwer, weil Bilder vollkommen anders gespeichert werden als Texte.
Ein Angreifer hat nun zwei Möglichkeiten. Entweder er kann ein Programm benutzen, das versucht, die Zeichen eines Captchas zu entziffern – was allerdings vielfach nicht so erfolgreich ist – oder er schickt das Captcha an von ihm kontrollierte Computer und lässt es von deren Benutzerinnen lösen. Genau das macht die in der Simulation vorgestellte

Malware. Typischerweise funktionieren diese *Captcha Breaker* so, dass das Opfer auf seinem Computer nicht weiter arbeiten kann, bis es den Text eingegeben hat.

HAL.SpamHammer.korg

Diese Malware ist ein Beispiel dafür, wie der Computer eines Opfers von einem Angreifer für seine Zwecke missbraucht werden kann. In unserem Fall kann der Angreifer vom Computer des Opfers unter dessen Namen E-Mails an beliebige Personen schicken. Somit wird das E-Mail Konto des Opfers zu einer Quelle von Spam Nachrichten. In der Realität infiziert ein Angreifer zunächst Tausende von Computern mit seiner Malware und lässt diese anschliessend gemeinsam für sich arbeiten. Dabei kann er seine Opfer nicht nur für das Versenden von Spam benützen, sondern sie auch dazu einsetzen, gezielte Angriffe gegen Organisationen zu führen, indem er beispielsweise gleichzeitig hunderttausende von E-Mails an einen bestimmten Mailserver schickt und diesen so lahmlegt.

Koobface – ein Beispiel für eine Malware

Koobface ist eine Malware, die erstmals im Dezember 2008 entdeckt wurde und ein so genanntes Botnet, eine Menge von infizierten Computern, die von einem Kontrollrechner des Angreifers gesteuert werden, aufbaut. Eine Besonderheit an dieser Malware ist, dass sich Koobface über soziale Netzwerke wie Facebook oder MySpace verbreitet. Ausserdem besteht Koobface aus verschiedenen Komponenten, die dem Angreifer eine grosse Flexibilität bezüglich der bösartigen Programme, die er auf den Computern seiner Opfer platzieren will, bieten. Wir werfen im Folgenden einen Blick darauf, wie sich Koobface verbreitet und welchen Schaden er anrichten kann.

Die Infizierung – Download Komponente

Eine typische Infizierung beginnt mit einer harmlos wirkenden Statusmeldung in Facebook, MySpace, Twitter oder anderen sozialen Netzwerken. Anstelle einer Statusmeldung kann auch eine Nachricht in der Inbox eines Benutzers erscheinen. Die Nachricht enthält einen Link, der auf ein Video verweist. Durch einen Klick auf den Link gelangt die Benutzerin auf eine Webseite, die gleich aufgebaut ist wie YouTube. Anstelle eines Films erscheint eine Meldung, dass die Benutzerin eine bestimmte Version des Flash-Players installieren muss, um den Film zu sehen und die Benutzerin wird aufgefordert, die Software herunter zu laden. Die *.exe* Datei, die herunter geladen wird, ist nicht die eigentliche Malware, sondern vielmehr ein Downloader, der mit dem Koobface Kontrollzentrum Verbindung aufnimmt. Anhand der Cookies, die er auf dem Computer der Benutzerin findet, teilt er dem Kontrollzentrum mit, bei welchen sozialen Netzwerken sie Mitglied ist, und lädt diejenigen Komponenten herunter, die ihm das Kontrollzentrum mitteilt.

Die Weiterverbreitungskomponenten

Diese Komponenten kann man als Koobface-Wurm bezeichnen. Koobface kennt rund ein Dutzend verschiedene soziale Netzwerke, darunter auch Facebook und MySpace. Die

Weiterverbreitungskomponenten verschicken Meldungen an die Freunde im sozialen Netzwerk der Benutzerin, die den Link auf die gefälschte Webseite enthalten.

Die Webserverkomponente

Diese Komponente verwandelt den Computer der Benutzerin ohne deren Wissen in einen Webserver. Das Koobface Kontrollzentrum kann den Computer nun als Quelle für das Herunterladen von Komponenten oder als Server für die gefälschte Webseite einsetzen.

Die Werbe- und gefälschte Antiviren-Komponente

Diese Komponente führt dazu, dass auf dem Computer der Benutzerin Browserfenster mit unerwünschter Werbung oder irreführenden Warnhinweisen geöffnet werden und dass eine bösartige Antivirensoftware installiert wird.

Captcha-Breaker-Komponente

Diese Komponente fordert die Benutzerin auf, ein Captcha zu lösen. Dabei erscheint das Captcha auf dem Bildschirm der Benutzerin zusammen mit einem Countdown, der vorgibt, den Computer nach 3 Minuten auszuschalten, falls das Captcha nicht beantwortet wird. Die Antwort wird an das Kontrollzentrum weitergeleitet.

Daten Diebstahl-Komponente

Diese Komponente ist eine Variante eines bekannten Trojaners, der verschiedene Informationen, beispielsweise E-Mail Identitäten, auf dem Computer der Benutzerin sucht und verschlüsselt an das Kontrollzentrum übermittelt.

Suchmaschinen Entführer

Diese Komponente fängt Suchanfragen der Benutzerin an *Google*, *Yahoo* und andere ab und leitet sie an andere zwielichtige Suchmaschinen um. Diese liefern nur Resultate von dubiosen Webseiten.

Ändern des DNS Servers

Diese Komponente ändert auf dem Computer der Benutzerin den Eintrag des DNS Servers, sodass die Benutzerin nicht auf die gewünschten Webseiten gelangt, sondern auf bösartige. Auch kann es sein, dass die Benutzerin nicht mehr auf gewisse Seiten von Herstellern von Antivirenprogrammen zugreifen kann.

Kontrollfragen

1) Beim Aufrufen einer Webseite erscheint eine Meldung, dass die Webseite nicht vollständig angezeigt werden kann, weil auf Ihrem Computer zuerst eine entsprechende Softwarekomponente installiert werden muss. Wie reagieren Sie? Begründen Sie Ihre Antwort.

2) Welches Ziel verfolgt ein Angreifer mit Social Engineering?

3) Weil ich kein Geld für teure Software habe, suche ich Webseiten, die gratis Programme anbieten und lade die Software von dort herunter. Dabei achte ich darauf, dass wirklich nur die Software installiert wird, die ich herunter geladen habe. Wie beurteilen Sie dieses Vorgehen?

4) Wenn ich mich bei einer Webseite registrieren/anmelden muss, mache ich das nur, wenn die entsprechende Seite die Daten verschlüsselt überträgt. Das heisst, ich mache das nur, wenn die URL in der Eingabezeile mit "*https://*" beginnt. Würden Sie dieses Vorgehen unterstützen? Begründen Sie.

5 – WWW Teil 2

Lernziele

- Sie können einschätzen, welche Angebote im Internet für einen Besucher ungewünschte Folgen haben können
- Sie wissen, wann ein Passwort als sicher gilt
- Sie wissen, welche Spuren Sie im Internet hinterlassen

Im vorherigen Kapitel haben Sie gesehen, dass Angreifer vielfach versuchen, uns so zu täuschen, dass wir selbst mithelfen, unseren Computer mit bösartiger Software zu infizieren. In diesem Kapitel geht es darum, Ihnen einige Beispiele aufzuzeigen, welche anderen Möglichkeiten für Dritte bestehen, um an unser Geld oder Informationen über uns zu gelangen.

Ungewollte Abonnemente

Im Internet gibt es viele Seiten mit Gratisangeboten. Das Spektrum reicht von kostenloser Software über Online-Spiele bis zu IQ- oder Partnerschaftstests. Einige dieser Angebote erweisen sich bei genauerem Hinsehen jedoch als kostenpflichtig. Anhand zweier Beispiele soll das Vorgehen der Betreiber solcher Webseiten aufgezeigt werden.

“Kostenlose” Software

Abgesehen von zeitlich limitierten Testversionen kann man grob zwei Arten von kostenlos angebotener Software unterscheiden. Verschiedene Softwareentwickler bieten kleine Programme an, welche Dateien, die mit ihrer Software erstellt wurden, anzeigen können. Als Beispiele seien hier der *Flash Player*, der *Real Player* oder der *Acrobat Reader* erwähnt. Andererseits gibt es viele Programme, deren Verwendung explizit kostenlos ist, beispielsweise die OpenSource Projekte *OpenOffice* oder *Gimp*.

Findige Betreiber sammeln solche Gratisangebote auf ihren Webseiten und bieten sie dort zum Herunterladen an. Allerdings bieten sie die Software nicht mehr gratis an, sondern verlangen eine Gebühr, meist in Form eines Abonnements. Wofür diese Gebühr erhoben wird, ist meist nicht ganz klar. Auch die Information, dass überhaupt eine Gebühr erhoben wird, ist bei einzelnen solcher Webseiten für Kunden oft schlecht ersichtlich. Der Aufbau der Webseiten ist in der Regel so, dass ein Besucher aufgefordert wird, sich unter Angabe detaillierter persönlicher Informationen zu registrieren, bevor er die gewünschten Programme herunter laden kann. Dass er mit der Registrierung auch gleich ein kostenpflichtiges Abonnement löst, wird oft nur irgendwo klein auf der Webseite oder erst am Schluss langer allgemeiner Geschäftsbedingungen erwähnt.

Beachten Sie, dass man bei der Registrierung keine Angaben zu einer Kreditkarte oder sonstigen Zahlungsangaben machen muss. Dadurch wird das Gefühl verstärkt, dass es sich um ein kostenloses Angebot handelt.

Wenn man etwas weiter nach unten scrollt, erscheint links unten der Hinweis auf die anfallenden Gebühren:

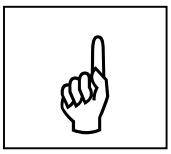
Füllt man die Registrierung aus, so erhält man wenig später eine E-Mail mit der Aufforderung, die Gebühr auf ein bestimmtes Konto einzuzahlen. Wird der geforderte Betrag nicht unverzüglich bezahlt, so erhält die Benutzerin nach wenigen Tagen weitere E-Mails, deren Ton deutlich schärfer ist. Damit soll die Benutzerin verunsichert werden.

Text gelöscht

Mit Zugang dieser Mahnung befinden Sie sich gem. §§ 286ff. BGB im Verzug.
Uns steht damit die sofortige Erhebung einer Leistungsklage oder alternativ die Beantragung eines Mahnbescheides und die damit einhergehende Eröffnung eines Mahnverfahrens durch unsere Rechtsanwälte zu.

Text gelöscht

Es gibt zwei Handlungsweisen, wie Sie verhindern können, in solche Fallen zu tappen. Viele kostenlose Programme können entweder bei der Homepage des Herstellers oder über eine eigens für die Software konzipierte Webseite herunter geladen werden, beispielsweise der *Flash Player* über die Webseite von Adobe oder *OpenOffice* über *openoffice.org*. Ausserdem gibt es anerkannte Webseiten von denen OpenSource Programme herunter geladen werden können.



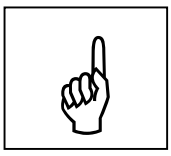
Wenn Sie detaillierte persönliche Angaben zur Registrierung angeben müssen, also beispielsweise Adresse, Wohnort, Telefonnummer oder gar Kreditkartennummer, ist das ein eindeutiges Zeichen, für eine Abonnements-Falle. Dagegen ist es nicht ungewöhnlich, für den Download eine in der Regel freiwillige Angabe einer E-Mail Adresse machen zu müssen.

“Gratis” Spiele, Tests etc.

Viele Menschen nutzen das Internet auch zum Vergnügen. Es gibt zahlreiche Webseiten, welche dies kommerziell zu nutzen versuchen. Dass dabei Gebühren erhoben weden, ist für die Benutzer nicht immer (leicht) ersichtlich.
Im folgenden Beispiel sieht man im Kleingedruckten, dass ein Benutzer ein Abo löst, welches 15 Franken pro Woche kostet und 5 Downloads pro Woche umfasst. Um welche Art von Downloads es sich dabei handelt, wird nicht weiter erklärt. Der angebotene IQ-Test erscheint ebenfalls dubios.

Beantwortet man die zehn Fragen, so gelangt man an die Stelle, an der das Abo gelöst werden muss.

Immerhin ist es bei dieser Seite so, dass der Benutzer mit einem Klick auf das entsprechende Kästchen die Geschäftsbedingungen und die anfallenden Kosten explizit akzeptieren muss.



Beachten Sie, dass die Kosten über das Handy des Benutzers abgerechnet werden. Dies zeigt, dass es die Betreiber dieser Webseite vor allem auf Jugendliche abgesehen haben, die noch keine Kreditkarte besitzen. Dieser Eindruck wird durch die Hinweise im Kleingedruckten noch verstärkt.

Ist das legal?

Betreiber solcher Websites bewegen sich hart an der Grenze des Erlaubten. Im Wesentlichen geht es dem Gesetzgeber um die Frage, ob die Hinweise, dass für den Benutzer Kosten entstehen, klar genug erkennbar sind. In den beiden erwähnten Beispielen dürfte der Hinweis beim IQ Test dieses Kriterium erfüllen, während es beim Software Download weniger klar ist. Dies insbesondere auch deshalb, weil der Hinweis auf die Kosten bei handelsüblichen Bildschirmgrössen erst sichtbar wird, wenn man bis ans Ende der Seite scrollt.

Passwörter und Authentifizierung

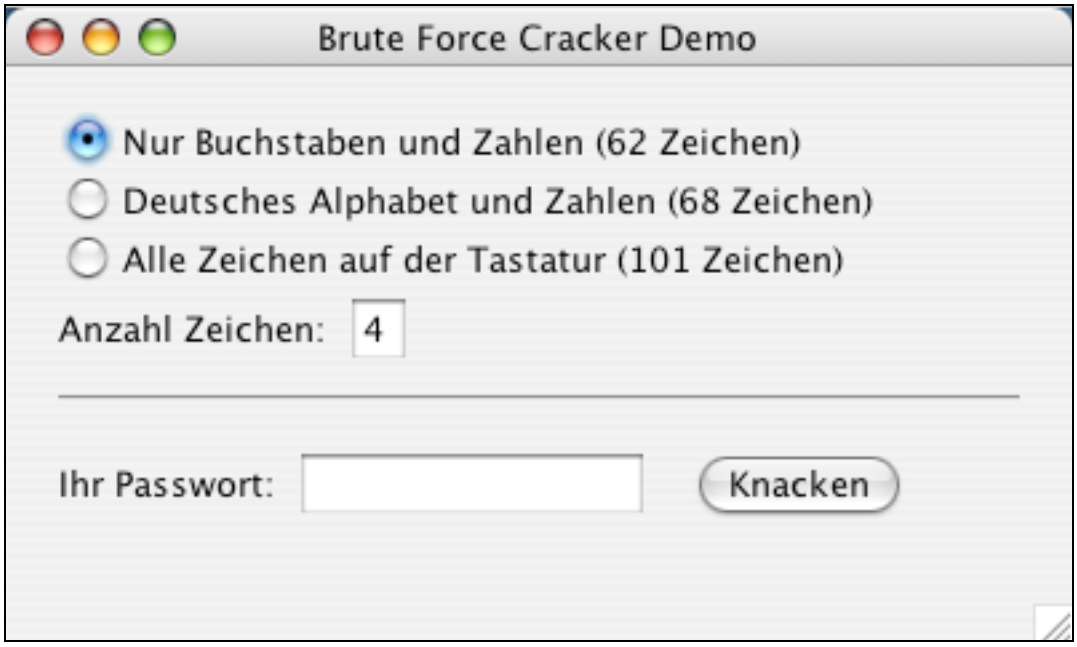
Nutzt man den Computer und das Internet häufig, so wächst die Zahl der Orte, an denen man sich registrieren muss, rasch an. Das beginnt beim eigenen Computer und geht bis zu E-Mail Konten, sozialen Netzwerken, Online-Shops etc. Seriöse Betreiber von Webseiten achten darauf, dass die Übermittlung der Benutzerdaten verschlüsselt geschieht und die Daten sicher aufbewahrt werden. Diese Vorsichtsmassnahmen nützen allerdings nur etwas, wenn ein Benutzer auch sorgfältig mit seinen Passwörtern umgeht. Dazu gehören die folgenden, teils offensichtlichen, Verhaltensgrundsätze:

- Passwörter vertraulich behandeln und nicht weitergeben.
- Wenn Sie Computer benützen, die auch anderen Personen zugänglich sind, achten Sie darauf, dass Sie sich beim Verlassen des Computers abmelden oder einen Passwort geschützten Bildschirmschoner einschalten.
- Speichern Sie Passwörter nicht auf dem Computer, schon gar nicht in einer Datei mit dem Namen *Passwörter*.
- Schreiben Sie die Passwörter nicht auf. Am besten ist es, sich die Passwörter auswendig zu merken. wenn das nicht möglich ist, notieren Sie sich eine Gedankenstütze, die für einen Dritten nichtssagend ist.
- Ändern Sie Ihre Passwörter regelmässig.
- Verwenden Sie genügend lange (mindestens 8 - 10 Zeichen) Passwörter.
- Verwenden Sie Passwörter, die nicht leicht zu erraten sind.
- Verwenden Sie nicht überall dasselbe Passwort.

Warum die letzten drei Punkte wichtig sind, wird im Folgenden kurz erläutert.

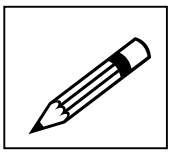
Länge der Passwörter

Wenn wir in einem Passwort alle Buchstaben (a bis z, A bis Z), Ziffern (0 bis 9), Umlaute (ä, ö, ü, Ä, Ö, Ü) sowie Satzzeichen und weitere Zeichen, die wir auf der Tastatur finden, zulassen, so erhält man eine Auswahl aus ungefähr 100 Zeichen (manchmal werden nur Buchstaben, Zahlen und wenige Sonderzeichen wie Bindestrich oder Unterstrich erlaubt). Für jede Stelle eines Passworts stehen somit ca. 100 Zeichen zur Auswahl. Für ein vierstelliges Passwort ergeben sich somit $100 \cdot 100 \cdot 100 \cdot 100 = 100000000 = 10^8$, also 100 Millionen, Möglichkeiten. Ein Computer braucht wenige Sekunden, um alle diese Möglichkeiten auszuprobieren. Weil hinter diesem Vorgehen keine grossen Überlegungen stecken, sondern einfach alle Möglichkeiten ausprobiert werden, bis eine passt, nennt man es auch *Brute-Force* (*Rohe Gewalt*) Methode.
Es steht ein Java Programm zur Verfügung, mit dem man ausprobieren kann, wie rasch ein Passwort mit der Brute-Force Methode geknackt werden kann.



Leicht zu erratende Passwörter

Ein leicht zu erratendes Passwort meint nicht, dass jemand Sie oder Ihr Umfeld kennt und so auf mögliche Passwörter schliessen könnte. Es geht vielmehr um Passwörter, die gewissen Gesetzmässigkeiten folgen, beispielsweise Wörter, Namen, Geburtsdaten, Buchstaben und Zahlen, die auf der Tastatur nebeneinander liegen und so weiter. Im Duden der deutschen Rechtschreibung gibt es ungefähr 135'000 Stichwörter – Kein Problem für einen Computer, diese alle auszuprobieren.



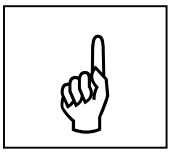
Die Kombination "*qwerpoiu*" scheint auf den ersten Blick ziemlich zufällig gewählt. Warum ist dieses Passwort aber alles andere als sicher?

Auch die Idee, gewisse Buchstaben durch ähnlich aussehende Zahlen zu ersetzen, beispielsweise "*Internet*" durch "*In73rn37*", macht ein Passwort nicht sicherer. Ein Angreifer kann sich eine Liste von solchen Passwörtern zusammenstellen (oder im Internet zusammensuchen...) und so versuchen, ein Passwort zu knacken. Weil er dabei nicht wie bei der Brute-Force Methode einfach alle Möglichkeiten ausprobiert, sondern eine Liste (sozusagen ein Wörterbuch häufiger Passwörter) abarbeitet, nennt man dieses Vorgehen auch *Dictionary* (*Wörterbuch*) Methode.

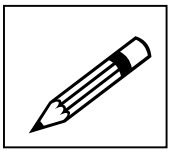
Verschiedene Orte – verschiedene Passwörter

Idealerweise benutzen Sie überall wo Sie sich registrieren müssen ein anderes Passwort und falls möglich sogar einen anderen Benutzernamen. Betreiber von interaktiven Webseiten, die viele Benutzer haben, sind auch ein begehrtes Ziel von Angreifern. Auch können Sie nicht ausschliessen, dass ein Mitarbeiter des Betreibers die Daten missbraucht. Verwenden Sie überall dasselbe Passwort, so ermöglichen Sie einem Angreifer, auf alle Ihre Benutzerkonten zuzugreifen.

In der heutigen Zeit greifen viele Benutzerinnen auf mehrere Internetseiten zu, die eine Registrierung verlangen. Dabei kann es schwierig werden, sich alle Passwörter zu merken. Man sollte aber mindestens so vorgehen, dass man für verschiedene Kategorien andere Passwörter verwendet, beispielsweise eines, um sich am eigenen Computer anzumelden, eines für E-Mail Konten und wieder ein anderes für Facebook.



Wie findet man nun ein Passwort, das leicht zu merken ist, aber auch sicher ist? Eine oft empfohlene Methode ist, die Anfangsbuchstaben eines Satzes, den man sich leicht merken kann, zu verwenden. Das Passwort "mkSNi5Jjai" kann als ziemlich sicher angeschaut werden (es enthält keine Sonderzeichen, was es noch sicherer machen würde). Weil es sich aus den Anfangsbuchstaben des Satzes "*meine kleine Schwester Nicole ist 5 Jahre jünger als ich*" ergibt, kann man es sich auch leicht merken.



Finden Sie einen Satz, den Sie sich leicht merken können und der sich als Passwort eignen würde.

Spuren im Internet

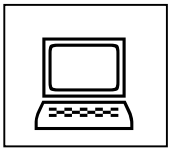
Wenn wir uns im Internet bewegen, so hinterlassen wir bewusst oder unbewusst Spuren. Abgesehen vom Datenschutz sind diese Spuren auch gefährlich, weil sie von einem Angreifer ausgewertet werden können. Die Orte, an denen wir Spuren hinterlassen, können grob in drei Kategorien unterschieden werden.

- Spuren auf unserem Computer. Cookies, kleine Einträge, die Webserver auf unserem Computer hinterlegen, wurde bereits im vorangehenden Kapitel erwähnt. Weiter versucht unser Browser, wenn wir eine Webseite aufrufen, eine Kopie dieser Seite auf unserem Computer zu speichern. Diese temporären Internetdateien werden im Fachjargon *Cache* genannt. Ausserdem kann sich unser Computer merken, welche Webseiten wir kürzlich besucht haben (*Verlauf* oder *Chronik* genannt) oder was wir bei Formularen eingegeben haben.
- Spuren zwischen unserem Computer und den Servern, auf deren Seiten wir zugreifen. Für jede Webseite, die wir aufrufen, muss unser Computer mit dem entsprechenden Server Kontakt aufnehmen. Dazwischen passieren die übermittelten Daten mehrere Netzwerkkomponenten, von denen einige, mindestens theoretisch, aufzeichnen können, welcher Computer welche Webseiten auf welchem Server abruft.
- Spuren auf den Servern der Webseiten, die wir aufrufen.

Temporäre Internetdateien und Verläufe

Dass ein Browser versucht, eine Kopie der Webseiten oder Teilen davon auf unserem Computer zu speichern (*Temporäre Internetdateien*, *Internet Cache*), hat im Wesentlichen zwei Gründe. Wenn eine Benutzerin eine Seite oft aufruft und diese Seite zwischen den

Aufrufen nicht verändert wurde, kann Zeit gespart werden, wenn die Seite nicht erneut vom Server geladen werden muss. Das ist insbesondere dann nützlich, wenn auf einer Seite speicherintensive Daten vorhanden sind (Bilder, Filme etc.). Der zweite Grund ist, dass es so möglich ist, im Browser Webseiten anzuzeigen, auch wenn der Computer keine Netzwerkverbindung hat. Leider kann ein Browser nicht zwischen gutartigen und bösartigen Webseiten unterscheiden, sodass auch Kopien von bösartigen Webseiten auf unserem Computer gespeichert werden – es sei denn, unser Antivirenprogramm schützt uns davor.
Verläufe dienen dazu, dass wir kürzlich besuchte Webseiten rasch wieder finden. Der Browser speichert die Adressen dieser Seiten, und kann uns so beispielsweise Vorschläge beim Eintippen einer URL machen oder kürzlich besuchte Links innerhalb einer Webseite anders darstellen. Letzteres kann einem Angreifer Informationen über unser Surfverhalten liefern, indem er testet, ob eine bestimmte Webseite, beispielsweise Facebook, kürzlich von uns besucht wurde.



Schauen sie im Browser, den Sie üblicherweise verwenden, welche Webseiten im Verlauf gespeichert sind. Temporäre Internetdateien und Internet Caches sind nicht immer leicht zu finden. Viele Browser verwenden dazu einen versteckten Ordner im Verzeichnis des Benutzers. Im Internet Explorer können Sie die Temporären Internetdateien über *Extras-> Internetoptionen->Allgemein* im Abschnitt *Browserverlauf* mit Klicken auf Einstellungen und anschliessend auf *Dateien anzeigen*, sichtbar machen.

Der Weg zwischen unserem Computer und einem Server

Damit Daten von unserem Computer zu einem Server und umgekehrt gelangen, werden sie über mehrere Stationen weitergeleitet. Grundsätzlich kann jede dieser Stationen die Daten aufzeichnen und auswerten. So könnte Ihr Provider jederzeit verfolgen, welche Webseiten Sie aufrufen, er könnte Ihre E-Mails lesen und so weiter. Aus Gründen des Datenschutzes ist das jedoch nur auf richterliche Anordnung erlaubt. Allerdings kann ein Angreifer versuchen, sich in diese Kette von Stationen einzuklinken. Aus diesem Grund ist es sehr wichtig, dass persönliche Daten wie Passwörter oder Kreditkartennummern nur bei Webseiten eingegeben werden, die diese Informationen verschlüsselt übertragen.

Was Betreiber von Webseiten speichern können

Es gibt eine Webseite, die aufzeigt, was Betreiber einer Webseite alles über Ihren Computer herausfinden können (und das natürlich ohne dass Sie es merken). Gehen Sie auf die Webseite *http://browserspy.dk*. Auf der linken Seite sehen Sie eine Spalte, mit verschiedenen Stichwörtern, von denen die meisten Ihnen nicht viel sagen werden. Deshalb hier ein paar Vorschläge, welche Stichwörter sich anzuklicken lohnt.

- *Browser*: Es werden eine Reihe von Informationen über den Browser, den Sie verwenden, angezeigt.

- *CSS Exploit*: Es wird angezeigt, ob Sie in letzter Zeit einige bekanntere Webseiten besucht haben oder nicht.
- *IP Address*: Es wird sowohl die IP-Adresse, über die Sie im Netz erreichbar sind (in der Regel die Adresse Ihres Routers/Kabelmodems, als auch die Adresse Ihres Computers im lokalen Netz angezeigt. Aufgrund der IP-Adresse kann ausserdem die ungefähre geografische Lage Ihres Computers herausgefunden werden.
- *Plugins*: Eine Liste aller für Ihren Browser installierten Plugins wird angezeigt.
- *Active X (nur Internet Explorer auf Windows)*: Zeigt die auf Ihrem Computer installierten ActiveX Komponenten an
- *Components (nur Internet Explorer auf Windows)*: Zeigt weitere installierte Komponenten für Internet Explorer an
- *Fonts via Flash/Java*: Zeigt eine Liste der auf Ihrem Computer installierten Schriftarten an.
- *JavaScript*: Zeigt die von Ihrem Browser verwendete Version von JavaScript an.

Kontrollfragen

1) Sie stossen im Internet auf die abgebildete Seite. Sie würden den IQ Test gerne machen. Gehen Sie dabei unerwünschte Verpflichtungen ein?

2) Welche der folgenden Passwörter würden Sie als sicher erachten?
   - nItRaMrEiEm
   - 5Z=3.r4
   - iwi3.S,gdaK
   - &.rg:67?rKD

3) Um möglichst wenig Spuren auf Ihrem Computer zu hinterlassen, beschliessen Sie, die Einstellungen Ihres Browsers so zu ändern, dass keine Verläufe gespeichert werden und der Speicherplatz für temporäre Dateien auf 0 gesetzt ist. Ausserdem beschliessen Sie, jedes Mal bevor Sie den Browser verlassen, alle Cookies zu löschen. Welche Konsequenzen haben diese Massnahmen? Nennen Sie sowohl Vor- als auch Nachteile.

6 – Aktive Angriffe

Lernziele

- Sie können grob erklären, wie ein Angreifer in Ihren Computer eindringen kann.
- Sie können herausfinden, welche Ports auf Ihrem Computer offen sind.
- Sie wissen, warum der Einsatz einer Firewall Ihren Computer vor ungewollten Zugriffen schützt.

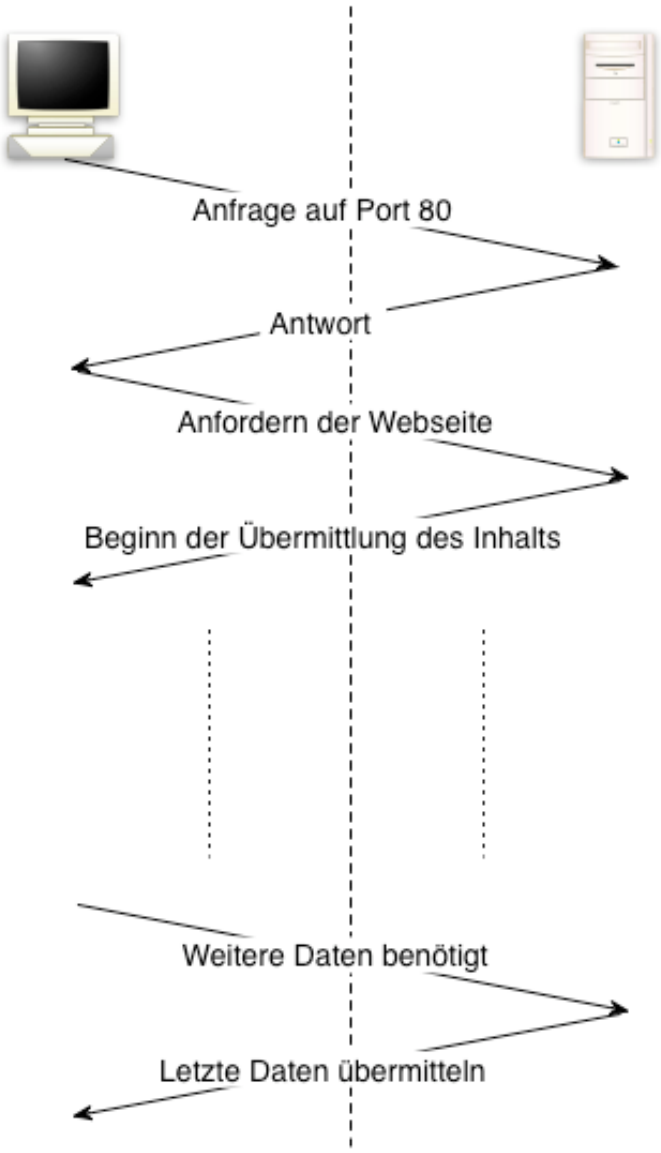
Antivirenprogramme schützen uns bis zu einem gewissen Grad davor, dass ungewünschte Software auf unseren Computer gelangt. Sie sind aber weitgehend nutzlos, wenn ein Angreifer dies gar nicht nötig hat, sondern von aussen auf unseren Computer zugreifen kann. In diesem Kapitel geht es darum, welche Möglichkeiten wir als Benutzer haben, solche Eingriffe zu verhindern oder wenigstens zu erschweren. Dabei wird davon ausgegangen, dass wir keinen eigenen Server betreiben. Dort kommt erschwerend hinzu, dass ein Server ja genau möchte, dass Aussenstehende auf ihn zugreifen können. Somit müssen dort zusätzliche Sicherheitsmassnahmen getroffen werden.

Kommunikation zwischen Computern

Wenn unser Computer mit einem anderen kommuniziert, so kann man grundsätzlich unterscheiden zwischen Informationen, die von unserem Computer an den anderen gesendet werden und solchen, die unser Computer empfängt. Informationen, die von unserem Computer an einen anderen verschickt werden, nennt man *ausgehende Verbindungen*, solche, die unser Computer empfängt *eingehende Verbindungen*. Ein wichtiger Punkt ist ausserdem, welcher Computer die Kommunikation beginnt.

Beispiel HTTP

Wenn sie in der Eingabezeile Ihres Browsers "*http://www.virtualab.ch*" eingeben, versucht Ihr Computer eine Verbindung zum Computer mit dem Namen *www.virtualab.ch* aufzubauen. Dazu schickt er eine Anfrage auf den Port 80 von *www.virtualab.ch*. Sofern dieser Computer tatsächlich ein Webserver ist, hört er diesen Port nach Anfragen ab und antwortet. Nun kann Ihr Computer die gewünschte Webseite anfordern. Dabei wird der Inhalt der Seite nicht als Ganzes übermittelt, sondern in kleine Pakete aufgeteilt. Hinzu kommt, dass Webseiten nicht unbedingt komplett auf einem Server gespeichert sein müssen. Somit muss sich Ihr Computer auch noch mit anderen Servern verbinden, bis er alle Teile der Webseite vollständig erhalten hat. Es herrscht also ein reger Verkehr von und zu Ihrem Computer.



Dieses Beispiel ist insofern typisch, als dass die Kommunikation von Ihrem Computer begonnen wird. Die eingehenden Verbindungen sind also Reaktionen auf ausgehende Verbindungen.

Wie unser Computer angegriffen werden kann

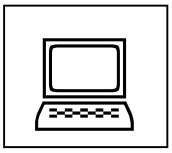
Damit jemand von aussen in unseren Computer eindringen kann, muss er unseren Computer zuerst einmal finden. Das bedeutet, dass er die IP-Adresse unseres Computers kennen muss. Kennt der Angreifer die Adresse, so versucht er als nächstes, eine offene Tür zu finden. Im Computerjargon ausgedrückt heisst das, er sucht nach offenen Ports. Im ersten Kapitel wurde bereits erklärt, was ein Port ist. Hier nochmals das Wichtigste in Kürze.
Computer bieten anderen ihre (Server-)Dienste an, indem ein entsprechendes Programm gestartet wird, das einen bestimmten Port abhört, ob ein Client mit ihm Verbindung aufnehmen will. Der vielleicht bekannteste Dienst ist der Webserver-Dienst, der in der Regel über den Port 80 angeboten wird. Viele Netzwerkspiele benützen ebenfalls bestimmte Ports, beispielsweise wird der Port 3724 von World Of Warcraft verwendet. Daneben gibt es aber auch Dienste, die weniger offensichtlich sind. Vielleicht haben Sie

an Ihrer Schule die Möglichkeit, Ihre Daten auf einem zentralen Server zu speichern. Dazu muss der Server einen entsprechenden Dienst anbieten und einen bestimmten Port abhören (welcher Port ist abhängig davon, wie Ihr Netzwerk aufgebaut ist). Vielleicht haben Sie Ihren Computer so eingestellt, dass Datum und genaue Uhrzeit über das Internet eingestellt werden. Dazu greift Ihr Computer auf einen entsprechenden Server zu, der über den Port 123 die aktuelle Uhrzeit mitteilt.
Wenn ein Angreifer auf unserem Computer einen offenen Port findet, so kann er versuchen, über diesen Port auf unseren Computer zu gelangen. Dazu nutzt er Fehler oder Sicherheitsmängel im Programm, das den Port abhört, aus.

Sie können nun natürlich argumentieren, dass Ihr Computer keine Serverdienste zur Verfügung stellt und deshalb gar keine Ports geöffnet sind. Das ist jedoch nicht der Fall. Wie wir feststellen können, ob hinter einer bestimmten IP-Adresse ein Computer existiert und welche Ports unser Computer abhört, wollen wir im folgenden Abschnitt etwas genauer betrachten.

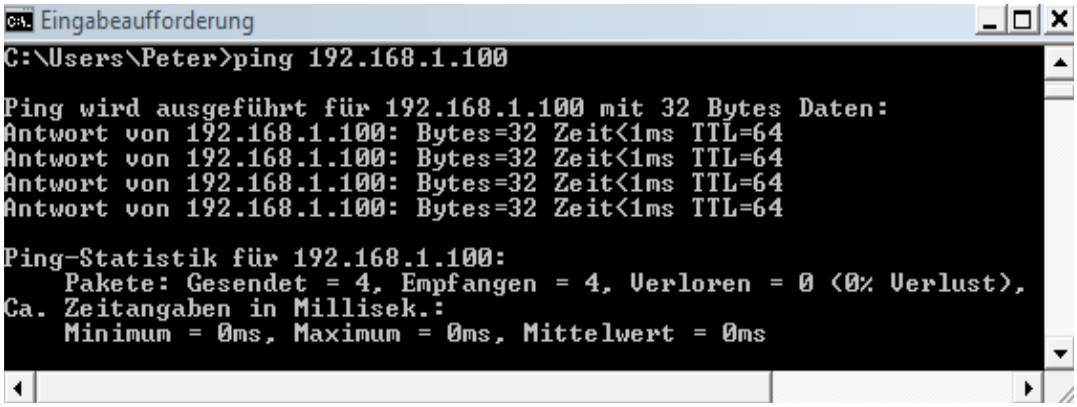
Wie sichtbar ist unser Computer?

Für Leute, die sich professionell mit Netzwerken beschäftigen ist es wichtig, eine einfache und schnelle Möglichkeit zu haben, wie sie herausfinden können, ob und wie schnell ein Computer in einem Netzwerk erreichbar ist. Das Kommando, das dafür benötigt wird, heisst *ping*. Wie der Name vermuten lässt, geht es bei diesem Kommando nicht darum, mit einem anderen Computer sinnvoll zu kommunizieren, sondern nur darum, ob er auf einen Aufruf von unserem Computer reagiert.

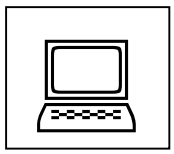


Ermitteln Sie die IP-Adresse Ihres Computers. Starten Sie anschliessend die Eingabeaufforderung (Windows) oder das Netzwerkdienstprogramm (Mac). Bei der Eingabeaufforderung tippen Sie *ping* gefolgt von der IP-Adresse des Computers Ihrer Mitschülerin und anschliessend die Eingabetaste. Auf dem Mac wählen Sie den entsprechenden Reiter, geben Sie die IP-Adresse ein und klicken auf *Ping*. Wenn der aufgerufene Computer reagiert, erscheinen sofort einige Zeilen, die anzeigen, wie schnell der Computer geantwortet hat. Sonst erscheint nichts und Sie können den Befehl manuell abbrechen oder die Eingabeaufforderung schliessen.

Ein erfolgreicher Ping-Aufruf könnte folgendermassen aussehen.

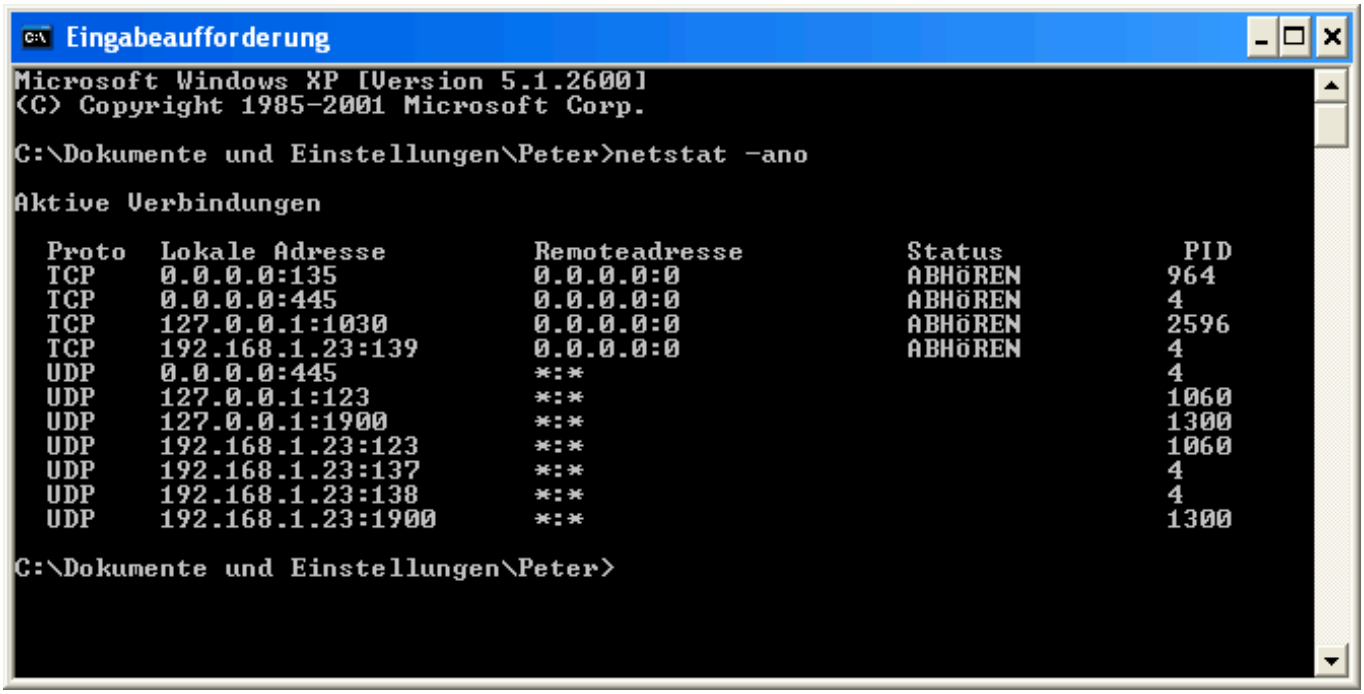


Ping-Aufrufe funktionieren nicht nur in lokalen Netzen. Auch kann statt einer IP-Adresse ein Domain-Name verwendet werden. Versuchen Sie einen externen Server mit einem Ping-Aufruf zu erreichen.



Als nächstes wollen wir prüfen, welche Ports unser Computer abhört. Auch dazu benötigen wir wieder die Eingabeaufforderung (Windows) oder das Netzwerkdienstprogramm (Mac). In der Eingabeaufforderung geben Sie den Befehl *netstat –ano* ein und drücken die Eingabetaste. Im Netzwerdienstprogramm wählen Sie den Reiter *Netstat*, dann die vierte Option, die den Status aller aktiven Socket Verbindungen anzeigt und klicken auf *Netstat*.

Auf einem frisch aufgesetzten PC mit Windows XP und allen Updates sieht die Ausgabe von Netstat wie in der folgenden Abbildung aus. Es ist wahrscheinlich, dass *Netstat* Ihnen in der obigen Übung mehr Zeilen ausgibt.



Diese Ausgabe benötigt noch ein paar Erklärungen.

- *Proto*: In dieser Spalte steht, welches Protokoll verwendet wird (TCP oder UDP). Auf die Unterschiede soll hier nicht näher eingegangen werden.
- *Lokale Adresse*: Hier findet man drei verschiedene IP-Adressen, jeweils gefolgt von einem Doppelpunkt und einem Port. Die Adresse 0.0.0.0 bezeichnet alle Netzwerkadressen, die der Computer hat. Meistens, aber nicht zwingend, ist das nur eine. Die Adresse 127.0.0.1, auch *Loopback* genannt, bezeichnet den Computer selbst. Diese Adresse wird intern vom Computer für sich selbst benützt. Die verbleibende Adresse ist die nach aussen verwendete IP-Adresse.
- *Remoteadresse*: Wenn eine Verbindung zu einem anderen Computer aufgebaut ist, steht hier die Adresse des fremden Computers. 0.0.0.0 oder *.* bezeichnet beliebige fremde Adressen.

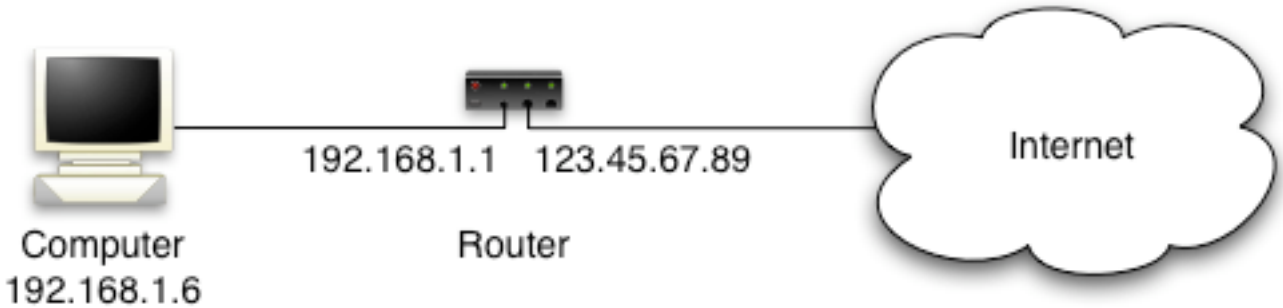
- *Status*: In dieser Spalte wird angezeigt, was unser Computer am entsprechenden Port macht. Am häufigsten trifft man *Abhören*, *Hergestellt* oder *Wartend* an.
- *PID*: In dieser Spalte steht die Prozessnummer des Prozesses, der die Verbindung eröffnet hat.

Alle Verbindungen, deren lokale Adresse nicht 127.0.0.1 ist, sind Verbindungen nach aussen. Das heisst, dass der Computer von dem diese Abbildung stammt, drei offene TCP Ports (135, 445 und 139) und fünf offene UDP Ports (445, 123, 137, 138 und 1900) hat.

Beachten Sie, dass *Netstat* alle Ports anzeigt, die von einem Programm abgehört werden. Das heisst, die Ports werden auch dann noch angezeigt, wenn Sie ein Schutzprogramm verwenden (siehe Abschnitt Firewall), das die Ports gegen aussen verbirgt. Wenn Sie feststellen wollen, welche Ports tatsächlich von aussen, und somit für einen potenziellen Angreifer sichtbar sind, können Sie von einem anderen Computer einen Portscan durchführen. Von einem Mac aus ist das mit dem Netzwerkdienstprogramm möglich, für PCs benötigt man spezielle Software, beispielsweise *Zenmap*.

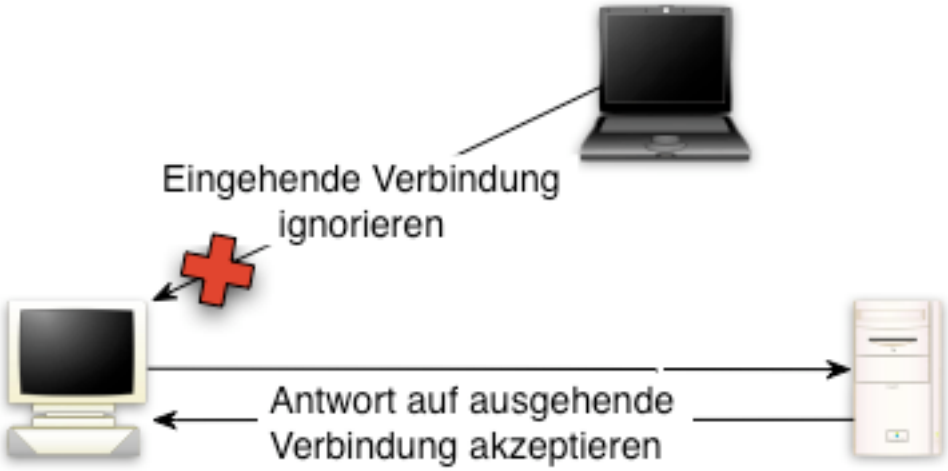
Wie unser Computer geschützt werden kann

In den meisten Fällen ist Ihr Computer gegen aktive Angriffe von aussen bereits recht gut geschützt. Das liegt an der Art und Weise, wie Ihr Computer mit dem Internet verbunden ist. Geschieht das über einen DSL Router, dann ist nach aussen nur die IP-Adresse des Routers sichtbar. Das heisst, dass ein Angreifer gar nicht direkt auf Ihren Computer zugreifen kann. Ihr Computer besitzt dann eine *lokale* IP-Adresse, der Router eine lokale und eine globale. Sie erkennen das daran, dass die IP-Adresse Ihres Computers mit 192.168 beginnt und der Router von Ihrem Computer aus unter 192.168.1.1 erreichbar ist. Nach aussen hin verfügt der Router über eine global IP-Adresse, im abgebildeten Beispiel 123.45.67.89.



Etwas anders ist die Situation, wenn Sie ein Kabelmodem benützen um ins Internet zu gelangen. Ein Kabelmodem ändert nur die Art, wie das Signal übertragen wird. Das heisst, dass Ihr Computer eine nach aussen sichtbare IP-Adresse besitzt, auf die jedermann zugreifen kann.

Ein Router bietet zwar einen gewissen Schutz vor Angriffen von aussen, nicht aber vor Computern im gleichen Subnetz, beispielsweise anderen Computer bei Ihnen zuhause. Es kann auch nicht ausgeschlossen werden, dass ein Angreifer durch den Router in das lokale Netz eindringen kann.
Idealerweise würde sich unser Computer so verhalten, dass wir das Internet unbehindert benutzen können aber ein Angreifer unseren Computer nicht findet. Das heisst, dass unser Computer ausgehende Verbindungen zulässt, eingehende Verbindungen jedoch nur, wenn die Kommunikation von unserem Computer gestartet wurde. Alle anderen eingehenden Verbindungen sollen ignoriert werden.



Programme, die diese Arbeit übernehmen, nennt man Firewall.

Firewall Programme

Die Aufgabe einer Firewall ist es, die Kommunikation zwischen unserem und fremden Computern zu regeln. Das heisst, eine Firewall überwacht die ein- und ausgehenden Verbindungen und legt fest, welche erlaubt sind und welche nicht. Weiter oben haben wir gesehen, dass unser Computer, unter Umständen ohne, dass es uns bewusst ist, gewisse Ports abhört. Eine Firewall sorgt dafür, dass diese Ports von aussen trotzdem nicht sichtbar sind.
Firewalls schützen Ihren Computer nicht nur vor unerwünschten Zugriffen von aussen, sie können auch abgehende Verbindungen überwachen, und Sie warnen, wenn ein Programm mit dem Internet Verbindung aufnehmen will oder dies ganz verbieten. So kann eine Firewall zur Erkennung von Infizierungen beitragen.

Wie bei Antivirenprogrammen gibt es auch bei Firewalls kostenlose und kommerzielle Versionen. Für professionelle Anwendungen gibt es ausserdem auch Firewalls als spezielle Hardware.

Das Installieren einer Firewall auf einem Computer ist nicht immer ganz einfach. Ist die Firewall zu restriktiv eingestellt, behindert sie die Arbeit am Computer, ist sie zu tolerant, nützt sie nichts mehr. Viele Firewalls sind standardmässig so eingestellt, dass sie alle eingehenden Verbindungsanfragen ignorieren und ausgehende Verbindungen nur von bekannten Programmen, beispielsweise Webbrowsern, zulassen. Bei anderen Programmen wird der Benutzer erst informiert und muss den Zugriff explizit erlauben oder verbieten. In der Regel merkt sich die Firewall, wie der Benutzer entschieden hat und verhält sich anschliessend dementsprechend. Leider ist diese Entscheidung für einen Benutzer nicht immer ganz einfach, weil es nicht immer leicht erkennbar ist, welches Programm oder warum ein Programm eine Verbindung mit dem Internet herstellen will. In solchen Fällen kann es sinnvoll sein, zuerst im Internet nach Informationen über das Programm zu suchen.

Kontrollfragen

Kommentieren Sie folgende Aussagen jeweils in wenigen Sätzen.

1) Ich muss auf meinem Computer unbedingt eine Firewall installieren, weil sonst jedermann auf ihn zugreifen kann.

2) Eine Firewall sollte so konfiguriert sein, dass sie alle eingehenden Verbindungen blockiert und alle ausgehenden zulässt.

3) Eine Firewall schützt meinen Computer zwar nicht vor Malware, kann aber helfen, Malware auf meinem Computer zu entdecken.

7 – Vertiefung E-Mail

Lernziele

- Den Aufbau einer E-Mail kennen lernen
- Die Funktionsweise eines E-Mail Clients selbst praktisch durchführen
- Erkennen, wie ein Angreifer beim Verschicken von ungewünschten E-Mails vorgeht.

SMTP – Simple Mail Transport Protocol

SMTP beziehungsweise ESMTP (*Extended SMTP*) wird von Mail Clients für das Versenden von E-Mails benutzt. SMTP benützt den TCP Port 25 und ist ein relativ einfaches Protokoll. Es ist deshalb durchaus möglich, das Protokoll "von Hand" auszuführen um damit die Funktionsweise eines Mail Clients zu demonstrieren.
In einem Terminalfenster (Linux/Mac) oder der Eingabeaufforderung (PC) können wir den *telnet*-Befehl dazu verwenden, Verbindung mit einem Mailserver aufzunehmen. Im Wesentlichen können bei der Kommunikation mit dem Mailserver drei Fälle auftreten, die unterschiedlich einfach nachvollziehbar sind.

SMTP ohne Authentifizierung

Wie sich aus dem Titel bereits schliessen lässt, ist diese Variante nicht sehr sicher. Man trifft sie deshalb in der Praxis nur dort an, wo der Betreiber des Mailservers sicher sein kann, dass nur vertrauenswürdige Clients Mails verschicken. Oft ist ein Mailversand auch nur lokal möglich, also zu Empfängern, die ein Mailkonto auf demselben Mailserver haben. Beispielsweise gibt es Provider, die das Versenden von E-Mails zwischen ihren Kunden ohne Authentifizierung zulassen. Falls Sie an Ihrer Schule über eigene E-Mail Konten verfügen, ist es gut möglich, dass Sie von innerhalb der Schule E-Mails ohne Authentifizierung an Klassenkameraden oder sogar an eine private E-Mail Adresse verschicken können.
Wenden wir uns nun einem konkreten Beispiel zu. Claudia sendet von ihrer Mailadresse *claudia@schule.ch* eine E-Mail an ihre Freundin Patrizia (*patrizia@daheim.ch*).

Die folgende Tabelle zeigt, wie die Kommunikation ablaufen könnte.

Wer	Daten	Kommentar
C	telnet schule.ch 25	Claudia versucht, mit dem Mailserver *schule.ch* über Port 25 Verbindung aufzunehmen. Es können einige Statusmeldungen folgen.
S	220 schule.ch ESMTP is glad to see you!	Kann die Verbindung aufgebaut werden, antwortet der Server mit einer Begrüssungsmeldung. Der Text nach ESMTP kann variieren.
C	HELO schule.ch	Claudia erwidert die Begrüssung mit HELO und dem Namen (oder der IP Adresse) des Servers.
S	250 schule.ch, we trust you [172.17.10.118]	Der Server bestätigt mit der IP Adresse von Claudia.

C	MAIL FROM:<claudia@schule.ch>	Claudia gibt an, von welchem Konto sie eine E-Mail schicken möchte.
S	250 <claudia@schule.ch> sender ok	Der Server bestätigt, dass der Absender existiert.
C	RCPT TO:<patrizia@daheim.ch>	Claudia gibt den Adressaten der E-Mail ein.
S	250 <patrizia@daheim.ch> recipient ok	Der Server bestätigt, dass er den Empfänger akzeptiert.
C	DATA	
S	354 Enter Mail, end with "." on a line by itself	Der Server teilt mit, wie er erkennt, wann der DATA Teil beendet ist. In der Regel geschieht das durch eine Zeile, in der nur ein Punkt steht.
C	Hallo Patrizia Am kommenden Samstag ist DIE Party. Kommst du mit? Ich schlage vor, wir treffen uns um sieben bei mir. Lg & bis dann Claudia .	
S	250 2989654 message accepted for delivery	Der Text nach 250 kann variieren. Die Zahl ist die Identifikationsnummer, die der Server der E-Mail zugeteilt hat.
C	QUIT	Claudia bricht die Verbindung zum Mailserver ab.
S	221 schule.ch ESMTP closing connection	Die Verbindung wird geschlossen.

Dieses Beispiel zeigt die einfachste Möglichkeit eine E-Mail zu verschicken. Wenn Patrizia die Nachricht empfängt, so fehlen einige Angaben, die normalerweise in einer E-Mail stehen.

- Von: Es steht die E-Mail Adresse <claudia@schule.ch> und kein Name.
- An: Bleibt leer
- Antworten: Bleibt leer
- Betreff: Bleibt leer

Damit der Empfänger einer E-Mail diese Angaben erhält, müssen sie am Anfang des (grau gefärbten) Nachrichtenteils stehen. Claudia müsste also im Nachrichtenteil folgendes eingeben:

C	FROM: "Claudia" <claudia@schule.ch> TO: <patrizia@daheim.ch> SUBJECT: Einladung REPLY-TO: "Claudia" <claudia@schule.ch> Hallo Patrizia Am kommenden Samstag ist DIE Party. Kommst du mit? Ich schlage vor, wir treffen uns um sieben bei mir. Lg & bis dann Claudia .

SMTP mit Klartext-Authentifizierung

Die Authentifizierung erfolgt in der Regel mit demselben Passwort, das auch für das Empfangen von E-Mails verlangt wird. Damit kann der Mailserver verhindern, dass irgendein fremder Benutzer das Mailkonto eines anderen Benutzers missbraucht. Die Authentifizierung erfolgt nach der Begrüssung und vor der Eingabe des Absenders (MAIL FROM: ...).
Die Authentifizierung kann verschlüsselt oder offen geschehen. Ein Mailclient kann herausfinden, welche Authentifizierungsmethoden ein Mailserver anbietet, indem er bei der Begrüssung anstelle von HELO den Befehl EHLO verwendet. Die Kommunikation könnte folgendermassen aussehen:

Wer	Daten	Kommentar
C	telnet schule.ch 25	Claudia versucht, mit dem Mailserver *schule.ch* über Port 25 Verbindung aufzunehmen. Es können einige Statusmeldungen folgen.
S	220 schule.ch ESMTP is glad to see you!	Kann die Verbindung aufgebaut werden, antwortet der Server mit einer Begrüssungsmeldung. Der Text nach ESMTP kann variieren.
C	EHLO schule.ch	Claudia erwidert die Begrüssung mit EHLO, damit der Server zusätzliche Informationen liefert.
S	250 schule.ch, we trust you [172.17.10.118] 250 HELP 250 AUTH LOGIN PLAIN 250 SIZE 15360000 250 OK	Der Server bestätigt und liefert Informationen, wie er mit Claudia kommunizieren kann.
C	AUTH PLAIN AGNsYXVkaWFAc2NodWxlLmNoAHRyczgwQzY0	Die Authentifizierung wird im Klartext übermittelt. Dass es auf den ersten Blick trotzdem unverständlich scheint, liegt daran, dass es *base64* codiert ist.
S	235 authentication succeeded	Claudia hat sich erfolgreich authentifiziert.
C	MAIL FROM:<claudia@schule.ch>	Claudia gibt an, von welchem Konto sie eine E-Mail schicken möchte.
S	250 <claudia@schule.ch> sender ok	Der Server bestätigt, dass der Absender existiert.
C	RCPT TO:<patrizia@daheim.ch>	Claudia gibt den Adressaten der E-Mail ein.
S	250 <patrizia@daheim.ch> recipient ok	Der Server bestätigt, dass er den Empfänger akzeptiert.
C	DATA	

S	354 Enter Mail, end with "." on a line by itself	Der Server teilt mit, wie er erkennt, wann der DATA Teil beendet ist. In der Regel geschieht das durch eine Zeile, in der nur ein Punkt steht.
C	Hallo Patrizia Am kommenden Samstag ist DIE Party. Kommst du mit? Ich schlage vor, wir treffen uns um sieben bei mir. Lg & bis dann Claudia .	
S	250 2989654 message accepted for delivery	Der Text nach 250 kann variieren. Die Zahl ist die Identifikationsnummer, die der Server der E-Mail zugeteilt hat.
C	QUIT	Claudia bricht die Verbindung zum Mailserver ab.
S	221 schule.ch ESMTP closing connection	Die Verbindung wird geschlossen.

Die Klartext-Authentifizierung verlangt nach dem Befehl AUTH PLAIN die base64-kodierte Bytefolge <Nullbyte>Benutzeradresse<Nullbyte>Passwort. Die Zeichen müssen deshalb zuerst von der ASCII-Kodierung in die Base64-Kodierung umgewandelt werden. Die nachfolgende Tabelle zeigt einen Ausschnitt der ASCII-Kode-Tabelle.

ASCII	Zeichen	ASCII	Zeichen	ASCII	Zeichen	ASCII	Zeichen
32	Space	55	7	78	N	101	e
33	!	56	8	79	O	102	f
34	"	57	9	80	P	103	g
35	#	58	:	81	Q	104	h
36	$	59	;	82	R	105	i
37	%	60	<	83	S	106	j
38	&	61	=	84	T	107	k
39	'	62	>	85	U	108	l
40	(	63	?	86	V	109	m
41	)	64	@	87	W	110	n
42	*	65	A	88	X	111	o
43	+	66	B	89	Y	112	p
44	,	67	C	90	Z	113	q
45	-	68	D	91	[	114	r
46	.	69	E	92	\	115	s
47	/	70	F	93	]	116	t
48	0	71	G	94	^	117	u
49	1	72	H	95	_	118	v
50	2	73	I	96	`	119	w
51	3	74	J	97	a	120	x
52	4	75	K	98	b	121	y
53	5	76	L	99	c	122	z
54	6	77	M	100	d	123	{

Die Kodierung verläuft nach folgendem Schema: Jeweils drei Bytes (= 24 Bits) werden in vier Gruppen zu je 6 Bits zerlegt. Einer 6-Bit Zahl wird gemäss folgender Tabelle wieder ein Zeichen zugewiesen.

Zahl	Zeichen	Zahl	Zeichen	Zahl	Zeichen	Zahl	Zeichen
0	A	16	Q	32	g	48	w
1	B	17	R	33	h	49	x
2	C	18	S	34	i	50	y
3	D	19	T	35	j	51	z
4	E	20	U	36	k	52	0
5	F	21	V	37	l	53	1
6	G	22	W	38	m	54	2
7	H	23	X	39	n	55	3
8	I	24	Y	40	o	56	4
9	J	25	Z	41	p	57	5
10	K	26	a	42	q	58	6
11	L	27	b	43	r	59	7
12	M	28	c	44	s	60	8
13	N	29	d	45	t	61	9
14	O	30	e	46	u	62	+
15	P	31	f	47	v	63	/

Im oben abgebildeten Beispiel beginnt die Zeichenfolge mit *AGNs*. Um diese vier Zeichen zu dekodieren, gehen wir wie folgt vor.

Code	**A**						**G**						**N**						**s**					
Zahl	0						6						13						44					
Binär	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	0	1	1	0	1	1	0	0
Byte	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	0	1	1	0	1	1	0	0
Zahl	0						99						108											
Zeichen	**Nullbyte**						**c**						**l**											

Wenn die Länge des zu kodierenden Textes nicht durch 3 teilbar ist, so geht die Kodierung nicht auf. In diesem Fall wird der Code mit einem oder zwei "=" ergänzt (siehe folgendes Beispiel).

Code	**K**						**w**						=						=					
Zahl	3						48																	
Binär	0	0	1	0	1	0	1	1	0	0	0	0												
Byte	0	0	1	0	1	0	1	1																
Zahl	43																							
Zeichen	**+**																							

Auf diese Weise lassen sich Benutzername und Passwort leicht entschlüsseln. Als Benutzername erhalten wir, wie erwartet, *claudia@schule.ch*. Finden Sie das Passwort selbst heraus?

Analog können wir vorgehen, um einen gegebenen Benutzernamen/Passwort zu kodieren. Anschliessend können wir diesen Kode in einer Telnet Session zum verschicken einer E-Mail verwenden.
Es steht eine Excel-Datei *Base64 Encoder-Decoder.xls* zur Verfügung, die Makros zur Kodierung und Dekodierung von Base64 Authentifizierungen enthält.

SMTP mit verschlüsselter Übertragung

Besteht ein Mailserver auf einer verschlüsselten Kommunikation, kann eine Demonstration, wie eine E-Mail verschickt wird, nur bis zum Beginn der Verschlüsselung gezeigt werden.

Wer	Daten	Kommentar
C	telnet schule.ch 25	Claudia versucht, mit dem Mailserver *schule.ch* über Port 25 Verbindung aufzunehmen. Es können einige Statusmeldungen folgen.
S	220 schule.ch ESMTP is glad to see you!	Kann die Verbindung aufgebaut werden, antwortet der Server mit einer Begrüssungsmeldung. Der Text nach ESMTP kann variieren.
C	EHLO schule.ch	Claudia erwidert die Begrüssung mit EHLO und dem Namen des Servers.
S	250 schule.ch, we trust you [172.17.10.118] 250 HELP 250 AUTH LOGIN PLAIN 250 SIZE 15360000 250 STARTTLS 250 OK	Der Server bestätigt und liefert Informationen, wie er mit Claudia kommunizieren kann.
C	STARTTLS	Claudia teilt dem Mailserver mit, dass sie mit der verschlüsselten Übertragung beginnen möchte.
S	220 ready to start TLS	Der Server bestätigt.
Ab hier erfolgt die weitere Kommunikation verschlüsselt		

Die ersten beiden Übertragungsarten sind offensichtlich unsicher, weil jemand, der den Netzwerkverkehr abhört, sowohl Passwörter wie auch Inhalt der E-Mail einfach erkennen kann. Die letzte Variante gilt als sicher.
Für die Verschlüsselung wird das TLS-Protokoll (*Transport Layer Security Protocol*) verwendet. Das Protokoll funktioniert ähnlich wie das SSL-Protokoll (*Secure Socket Layer Protocol*), das vor allem bei verschlüsselten Webseiten eingesetzt wird.

Aufbau einer E-Mail

Im ersten Beispiel haben wir gesehen, was im Minimum nötig ist, damit eine E-Mail verschickt werden kann. Auf dem Weg zum Empfänger werden der E-Mail weitere Informationen hinzugefügt, beispielsweise über welche Mailserver die E-Mail auf ihrem Weg bis zum Empfänger geschickt wurde oder ob die E-Mail vom empfangenden Mailserver einer Viren- oder Spamkontrolle unterzogen wurde.
Um ersichtlich zu machen, was genau beim Empfänger ankommt, können wir von unserem Mail-Client den Quelltext (manchmal auch Kopfzeile genannt) der E-Mail anzeigen lassen. So könnte unser obiges Beispiel-E-Mail bei Patrizia folgendermassen ankommen:

```
X-Virus-Scanned: by cgpav
Return-Path: <claudia@schule.ch>
Received: by smtp.daheim.ch (Verwendeter Mailserver)
  with PIPE id 4567523; Thu, 11 Feb 2010 14:38:25 +0100
X-TFF-CGPSA-Version: 1.5
X-CGPANTIVIRUS-Filter: Scanned
X-Spam-Checker-Version: SpamAssassin 3.2.5 (2008-06-10) on
    mail.daheim.ch
X-Spam-Level:
X-Spam-Status: No, score=0.2 required=2.0 tests=AWL,BAYES_00
    autolearn=disabled version=3.2.5
Received: from mail.kanton.ch ([123.123.123.123] verified)
  by smtp.daheim.ch (Verwendetet Mailserver)
  with ESMTP id 4567521 for patrizia@daheim.ch; Thu, 11 Feb 2010 14:38:20 +0100
Received-SPF: none
 receiver=smtp.daheim.ch; client-ip=123.123.123.123; envelope-from=claudia@schule.ch
Received: from schule.ch ([192.168.13.236])
          by mail.kanton.ch
          (Verwendeter Mailserver) with ESMTP
          id <20100211133820.FTBX6780.mail.kanton.ch@schule.ch>
          for <patrizia@daheim.ch>; Thu, 11 Feb 2010 14:38:20 +0100
Received: from schule.ch ([172.17.10.118])
    by schule.ch with edge
    id 2989654; Thu, 11 Feb 2010 14:38:20 +0100
X-SourceIP: 172.17.10.118
Date: Thu, 11 Feb 2010 14:38:20 +0100
Message-Id: <20100211133820.FTBX6780.mail.kanton.ch@schule.ch>
From: "Claudia"<claudia@schule.ch>
To: <patrizia@daheim.ch>
Subject: Einladung
Reply-to: "Claudia"<claudia@schule.ch>

Hallo Patrizia
Am kommenden Samstag ist DIE Party. Kommst du mit?
Ich schlage vor, wir treffen uns um sieben bei mir.

Lg & bis dann Claudia
```

In den Zeilen 33 bis 37 steht der eigentliche Mailinhalt, der von einem Mail-Client angezeigt wird. Davor stehen Informationen, die von einem Mail-Client teilweise verwendet werden, um anzuzeigen, von wem die E-Mail stammt, wann die E-Mail empfangen wurde, an welche E-Mail Adresse eine Antwort geschickt wird etc.
Aus den Zeilen 1 und 6 können wir erkennen, dass auf dem Mailserver, den Patrizia benutzt, ein Antivirenprogramm installiert ist, das einkommende E-Mails auf Viren prüft.
Aus den Zeilen 7 bis 11 (und, – etwas weniger klar erkennbar – auch 5) geht hervor, dass auf dem Mailserver auch eine Antispam-Software installiert ist, die unsere E-Mail nicht als Spam einstuft.
Die meisten der übrigen Zeilen (3, 4 und 12 bis 14 und 17 bis 24) beziehen sich auf den Weg, den die E-Mail zurückgelegt hat. Empfangen wurde sie vom Server *smtp.daheim.ch* (Zeile 3) von einem Server *mail.kanton.ch* (Zeile 12), der wiederum die E-Mail vom Server *schule.ch* (Zeile 17) erhalten hat. Dieser schliesslich hat die Mail von Patrizias Computer über die IP 172.17.10.118 (Zeile 22) erhalten.
Die Zeilen 2 und 28 bis 31 entsprechen dem, was wir beim Verschicken der E-Mail eingegeben haben. Zeile 2 enthält die E-Mail Adresse, die wir nach der Identifizierung bei "*MAIL FROM:*" eingegeben haben. Die Zeilen 28 bis 31 entsprechen den Informationen, die wir im Datenteil nach "*DATA*" gemacht haben. Im normalen Anzeigemodus der E-Mails erscheinen diese Informationen ebenfalls. Steht vor einer E-Mail Adresse jeweils ein Name, so wird dieser anstelle der E-Mail Adresse angezeigt.

- *Reply-to*: Falls eine entsprechende Zeile existiert, erscheint die angegebene E-Mail im Feld *Antworten an*. Möchte ein Benutzer auf die E-Mail antworten, so wird diese E-Mail Adresse verwendet.
- *To*: Falls eine entsprechende Zeile existiert, erscheinen alle angegebenen E-Mail Empfänger im Feld *An*.
- *From*: Falls eine entsprechende Zeile existiert, erscheint die angegebene E-Mail im Feld *Von*. Fehlt ein *Reply-to*, so wird diese E-Mail Adresse für die Antwort verwendet. Fehlen sowohl *Reply-to* als auch *From*, so wird für die Antwort die E-Mail Adresse aus Zeile 2 verwendet.

Da alle diese Felder beliebige Namen und/oder E-Mail Adressen enthalten können, ergeben sich für einen Angreifer mehrere Möglichkeiten, uns zu täuschen. Insbesondere die Angabe einer falschen Adresse beim *Return-Path* ist bei Angreifern sehr beliebt, weil sie damit ihre Identität verbergen können.

In unserem Beispiel haben wir keine Angaben darüber gemacht, woraus der eigentliche Inhalt der E-Mail besteht. Ein Mail Client interpretiert dies so, dass er den gesamten Inhalt als Text betrachtet. Meistens ist das für den heutigen Gebrauch nicht ausreichend. Zum einen gibt es immer mehr E-Mails, die wie eine Webseite aufgebaut sind, also nicht nur Text, sondern auch HTML Code für Formatinformationen, Bilder etc. enthalten. Andererseits müssen Anhänge vom übrigen Inhalt unterschieden werden. Dies geschieht, indem der Inhalt einer E-Mail explizit bezeichnet wird mithilfe von *Content-Type* Zeilen.

Beispiel: Content-Type: text/plain;

Diese Zeilen gehören zum *MIME-Standard* (*Multipurpose Internet Mail Extensions*), der weitere Kommandos enthält, mit denen sich der Inhalt genauer definieren lässt, beispielsweise *Content-Transfer-Encoding*, welches angibt, wie der Inhalt für die Übermittlung kodiert ist.

Einige oft vorkommende Typen sind:

Darstellung des Inhalts

- text/plain Für normale Textinhalte
- text/html Für Inhalte, die aus HTML Code bestehen

Oft wird zusätzlich angegeben, welcher Zeichensatz verwendet wird, beispielsweise *iso-8859-1* (Latin 1, Westeuropäisch).

Inhalte, die aus mehreren Teilen bestehen

- multipart/alternative; boundary = "naechsterTeil"

  Es folgen mehrere Teile, von denen nur einer vom Mail-Client effektiv ausgewählt wird. Am häufigsten trifft man diesen Typen an, wenn der Inhalt einerseits als normaler Text und andererseits als HTML-Code geschickt wird. So können auch Mail-Clients, die kein HTML interpretieren, den Inhalt der Mail verständlich darstellen. Die als *boundary* angegebene Zeichenfolge trennt die einzelnen Teile voneinander.

```
1  Content-Type: multipart/alternative;
2      boundary="4=_Part_12345_6789.0ABC"
3
4  --4=_Part_12345_6789.0ABC
5  Content-Type: text/plain; charset=iso-8859-15
6
7  Hier folgt der Inhalt als normaler Text
8
9  --4=_Part_12345_6789.0ABC
10 Content-Type: text/html; charset=iso-8859-15
11
12 Hier folgt der Inhalt als HTML Code
13
14 --4=_Part_12345_6789.0ABC--
```

  Beachten Sie, dass die Trennzeile nicht nur zwischen den Teilen, sondern auch am Anfang und am Schluss stehen muss. Ausserdem müssen jeder Trennung zwei "-" vorangestellt werden und bei der letzten Trennung müssen am Schluss nochmals zwei "-" angehängt werden.

  Die Trennzeile muss natürlich so gewählt werden, dass sie nicht im eigentlichen Inhalt vorkommt. Deshalb wird in der Regel eine (teilweise) zufällige Zeichenfolge gewählt.

Da man bei seriösen E-Mails davon ausgeht, dass alle Teile inhaltlich mehrheitlich übereinstimmen und sich nur in der Darstellung des Inhalts unterscheiden, werden E-Mails, deren Inhalte in den einzelnen Teilen zu stark voneinander abweichen, oft von Spamfiltern abgefangen.

- multipart/mixed; boundary = "naechsterTeil"

  Dieser Typ wird in der Regel dazu verwendet, Inhalt und Anhänge zu trennen.

```
Content-Type: multipart/mixed; boundary="========MAIL123EDF53GH2"

--========MAIL123EDF53GH2
Content-Type: text/plain; charset="iso-8859-1"
Content-Transfer-Encoding: 8bit

Hier steht der Inhalt

--========MAIL123EDF53GH2
Content-Type: application/pdf;
 name="datei.pdf"
Content-Transfer-Encoding: base64
Content-Disposition: attachment;
 filename="datei.pdf"

Hier steht der Anhang

--========MAIL123EDF53GH2--
```

  Anhänge von E-Mails werden in der Regel *Base64* kodiert, um zu vermeiden, dass zufälligerweise eine Zeichenfolge im Anhang auftritt, die entweder der Trennzeile oder dem Ende der E-Mail (Punkt auf einzelner Zeile) entspricht.

Wenn man selbst via telnet ein E-Mail mit Anhang verschicken möchte, so sollte man beachten, dass die angehängte base64 kodierte Datei in der Regel nicht auf einer Zeile Platz hat. Es ist aber problemlos möglich, die Datei in mehrere Zeilen zu zerlegen.

Experimentieren mit der Viren Testdatei (siehe Anhang B)

Mit der Testdatei können wir verschiedene Dinge überprüfen.

Als ausführbare Datei (z.B. mit der Erweiterung .exe) im Anhang

Wir verschicken eine E-Mail mit der Testdatei im Anhang und schauen, ob sie überhaupt beim Empfänger ankommt.

- Kommt die E-Mail nicht an, so wurde die E-Mail unterwegs von einem Antiviren Programm geprüft, der Testvirus wurde erkannt und die Mail gelöscht. Es kann

ausserdem sein, dass Sie als Absender eine Mitteilung erhalten, dass Sie eine infizierte Datei verschickt haben.

- Kommt die E-Mail an, so sollte unser Antiviren Programm den Testvirus erkennen. Wann das Programm den Testvirus erkennt, ist abhängig vom verwendeten Programm und den Einstellungen. Je nach dem wird der Testvirus bereits beim Empfang der E-Mail erkannt und sofort gelöscht. Es kann aber auch sein, dass das Antiviren Programm erst Alarm schlägt, wenn wir versuchen, die Datei zu öffnen.
- Kommt die E-Mail an und lässt sich der Testvirus öffnen oder als Datei speichern, ohne dass unser Antiviren Programm reagiert, so heisst das, dass das Antiviren Programm entweder ausgeschaltet oder so konfiguriert ist, dass es E-Mails nicht auf Viren testet. In diesem Fall sollten Sie dringend die Einstellungen Ihres Antiviren Programms überprüfen und ändern.

Als "harmlose" Datei (z.B. mit der Erweiterung .txt) im Anhang

Auch hier verschicken wir eine E-Mail mit der Testdatei im Anhang und schauen, ob sie überhaupt beim Empfänger ankommt. Da Textdateien eigentlich keine Gefahr darstellen, werden sie von Antiviren Programmen oft nicht geprüft. Es kann also durchaus sein, dass Sie die E-Mail empfangen und den Anhang auch öffnen können. Das ist nicht weiter schlimm. Wenn Sie die Datei speichern und anschliessend manuell auf Viren überprüfen, sollte Ihr Antiviren Programm jedoch den Testvirus erkennen. Ebenso sollte der Testvirus erkannt werden, wenn Sie von Hand versuchen, die Erweiterung von *.txt* in *.exe* zu ändern.

Die Testsequenz als Text in einer E-Mail verschicken

Nun können wir ausprobieren, was passiert, wenn die Zeichenfolge des Testvirus direkt in der E-Mail steht.
Was erwarten Sie? Kommt die E-Mail an? Wird sie von einem Antiviren Programm erkannt?

8 – Vertiefung WWW

Vorkenntnisse

- Grundkenntnisse in HTML
- Grundkenntnisse in JavaScript
- Grundkenntnisse in Java

Lernziele

- Anhand von konkreten aber harmlosen Beispielen, die auch selbst realisiert werden können, ein tieferes Verständnis für mögliche Angriffspraktiken gewinnen.

Einführung

Ein Angreifer kann auf verschiedene Arten versuchen, seinen Code auf einem seriösen Webserver zu platzieren.

- Er kann versuchen, direkten Zugriff auf den Server zu erhalten, indem er Sicherheitslücken auf dem Server ausnützt. Diese können entweder durch ungenügende Wartung oder Fehler in der verwendeten Software auftreten.
- Bei immer mehr Servern ist es möglich, dass die Benutzerinnen selbst Inhalte auf dem Server platzieren können. Beispiele dafür sind nicht nur Soziale Netzwerke wie Facebook oder MySpace, sondern auch Foren, Blogs, Bewertungen, Rezensionen etc. Oft kann dabei nicht nur Text, sondern auch (in eingeschränktem Mass) HTML Code eingefügt werden. Ein Angreifer kann versuchen, auf diese Art Code einzufügen, der einen Webserver infiziert.
- Wie bereits oben erwähnt, vermieten viele Betreiber Teile ihrer Webseite an Firmen, die darauf Werbung platzieren. Durch mehrfache Untervermietung kann die Kontrolle darüber, wer für den Inhalt verantwortlich ist, verloren gehen und ein Angreifer kann seinen Code auf der Webseite platzieren.
- Nicht jeder Betreiber einer Webseite will das Rad jedes Mal neu erfinden. So gibt es Webseiten, die nützen so genannte Widgets von Drittanbietern. Dies sind in der Regel Links auf Javascripts oder iFrames auf fremden Webseiten. Ein Beispiel dazu wäre ein gratis Traffic Counter, der die Besucheranzahl zählt.

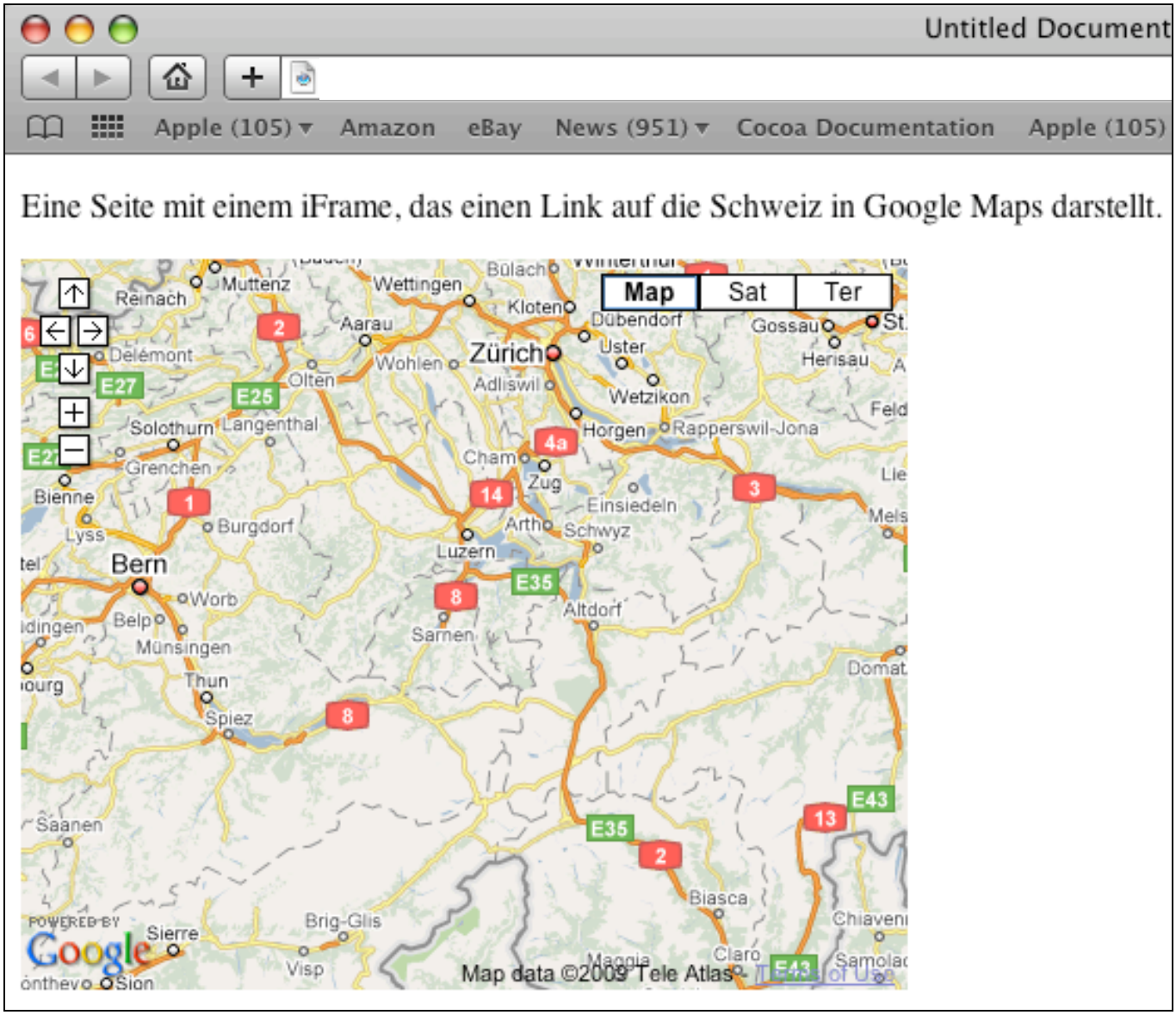
In der Regel, versucht ein Angreifer nicht, bösartigen Code auf den Webserver zu platzieren. Er versucht vielmehr, einen Link zu einem Server, der ihm gehört unterzubringen. Über diesen Server hat er die vollständige Kontrolle und kann damit auch einfach die Art des Angriffs ändern.

Versteckte iFrames

Mit dem <iframe>-Tag kann innerhalb einer Webseite eine “fremde” Quelle, oft wiederum eine HTML Datei, dargestellt werden. Im Gegensatz zu Frames, die eine feste Aufteilung des Browserfenster bewirken, können iFrames wie beispielsweise Bilder irgendwo auf der Seite platziert werden. Eine sinnvolle Anwendung des <iframe>-Tags

könnte beispielsweise die Einbettung einer Online Karte wie beispielsweise Google Maps oder Map Search als Wegbeschreibung in eine Webseite sein.

```
<body>
<p>Eine Seite mit einem iFrame, das einen Link auf die Schweiz in Google Maps darstellt.</p>

<iframe width="425" height="350" frameborder="0" scrolling="no" marginheight="0"
marginwidth="0" src="http://maps.google.com/?
ie=UTF8&amp;ll=46.882723,8.305664&amp;spn=2.849641,3.411255&amp;z=8&amp;output=embed">
</iframe>

</body>
```



Dieses an sich nützliche Tag kann von einem Angreifer missbraucht werden. Er kann in eine seriöse Webseite ein <iframe>-Tag platzieren, das einen Link enthält, der entweder einen Download auslöst oder auf eine Seite mit bösartigem Code führt. Damit ein Benutzer vom iFrame nichts merkt, kann er die Breite und Höhe des iFrames auf "0" setzen.

Das folgende (harmlose) Beispiel lädt in einem unsichtbaren iFrame eine fremde HTML Datei, die eine MP3-Audiodatei enthält, die automatisch abgespielt wird.

```
<iframe src="http://192.168.1.1/embeddedMP3.html" width="0" height="0"
frameborder="0"></iframe>
```

Um das Entdecken von bösartigem Code zu erschweren, können iFrames auch (mehrfach) geschachtelt werden, das heisst, eine eingebettete Datei enthält wiederum ein iFrame. Dadurch wird es schwierig, herauszufinden, von welcher Seite der bösartige Code tatsächlich stammt.

JavaScript

JavaScript wird heute sehr oft in Webseiten verwendet. JavaScript ist eine Programmiersprache, die Code enthält, der vom Browser der Benutzerin ausgeführt wird. Im Gegensatz dazu stehen Programmiersprachen wie PHP, ASP oder JSP, die vom Webserver ausgeführt werden. Mit Hilfe von JavaScript kann die Funktionalität und das Aussehen von Webseiten verbessert werden. Einfache Beispiele für den Einsatz von JavaScript sind beispielsweise Buttons, die ihr Aussehen ändern, wenn man mit der Maus darüber fährt, elementare Tests in Formularen, beispielsweise, ob bestimmte Felder ausgefüllt wurden oder aufspringende Hinweisfenster.
Mit JavaScript können aber auch anstelle der eingegebenen URL eine andere Webseite geladen werden (automatische Umleitung) oder Dateien automatisch herunter geladen werden.
JavaScript kann entweder direkt in HTML Code eingebettet sein oder in einer eigenen Datei mit der Erweiterung *.js*, die von der Webseite importiert wird, stehen.

Angreifer versuchen, den JavaScript Code möglichst schwer verständlich zu machen. Einerseits wird es damit schwieriger festzustellen, wohin eine automatische Umleitung führt und andererseits haben Schutzprogramme dann mehr Mühe, zu merken, dass die Webseite infiziert ist.

Das folgende JavaScript sieht auf den ersten Blick recht chaotisch aus:

```
<SCRIPT type="text/javascript">
function otqzyu(nemz)juyu="lo";sdfwe78="catio";
kjj="n.r";vj20=2;uyty="eplac";iuiuh8889="e";vbb25="('";
awq27="";sftfttft=4;fghdh="'ht";ji87gkol="tp:/";
polkiuu="/ww";jbhj89="w.g";jhbhi87="oo";hgdxgf="gl";
jkhuift="e.c";jygyhg="om'";dh4=eval(fghdh+ji87gkol+
polkiuu+jbhj89+jhbhi87+hgdxgf+jkhuift+jygyhg);je15="')";
if (vj20+sftfttft==6) eval(juyu+sdfwe78+kjj+ uyty+
iuiuh8889+vbb25+awq27+dh4+je15);
otqzyu();//
</SCRIPT>
```

Mit ein wenig Geduld merkt man, dass die JavaScript Funktion eigentlich dem Befehl

```
location.replace('http://www.google.com')
```

entspricht, also den Benutzer automatisch auf die Webseite von Google umleitet.

Neben JavaScript können auch andere Script Sprachen wie *Flash (ActionScript)* oder *VisualBasic* in ähnlicher Weise für Angriffe verwendet werden.

Ein Beispiel für ein typisches Angriffsszenario

- Ein Browser lädt ein *iFrame* über eine infizierte Webseite.
- Das *iFrame* enthält *JavaScript* Code, der ein unsicheres *ActiveX* Element aufruft.
- Das JavaScript enthält weiter Code, der eine *XMLHTTP*-Anfrage startet, um eine ausführbare Datei herunter zu laden. (Ein XMLHttp-Request ermöglicht es, dass eine Script-Sprache wie JavaScript bei einem Server selbständig eine Webseite anfordern und die Antwort auch gleich verarbeiten kann. Somit können aktuelle (im Browser angezeigte Inhalte) dynamisch verändert werden. Diese Technik wird heute, vor allem im Zusammenhang mit *Ajax*, immer öfter verwendet, beispielsweise von Google Maps oder Facebook.)
- Mit Hilfe von *adodb.stream* wird die ausführbare Datei auf die Harddisk des Benutzers geschrieben. (adodb.stream ist ein Microsoft ActiveX Data Object)
- Die ausführbare Datei wird mit *Shell.Application* gestartet.

Client - Server Beispiel für Downloads

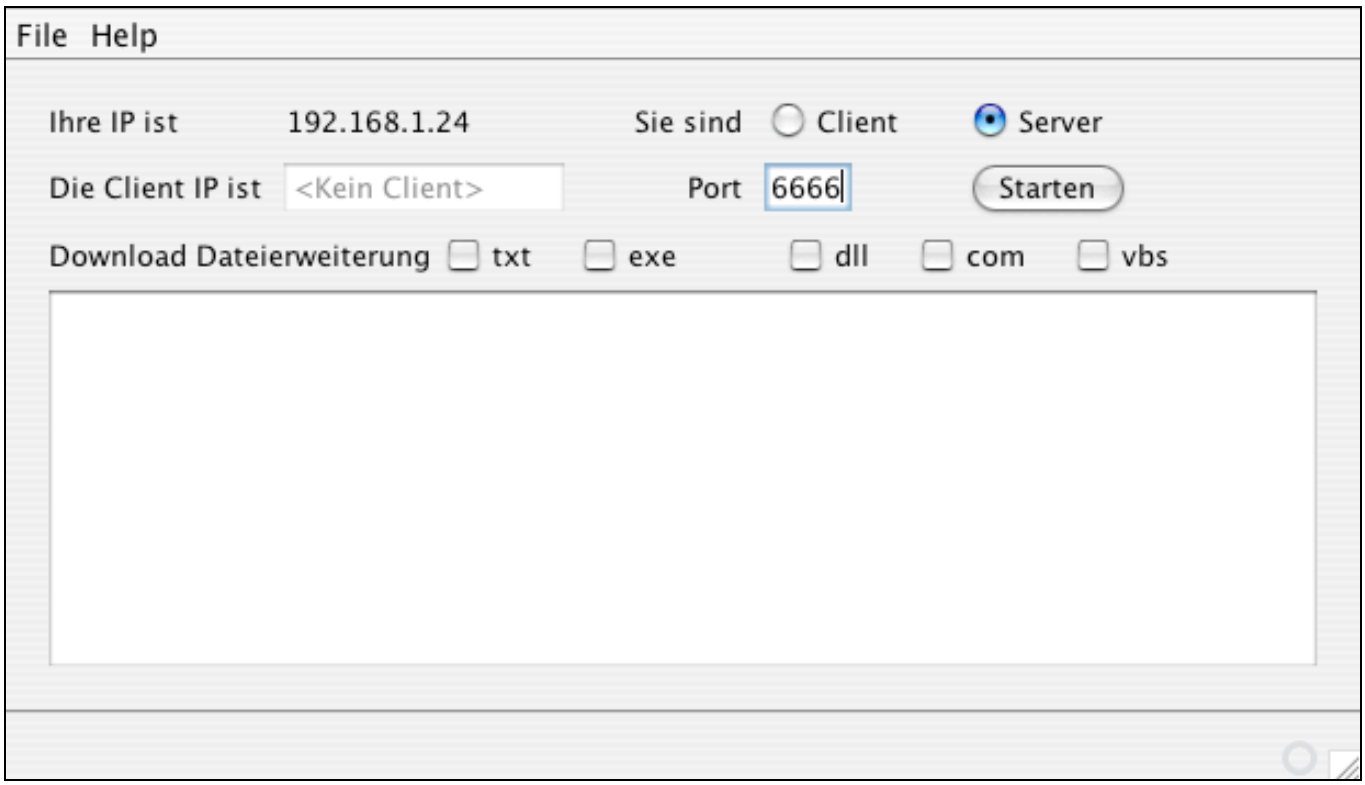
In diesem Abschnitt wird ein kleines Java Programm vorgestellt, das die Idee eines Downloaders grob erklärt. Das Programm kann wahlweise als Client oder Server verwendet werden. Der Client dient als Downloader, der versucht zum Server Kontakt aufzunehmen. Der Server übermittelt die Virentestdatei *eicar* (siehe Anhang B) an den Client zusammen mit der Angabe, mit welcher Erweiterung er die Datei speichern soll. Die Dateien werden im gleichen Verzeichnis gespeichert, in dem sich der Client befindet. Da das Programm im Benutzermodus mit den entsprechenden Rechten abläuft, können zwei Dinge getestet werden. Einerseits, ob Ihr Computer, beziehungsweise eine installierte Firewall, überhaupt zulässt, dass eine Verbindung hergestellt werden kann, und andererseits, ob und wann Ihr Antivirenprogramm die Virentestdatei erkennt.

Um den Programmcode zu verstehen, sollte neben grundlegenden Javakenntnissen die Bedeutung von Java-Threads bekannt sein.

Die wesentlichen Teile des Programms sind die beiden Klassen *Sender* und *Receiver*, beides Unterklassen der Java-Klasse *Thread*.

Die Oberfläche

Wird das Programm gestartet, so kann man wählen, ob es als Server oder als Client dienen soll. Im Servermodus kann man auswählen, welcher Port verwendet werden soll (beachten Sie, dass Ports kleiner als 1024 in der Regel besondere Rechte erforden) und mit welchen Erweiterungen die Virentestdatei beim Client gespeichert werden soll.
Als Client muss man die IP-Adresse des Servers sowie den Port angeben. Dieser muss mit dem im Server angegebenen Port übereinstimmen.



Klickt man auf *Start*, wird der entsprechende Modus (Client oder Server) gestartet. Es ist darauf zu achten, dass der Server vor dem Client gestartet werden muss, sonst kann der Client keine Verbindung aufnehmen.

Die Sender Klasse

Diese Klasse stellt den Serverteil des Programms dar.

```
1  public class Sender extends Thread {
2      ServerSocket s = null;
3      Socket cs = null;
4      JTextArea ta = null;
5      int extensions[] = new int [5];
6
7      public void init(int port, JTextArea outputTextArea, int[] e) throws IOException {
8          s = new ServerSocket(port);
9          ta = outputTextArea;
10         extensions = e;
11     }
12
13     public void run() {
14         try {
15             ta.setText("Warte auf Client...\n");
16             cs = s.accept();
17             PrintWriter out = new PrintWriter(cs.getOutputStream(), true);
18             out.print(extensions[0]);
19             out.print(extensions[1]);
20             out.print(extensions[2]);
21             out.print(extensions[3]);
22             out.print(extensions[4]);
23             out.println("X5O!P%@AP[4\\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*");
24             out.close();
25             cs.close();
26             s.close();
27             ta.append("Folgende Daten gesendet\n");
28             ta.append("X5O!P%@AP[4\\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*\n");
29         } catch (IOException e) {
30             ta.append("Verbindung nicht akzeptiert\n");
31         }
32     }
33
34     public void close() {
35         try {
36             s.close();
37         } catch (IOException e) {
38             ta.append("Problem beim schliessen der Verbindung\n");
39         }
40     }
41 }
```

Der Sender verwendet folgende Variabeln:

- Einen ServerSocket *s*, der den angegeben Port abhört bis ein Client Verbindung aufnimmt.
- Einen Socket *cs*, über den die Kommunikation mit dem Client abläuft.
- Eine JTextArea *ta*, die dem Textfeld im angezeigten Fenster entspricht. Der Sender verwendet sie zur Ausgabe von Mitteilungen.
- Einen Integer Array *extensions*, der für die fünf möglichen Dateierweiterungen entweder 0 (Erweiterung soll nicht verwendet werden) oder 1 (Erweiterung soll verwendet werden) enthält.
- Auf Zeile 17 wird ausserdem ein PrintWriter *out* verwendet, der die Daten übermittelt.

Für die Initialisierung (Zeilen 7 bis 11) erhält der Sender den zu verwendenden Port, das Textfeld sowie den Array mit den Informationen über die Dateierweiterungen. Anschliessend beginnt der ServerSocket den angegeben Port abzuhören.

Wenn der Server gestartet wird, wird die *Run* Methode des Senders ausgeführt. Auf Zeile 16 wartet der Sender, bis ein Client Verbindung aufnehmen will. Auf den Zeilen 18 bis 23 übermittelt der Sender die Daten.

Die Receiver Klasse

Diese Klasse stellt den Clientteil des Programms dar.

Der Receiver verwendet folgende Variabeln:
- Einen Socket *s*, der die Verbindung zum Server aufnimmt
- Eine JTextArea *ta*, die dem Textfeld im angezeigten Fenster entspricht. Der Receiver verwendet sie zur Ausgabe von Mitteilungen.
- Eine boolean Variable, die auf wahr gesetzt wird, sobald der Client die Daten empfangen hat.

In der *Run* Methode werden ausserdem folgende Variablen verwendet:
- Einen BufferedReader *message* (Zeile 12), der die empfangenen Daten speichert.
- Einen String *input* (Zeile 14), der den Inhalt der Datei speichert.
- Einen Integer Array *ext* (Zeile 20), der für die fünf möglichen Dateierweiterungen entweder 0 (ASCII 48, Erweiterung soll nicht verwendet werden) oder 1 (ASCII 49, Erweiterung soll verwendet werden) enthält.
- Eine File Variable *f* (Zeile 30), die die Datei mit der gewünschten Endung erzeugt.
- Einen BufferedWriter *output* (Zeilen 33, 39, 45 und 51), der den Inhalt in das File schreibt.

Für die Initialisierung (Zeilen 6 bis 10) wird die IP-Adresse des Servers als String, der zu verwendende Port sowie das Textfeld übergeben. Anschliessend versucht der Client eine Verbindung zum Server herzustellen.

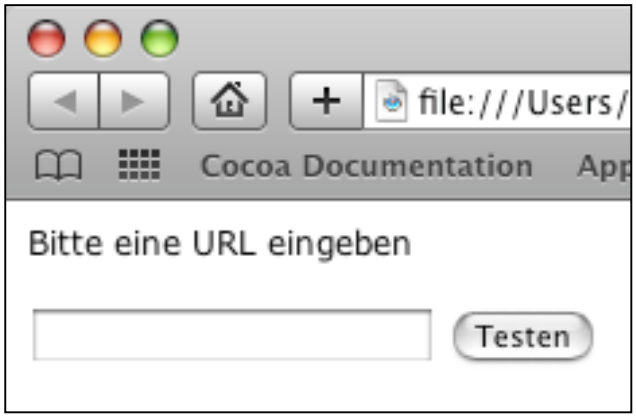
Auf Zeile 18 prüft der Client, ob die Daten schon empfangen wurden, falls ja werden sie auf den Zeilen 21 bis 26 gelesen.
Auf den Zeilen 31 bis 36 wird, falls vom Server gewünscht, eine Textdatei (.txt) mit dem übermittelten Inhalt erzeugt, auf den folgenden Zeilen die übrigen Dateien.

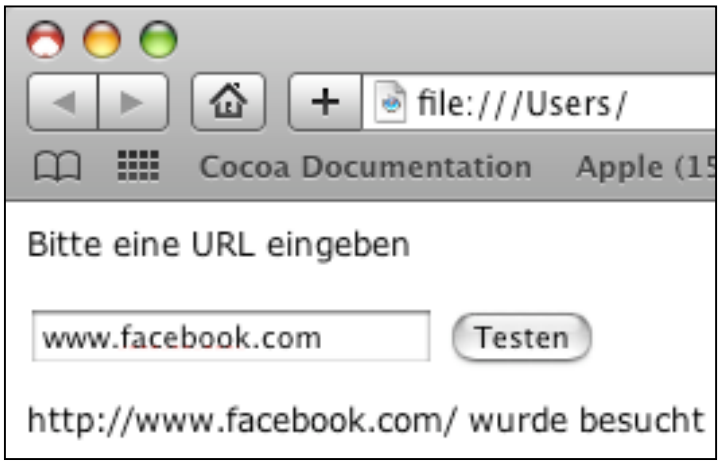
```
public class Receiver extends Thread {
    Socket s = null;
    JTextArea ta = null;
    boolean done = false;

    public void init(String server, int port, JTextArea outputTextArea) throws IOException {
        s = new Socket(server, port);
        ta = outputTextArea;
    }

    public void run() {
        BufferedReader message = null;
        ta.setText("Warte auf Server...\n");
        String input = null;
        try {
            message = new BufferedReader(new InputStreamReader(s.getInputStream()));
            while (!done) {
                if (message.ready()) {
                    done = true;
                    int [] ext = new int [5];
                    ext[0] = message.read();
                    ext[1] = message.read();
                    ext[2] = message.read();
                    ext[3] = message.read();
                    ext[4] = message.read();
                    input = message.readLine();
                    ta.append(input);
                    message.close();
                    s.close();
                    File f;
                    if (ext[0] == 49) {
                        f = new File("VirusTest.txt");
                        Writer output = new BufferedWriter(new FileWriter(f));
                        output.write(input);
                        output.close();
                    }
                    if (ext[1] == 49) {
                        f = new File("VirusTest.exe");
                        Writer output = new BufferedWriter(new FileWriter(f));
                        output.write(input);
                        output.close();
                    }
                    if (ext[2] == 49) {
                        f = new File("VirusTest.dll");
                        Writer output = new BufferedWriter(new FileWriter(f));
                        output.write(input);
                        output.close();
                    }
                    if (ext[3] == 49) {
                        f = new File("VirusTest.com");
                        Writer output = new BufferedWriter(new FileWriter(f));
                        output.write(input);
                        output.close();
                    }
                    if (ext[4] == 49) {
                        f = new File("VirusTest.vbs");
                        Writer output = new BufferedWriter(new FileWriter(f));
                        output.write(input);
                        output.close();
                    }
                }
            }
        } catch (IOException e) {
            ta.append("Keine Antwort vom Server\n");
        }
    }

    public void close() {
        done = true;
    }
}
```

JavaScript für besuchte Webseiten

Im Beispiel von Koobface haben wir gesehen, dass der Downloader anhand der vorhandenen Cookies feststellt, bei welchen sozialen Netzwerken eine Benutzerin Mitglied ist. Ein Angreifer kann das aber auch herausfinden, ohne zuvor ein (bösartiges) Programm auf dem Computer der Benutzerin zu platzieren. Webbrowser speichern besuchte Webseiten über eine gewisse Zeit (Verlauf). Beim Schreiben einer Webseite hat man die Möglichkeit, besuchte und unbesuchte Links unterschiedlich darzustellen, indem man für die Untervarianten des <a>-Tags (*a:link* und *a:visited*) verschiedene Stile definiert. Mit Hilfe eines kleinen JavaScript Programms kann ein Angreifer beispielsweise versteckte Links zu bekannten Webseiten einbauen und aufgrund der Darstellung feststellen, ob die Links kürzlich besucht wurden oder nicht.

Das folgende Codebeispiel zeigt, wie das funktioniert. In einem Browserfenster kann eine URL eingegeben werden. Ein Klick auf die Schaltfläche *Testen* prüft, ob die entsprechende URL kürzlich besucht wurde (also im Verlauf des Browsers gespeichert ist).





Natürlich kann ein solcher Test auch im Versteckten ablaufen. Anstatt eine URL einzugeben, kann eine Liste von URLs fest vorgegeben sein und anstelle einer Ausgabe, ob die Seite kürzlich besucht wurde oder nicht, kann ein Angreifer eine beliebige andere Reaktion programmieren.

```
1  <html>
2  <head>
3  <title>Visited URL Test</title>
4  <style>
5      a   {color:#000000; display:none}
6      a:visited {color:#FF0000; display:inline}
7  </style>
8  <script type="text/javascript">
9  function testen() {
10     var a = document.createElement('a');
11     var url = document.getElementById("URL").value;
12     a.href = "http://" + url;
13     document.body.appendChild(a);
14     if (window.getComputedStyle(a, null).display == "none")
15         document.getElementById("resultat").innerHTML = a.href + " wurde in letzter Zeit nicht besucht";
16     else
17         document.getElementById("resultat").innerHTML = a.href + " wurde besucht";
18     document.body.removeChild(a);
19 }
20 </script>
21 </head>
22
23 <body style="font-family:Verdana, Arial, Helvetica, sans-serif; font-size:12px">
24     <p>Bitte eine URL eingeben<br /><br>
25     <input type="text" id="URL" />
26     <input type="button" value="Testen" onClick="testen()" /><br /></p>
27     <p id="resultat"></p>
28 </body>
29 </html>
```

Erklärungen zum Code:

- In den Zeilen 5 und 6 werden die unterschiedlichen Darstellungen für unbesuchte und besuchte Links festgelegt. Worin die Unterschiede liegen, spielt an und für sich keine Rolle, es ist nur darauf zu achten, dass der Test in Zeile 14 entsprechend angepasst wird.
- Das in den Zeilen 10 bis 13 definierte Link Tag wird in Zeile 18, wenn es nicht mehr gebraucht wird, wieder entfernt. Somit erscheint der Link nicht auf der Webseite.
- Das JavaScript wird in Zeile 26 bei einem Klick auf die Schaltfläche ausgeführt. Natürlich könnte man den Befehl zur Ausführung auch automatisch erteilen.

Passwortverschlüsselung

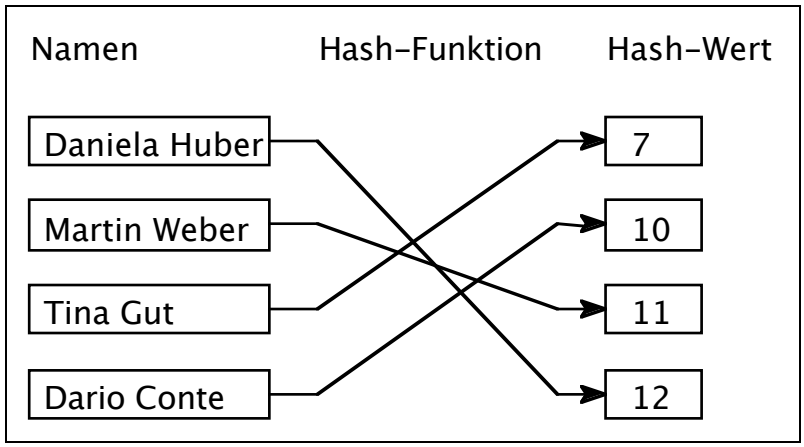
Überall, wo Sie sich mit einem Passwort anmelden müssen, wird das Passwort auch gespeichert. Das gilt für Ihr Benutzerkonto auf Ihrem Computer genau so wie für Online-Dienste. Die Passwörter sollten dabei so gespeichert sein, dass jemand der (berechtigen oder unberechtigten) Zugriff darauf hat, sie trotzdem nicht entziffern kann. Die Passwörter müssen also verschlüsselt gespeichert werden, und zwar so, dass folgende Bedingung erfüllt ist:

- Selbst wenn jemand weiss, nach welchem Vorgehen ein Passwort verschlüsselt wird, kann er aus einem verschlüsselten Passwort das unverschlüsselte nicht (innerhalb praktisch nützlicher Frist) finden.

Es geht also darum, zu einem Passwort *P* eine Verschlüsselung *V* zu finden, sodass es "einfach" ist, aus *P* den Wert für *V* zu finden, aber umgekehrt "sehr schwierig" (im

Idealfall unmöglich) ist, von *V* auf *P* zu schliessen. Sie können sich das konkret etwa so vorstellen: Es ist sehr einfach einen Teller zu zerschlagen, aber unmöglich, den Teller wieder so zusammenzusetzen, dass er wieder wie neu aussieht.

In der Informatik verwendet man dafür so genannte kryptografische Hash-Funktionen. Im Allgemeinen sind Hash-Funktionen Regeln, wie bestimmte komplexe Daten von variabler Grösse in einfachere (normalerweise eine Zahl) zu übersetzen sind. Als Beispiel für eine Hash-Funktion können wir einer Menge von Namen jeweils die Anzahl Buchstaben (ohne Leerschläge) zuordnen.



Es ist einsichtlich, dass die Hash-Funktion aus obigem Beispiel dazu führen kann, dass gewisse Namen denselben Hash-Wert bekommen. Beispielsweise würde *Sandra Meier* ebenfalls denselben Wert wie *Martin Weber* (11) bekommen. In einem solchen Fall spricht man von einer *Kollision*.

Beim Verschlüsseln von Passwörtern sollte eine Hash-Funktion gewählt werden, die mindestens die folgenden Eigenschaften hat:

- Kennt man den Hash-Wert, so sollte es schwierig sein, das zugehörige Passwort zu finden
- Kennt man ein bestimmtes Passwort, so sollte es schwierig sein, ein anderes Passwort zu finden, das denselben Hash-Wert hat.
- Es sollte schwierig sein, zwei Passwörter zu finden, die denselben Hash-Wert haben.

Ausserdem wird in der Regel auch noch darauf geachtet, dass Passwörter, die sich nur geringfügig voneinander unterscheiden, zu gänzlich verschiedenen Hash-Werten führen.

Passwortverschlüsselung unter Windows

Seit der Einführung von Windows Vista werden Passwörter in Windows als *NT Hash*, eine MD4 Verschlüsselung, gespeichert. MD4 gehört zu einer Reihe von Verschlüsselungsverfahren, die oft verwendet werden. Die Idee dieser Verschlüsselung kann mit der Excel-Datei *Idee einer Hash Verschlüsselung.xls* ausprobiert werden. Die Verschlüsselung geschieht nach folgendem Vorgehen:

- Jedes Zeichen des Passworts wird zunächst in eine Zahl umgewandelt (Die Excel Datei verwendet Zahlen von 1 bis 99 für die üblichen auf einer Tastatur vorkommenden Zeichen). Jede Zahl wird zweistellig dargestellt.

  Beispiel: `Hallo` wird dargestellt als: 08 27 38 38 41

  Diese Zahlenfolge hat eine Länge von 10 Ziffern. Der Folge werden nun eine 1 und die (zweistellige) Länge der Zahlenfolge angehängt. Dazwischen werden so viele Nullen eingefügt, dass die Länge der erweiterten Folge durch drei teilbar ist.

  Beispiel: 08 27 38 38 41 10 01 0 (Die Länge ist nun 15)

  Diese Zahlenfolge unterteilen wir in Dreiergruppen.

  082 738 384 110 010

  Die echte MD4 Verschlüsselung arbeitet natürlich nicht mit Dezimalzahlen, sondern mit Binärzahlen. Die Länge des Passworts wird als 64-Bit Zahl dargestellt. Zwischen der eingefügten 1 und der Länge werden so viele Nullen eingefügt, dass die Länge der Bitfolge durch 512 teilbar ist und somit in Gruppen zu je 512 Bits unterteilt werden kann.

- Nun definieren wir drei dreistellige Zahlen A, B und C. In der Excel Datei sind das 123, 456 und 789. Beim echten MD4 werden vier 32-Bit Zahlen definiert, die die folgenden Werte haben:

A:	Dezimal:	19'088'743	Hexadezimal:	01 23 45 67
B:	Dezimal:	2'309'737'967	Hexadezimal:	89 ab cd ef
C:	Dezimal:	4'275'878'552	Hexadezimal:	fe dc ba 98
D:	Dezimal:	1'985'229'328	Hexadezimal:	76 54 32 10

  Ausserdem verwendet der echte MD4 noch zwei weitere Konstanten 5a 82 79 99 und 6e d9 eb a1.

- Nach diesen Vorbereitungen passiert die eigentliche Verschlüsselung. Diese besteht im Wesentlichen aus Additionen und logischen Operationen. Die Excel Datei verwendet Addition (Tausenderstellen werden jeweils gestrichen, z. B. 634 + 583 ⇒ 217), Subtraktion von 999 (zur Andeutung eines bitweisen NICHT) und Rotation (Hunderterstelle wird an die Einerstelle gesetzt, z. B. 736 ⇒ 367).
  Mit jedem Dreierblock P_i des Passworts wird nun folgende Operation durchgeführt:

  $A^* = C$
  $B^* = B + \text{Rotation}(A + P_i + B + 999 - C)$
  $C^* = B$

Das Verschlüsselte Passwort ergibt sich schliesslich aus der Aneinanderreihung von A, B und C und ist somit immer eine 9-stellige Zahl (eventuell führende Nullen eingerechnet).

Die echte MD4 Verschlüsselung führt für jeden 512-Bit-Block folgendes aus. Zuerst wird der Block in 16 Blöcke zu je 32 Bit unterteilt. Auf jeden dieser Blöcke wird eine Operation ähnlich derjenigen, die in der Excel Datei verwendet wird, angewendet. Anschliessend wird in einer zweiten Runde eine zweite Operation wieder auf alle 16 Blöcke angewendet und schliesslich noch eine dritte Runde mit einer dritten Operation. Dieses Vorgehen wird für alle 512-Bit-Blöcke wiederholt. Am Schluss wird das verschlüsselte Passwort durch aneinanderreihen der Zahlen A, B, C und D gebildet. Ein MD4 Passwort hat somit immer eine Länge von 128 Bit.

Knacken von Passwörtern

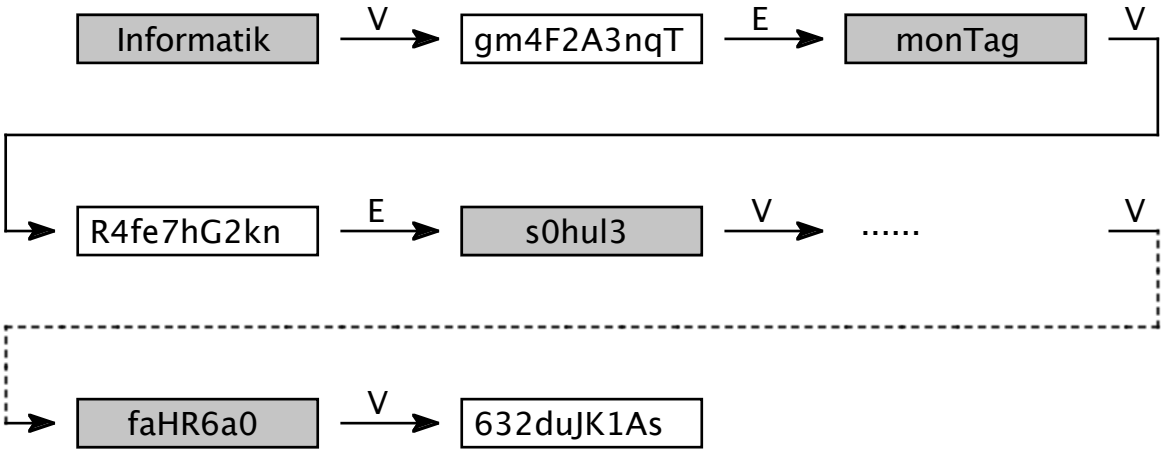
Wenn Sie den vorherigen Abschnitt über Passwortverschlüsselung gelesen haben, so scheint es (fast) unmöglich zu sein, ein auf diese Weise verschlüsseltes Passwort zu knacken. Es ist auch tatsächlich nicht möglich, aus einem Hash-Wert (verschlüsseltes Passwort) das Passwort zu berechnen. Leider ist das für einen Angreifer aber auch gar nicht nötig. Der grosse Nachteil dieser Verschlüsselung ist, dass ein bestimmtes Passwort immer auf dieselbe Verschlüsselung führt. So wird beispielsweise bei der MD4 Verschlüsselung das Passwort “abc” immer zu “a448017aaf21d8525fc10ae87aa6729d” verschlüsselt. Somit kann ein Angreifer in aller Ruhe viele mögliche Passwörter berechnen und sobald er bei einem Angriff ein verschlüsseltes Passwort antrifft, kontrollieren, auf welches die Verschlüsselung passt.

Als aufmerksamer Leserin sollten Sie jetzt Einspruch erheben: Ein Passwort kann ja (fast) beliebig lang sein und für jede Stelle im Passwort kann irgendein Zeichen der Tastatur verwendet werden. Bei einem 8-stelligen Passwort ergibt das rund 10^{16} Möglichkeiten – viel zu viel als dass ein Angreifer in kurzer Zeit alle durchprobieren kann, auch wenn er die Verschlüsselung kennt.
Mit dieser Aussage haben Sie im Prinzip Recht, es gibt jedoch ein Aber. Ein Angreifer kann die Anzahl Versuche dramatisch reduzieren, indem er so genannte *Rainbow Tables* benützt. Die Idee dahinter ist die folgende:

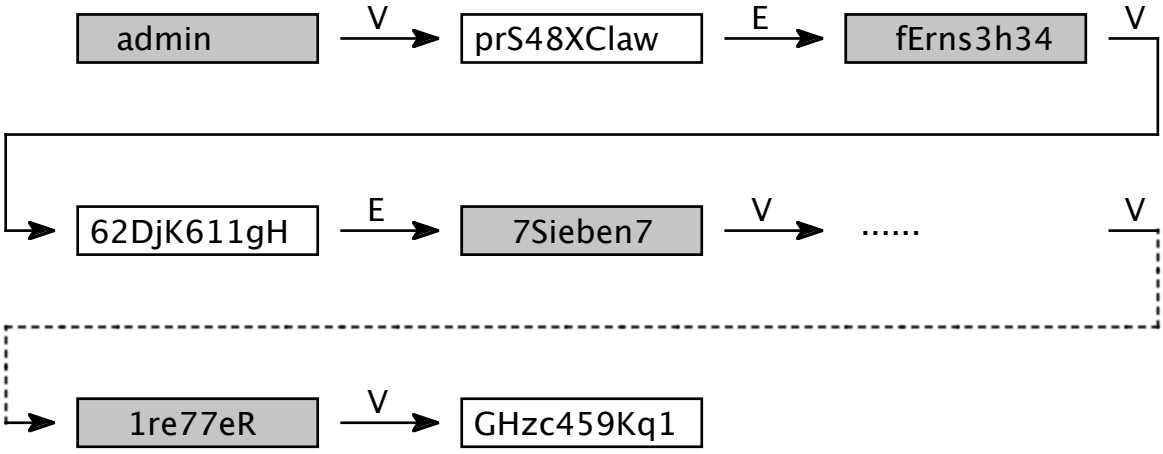
Es ist zwar nicht möglich, ein verschlüsseltes Passwort zu entschlüsseln, man kann jedoch eine Operation finden, die ein verschlüsseltes Passwort in ein falsches entschlüsselt. Was auf den ersten Blick wenig sinnvoll erscheint, entpuppt sich bei genauerem Betrachten als das Ei des Kolumbus. Das falsche Passwort kann nämlich wieder mit der richtigen Verschlüsselung verschlüsselt werden. Dadurch erhält man eine neue Verschlüsselung, die man wiederum zu einem falschen Passwort entschlüsseln kann, und so weiter.

Ein Beispiel:
Nehmen wir an, das Passwort *Informatik* wird richtig zu *gm4F2A3nqT* verschlüsselt. Unsere falsche Entschlüsselung liefert beispielsweise das Passwort *monTag*. Dieses verschlüsseln wir wieder richtig zu *R4fe7hG2kn*. Dieses entschlüsseln wir wieder zum

(falschen) Passwort *s0hul3*. Dieses verschlüsseln wir wieder richtig und so weiter. Somit entsteht eine Folge von Passwörtern und Verschlüsselungen:



Ausserdem legen wir fest, wie lang die Folge werden soll. Als nächstes beginnen wir mit einer neuen Folge und einem neuen, bisher noch nicht vorgekommenen Passwort:



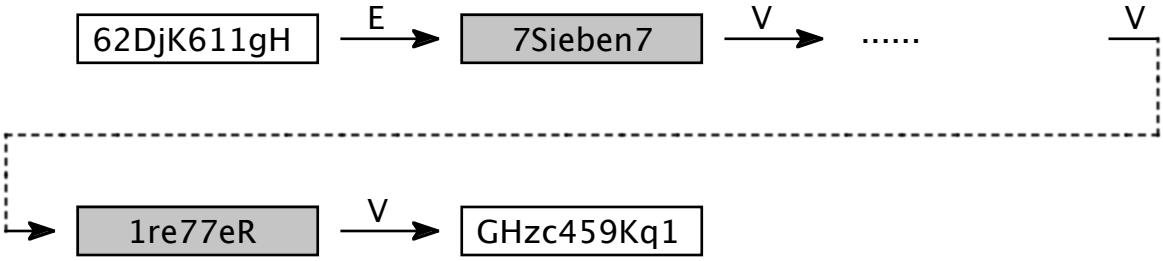
Und nun kommt der wichtige Schritt. Von diesen Folgen speichern wir jeweils das Anfangspasswort und die letzte Verschlüsselung in einer Tabelle, also beispielsweise

Informatik	632duJK1As
admin	GHzc459Kq1
...	...

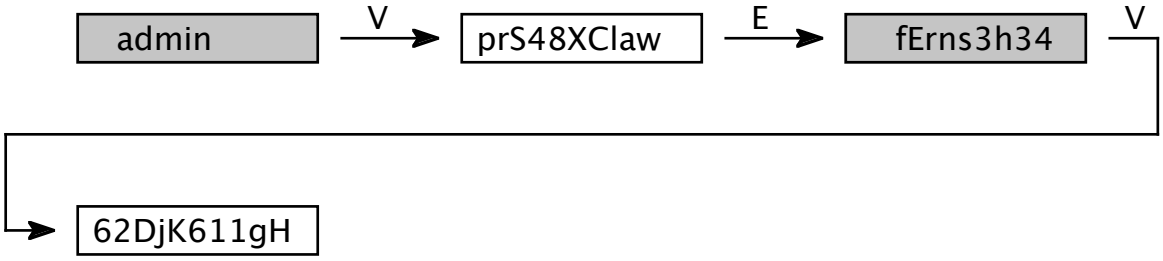
Eine solche Tabelle wird *Rainbow Table* genannt.

Haben wir nun ein verschlüsseltes Passwort, das wir knacken möchten, so wenden wir dasselbe Verfahren zum Ent- und Verschlüsseln an, bis wir auf einen der Werte in der zweiten Spalte der Tabelle treffen. Wir wissen nun, dass sich das gesuchte Passwort in jener Folge befinden muss. Also beginnen wir mit dem entsprechenden Anfangspasswort, bis wir wissen, welches Passwort auf die zu knackende Verschlüsselung führt.

Nehmen wir an, wir haben das verschlüsselte Passwort *62DjK611gH* gefunden. Wenn wir dieses entschlüsseln dann das Ergebnis wieder verschlüsseln und so weiter, gelangen wir irgendwann zur Verschlüsselung *GHzc459Kq1*.



Wir wissen nun also, dass sich das gesuchte Passwort in der Folge befindet, die mit *admin* beginnt. Also durchsuchen wir diese Folge, bis wir das Passwort *fErns3h34* finden, das zu *62DjK611gH* verschlüsselt wird.



Im Internet findet man Rainbow Tables unterschiedlicher Grösse, für das Knacken unterschiedlicher Passwörter. So existiert beispielsweise eine knapp 65GB grosse Tabelle, die in der Lage ist, jedes beliebige Windows XP Passwort in vernünftiger Zeit zu knacken. Kleinere Tabellen können Passwörter bis zu einer bestimmten Länge oder nur mit bestimmten Zeichen innert Sekunden bis wenigen Minuten herausfinden.

9 – Quellen

Auf Wikipedia findet man Erklärungen und detaillierte Informationen zu den im Leitprogramm erwähnten technischen Ausdrücken und Verfahren. Dabei lohnt es sich, sowohl die deutsche als auch die englische Seite zu einem Begriff zu konsultieren.

Alle erwähnten Links entsprechen dem Stand 5. März 2010.

Weitere Unterrichtsmaterialien

- http://www.bsi-fuer-buerger.de
  Das Bundesamt für Sicherheit in der Informationstechnik Deutschland stellt auf dieser Seite viele nützliche Informationen über Malware und den allgemeinen Umgang mit dem Internet zur Verfügung. Unter anderem findet man auch einen als Einführung ins Thema durchaus geeigneten Film (ca. 6 Minuten).
- Michael Näf, Patrick Streule, Werner Hartmann – Risiko Internet, Orell Füssli Verlag Zürich, 2000
  http://www.swisseduc.ch/informatik/internet/internet_sicherheit/index.html
  Kostenlose Online Version des gleichnamigen Buches. Ein gut geschriebenes, leicht verständliches Buch zum Selbststudium. Neben Malware wird auch auf Datenschutz und Datenverschlüsselung beispielsweise beim Online Shopping eingegangen
- http://browserspy.dk/
  Homepage von Henrik Gemal. Enthält eine grosse Menge von Scripts, die demonstrieren, welche Informationen ein Browser einem Betreiber einer Webseite mitteilt. (Englisch)
- http://www.eicar.org/anti_virus_test_file.htm
  Die Organisation Eicar stellt kostenlos ein Viren Testfile zur Verfügung, das beispielsweise zum Testen der eingesetzten Antiviren-Software verwendet werden kann. (Englisch)

Informationen

- http://www.melani.admin.ch
  Die Homepage der Melde- und Analysestelle Informationssicherung informiert über aktuelle Bedrohungen und veröffentlicht halbjährlich Lageberichte über Tendenzen in der Bedrohung.
- http://www.scip.ch/?vuldb
  Homepage einer Schweizer Information Security Firma mit einer deutschsprachigen Datenbank über aktuelle Sicherheitsmängel diverser Betriebssysteme und Programme. Neben einer kurzen Beschreibung der Schwachstelle findet man auch Angaben zu Patches.
- Niels Provos, Dean McNamee, Panayiotis Mavrommatis, Ke Wang, Nagendra Modadugu – Google, 2007
  The Ghost in the Browser – Analysis of Web-based Malware
  http://www.usenix.org/events/hotbots07/tech/full_papers/provos/provos.pdf
  Ein White-Paper über Malware Techniken, die Google beobachtet hat. Mit Beispielen. (Englisch)

- Jonell Baltazar, Joey Costoya, Ryan Flores – TrendMicro – The Real Face of KOOBFACE
  http://us.trendmicro.com/imperia/md/content/us/trendwatch/researchandanalysis/the_real_face_of_koobface_jul2009.pdf
  Eine detaillierte Beschreibung, wie Koobface bei der Infektion vorgeht. Gibt eine gute Übersicht über verschiedene Arten von Malware. (Englisch)
- http://www.verfassungsschutz.niedersachsen.de/master/0,,C1565471_N1179837_L20_D0_I541,00.html
  Homepage des Verfassungsschutzes Niedersachsen mit Informationen und Tipps zu einer sicheren Passwortwahl.
- http://www.what-is-exe.com/
  Eine Webseite, die eine Vielzahl von .dll und .exe Dateien kurz erklärt und angibt, ob es sich um seriöse Dateien oder Spyware, Adware oder Viren handeln könnte. (Englisch)
- http://www.maawg.org/email_metrics_report
  Homepage der Messaging Anit-Abuse Working Group, einer Organisation, die unter anderem Statistiken über den Missbrauch von E-Mail veröffentlicht. (Englisch)
- Steve Anson, Steve Bunting – Windows Network Forensics and Investigation, Wiley Publishing Inc., 2007
  Ein Buch, das sich in erster Linie an Sicherheitsexperten wendet, deren Aufgabe es ist, Windows Netzwerke auf Infizierungen zu prüfen. Trotzdem ist das Buch ziemlich leicht verständlich und enthält gute Beispiele für mögliche Angriffsszenarien. (Englisch)

Filme

- Chris Walters – Flash-Based Malware Ad Sneaks Onto Legit Websites Via DoubleClick (2007)
  http://consumerist.com/2007/11/flash-based-malware-ad-sneaks-onto-legit-websites-via-doubleclick.html
  Zeigt in einem Film ein Beispiel für eine Malware, die über ein Werbebanner einer seriösen Webseite verbreitet wird. Qualität des Films nicht besonders. (Englisch)
- Corey Nachreiner – WatchGuard Technologies – Video Tutorials
  http://www.watchguard.com/education/videos.asp?t=main
  Videos zum Thema Malware. Empfehlenswert: Drive-By Download. Sonst teilweise relativ technisch. (Englisch). Videos können herunter geladen werden.

Verschiedenes

- http://learn-networking.com/category/network-security
  Eine Homepage, die vor allem Übungsmaterial für angehende Netzwerktechniker bereitstellt. Die erwähnte Seite führt auf Links zu drei bekannten Trojanern aus der Zeit um die Jahrtausendwende. (Englisch)
- http://nmap.org/zenmap
  Eine Webseite, von der aus man einen kostenlosen Portscanner alle Plattformen herunterladen kann.
- http://www.wireshark.org

Eine Webseite, die ein kostenloses Programm zur Überwachung des Netzwerkverkehrs zum Download zur Verfügung stellt. Die Pakete können nach Dienst gefiltert werden und die Resultate graphisch übersichtlich dargestellt. Für Windows und Mac (auf dem Mac wird X11 benötigt).

- http://www.metasploit.com/
  Eine Webseite, welche diverse Angriffssoftware zu Testzwecken zur Verfügung stellt. Achtung: Die Angriffe sind echt, können also einen ungeschützten Computer tatsächlich infizieren. Für Experimente sollte daher ein Testumgebung verwendet werden... (Englisch)
- http://ophcrack.org/
  Eine Webseite, welche ein Programm gratis zur Verfügung stellt, das mit Hilfe von Rainbow Tables Passwörter von Windows knackt. (Englisch)

Anhang A

Lösungen zu den Kontrollfragen Kapitel 1

1) Eine lokale IP-Adresse wird von Routern nicht weitergegeben. Die Konsequenzen daraus sind, dass ein Computer mit einer lokalen Adresse von aussen nicht direkt erreichbar ist. Computer mit einer globalen IP-Adresse sind von überall her erreichbar.

2) Ein DNS Server übersetzt Domain Namen in IP-Adressen und umgekehrt. Somit ermöglicht ein DNS Server, dass wir beispielsweise Webseiten mit *www.beispiel.ch* ansprechen können und nicht mit 123.45.67.89.

3) Im Normalfall benötigen Sie entweder einen DSL-Router oder ein Kabelmodem. Selten wird heute eine (langsame) Verbindung mit einem Modem über die analoge Telefonleitung oder ISDN verwendet.

4) Das ist möglich, wenn Sie die IP-Adresse des Servers kennen.

Lösungen zu den Kontrollfragen Kapitel 2

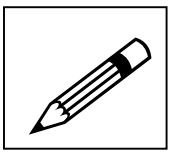
1) Es gibt zwei Hauptpunkte, warum Daniel seine Meinung ändern sollte. Erstens kann er seinen Computer auch schützen, ohne Geld auszugeben, weil es verschiedene Schutzprogramme auch gratis gibt. Dies betrifft sowohl Antivirenprogramme als auch Firewalls und Antispywareprogramme. Zweitens geht es nicht nur darum, ob Daniel auf seinem Computer für einen Angreifer interessante Dinge gespeichert hat. Es geht vor allem auch darum, dass ein Angreifer Daniels Computer in sein Botnet integrieren kann und für Angriffe auf Computer von Drittparteien nützen kann oder dass er auf Daniels Computer illegale Dateien platziert und diese je nach dem zum Download freigibt. Es gab beispielsweise 1999 einen Fall, bei dem auf dem Computer eines schwedischen Wissenschaftlers Kinderpornographie gefunden wurde, die über einen Trojaner dort platziert wurde. Es dauerte fünf Jahre, bis er rehabilitiert wurde.

2) Viele der bösartigen Programme, die heute verwendet werden, tragen die Merkmale verschiedener Kategorien. So kann beispielsweise ein Trojaner als Downloader für verschiedene Arten von Malware funktionieren, oder ein Wurm kann auch Eigenschaften eines Trojaners haben und so weiter.

3) Folgende Anzeichen *können* ein Hinweis darauf sein, dass sich auf Ihrem Computer Malware befindet.
   - Ihre Internetverbindung ist plötzlich sehr viel langsamer als früher.
   - Falls Sie die Möglichkeit haben, zu überwachen, welche Programme auf das Internet zugreifen, und Sie stellen fest, dass ein seltsames Programm häufig auf das Internet zugreift.

- Auf Ihrem Bildschirm erscheinen periodisch Fenster, die für irgendwelche Produkte werben.
- Ihr Computer verhält sich plötzlich seltsam, beispielsweise unerwartete Abstürze, verschwundene Dateien oder Ähnliches.
- Ihr E-Mail Konto wurde gesperrt, weil damit Spam verschickt wurde.
- Freunde in sozialen Netzwerken beklagen sich bei Ihnen, dass sie Mitteilungen mit einem verdächtigen Inhalt von Ihnen bekommen.
- Wenn Sie nach einem Begriff googeln, erscheinen zuoberst Links auf dubiose Webseiten.

Lösungen zu den Aufgaben Kapitel 3

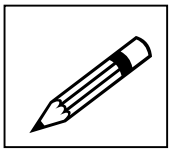


Welche der folgenden E-Mails erscheinen Ihnen seriös (können Sie wahrscheinlich ohne Bedenken öffnen), bei welchen sind Sie unsicher, ob sie Spam enthalten oder gefährlich sein könnten und welche E-Mails würden Sie ungelesen löschen, weil sie sicher unseriös sind?

@	Absender	Betreff	Datum
@	Englischlehrer	Aufgaben für nächsten Dienstag	
	Mahnung	Offene Rechnung	
	Lotterie Schweiz	Sie haben gewonnen!	
	Walter	Re:	
@	Patrick@vss.ch	Umfrage für unsere Maturarbeit	
@	Rita	Dein Bild auf Facebook	
	MySpace	Spaceman möchte dein Freund auf MySpa	
	Lea@vss.ch	I need your help	
@	Robbie	Fwd: Important!	

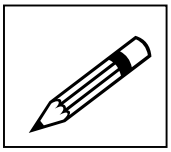
Die E-Mails von Ihrem Englischlehrer und von Patrick sind mit grosser Wahrscheinlichkeit seriös und können ohne Bedenken geöffnet werden.
Die E-Mails von Mahnung, Lotterie Schweiz und Rita sind mit grösster Wahrscheinlichkeit unseriös und können ungelesen gelöscht werden. Solche E-Mails versuchen oft, einen Benutzer entweder zu erschrecken (Androhung von Gerichtsverfahren, Peinliche Bilder oder Videos des Benutzers im Internet etc.), ihm einen finanziellen Gewinn in Aussicht zu stellen, oder um finanzielle Hilfe zu bitten. Dadurch soll der Benutzer veranlasst werden, Links oder Anhänge in der E-Mail anzuklicken, die unseriös oder gefährlich sind.
Wenn Sie die E-Mail von Walter anschauen, so scheint diese E-Mail eine Antwort auf eine E-Mail mit leerem Betreff (Re: oder Aw: oder ähnliches deuten darauf hin) zu sein. Da stellt sich natürlich die Frage, ob Sie eine solche E-Mail an Walter geschrieben haben oder Sie eine E-Mail an mehrere Personen, darunter auch Walter, mit leerem Betreff

erhalten haben. Falls nicht, so ist die E-Mail mit grosser Wahrscheinlichkeit unseriös und kann ungelesen gelöscht werden.
Bei E-Mails mit fremdsprachigem Betreff sollten Sie eigentlich immer, auch wenn Ihnen der Absender seriös vorkommt, stutzig werden. Ist es realistisch, dass Ihnen der Absender in einer Fremdsprache schreibt? Gerade wenn Sie den Absender nicht kennen, dürfte es sich um eine unseriöse E-Mail handeln, die Sie ungelesen löschen können. Sonst können Sie die E-Mail mit der nötigen Vorsicht öffnen.
Falls Sie kein MySpace-Konto haben, so sollten Sie die betreffende E-Mail nicht öffnen. Sonst können Sie sie mit der nötigen Vorsicht öffnen.



Welche der E-Mails erscheinen Ihnen seriös? Auf welche Links können Sie klicken und bei welchen sollten Sie vorsichtig sein? Begründen Sie Ihre Entscheidung.

Die Information über die Freundanfrage scheint seriös zu sein. Jedoch handelt es sich dabei um einen Standardtext, der natürlich auch von jemandem kopiert werden kann. Kontrollieren Sie auf alle Fälle, ob die Links tatsächlich zu MySpace führen. Oder noch besser: Klicken Sie nicht auf die Links sondern loggen Sie sich wie gewohnt bei MySpace ein.
Die Virenwarnung ist ganz sicher unseriös. Keine Organisation verschickt solche Warnungen. Auf den angegebenen Link sollten Sie keinesfalls klicken.
Die E-Mail von MSN sollte Sie auch stutzig machen. Wenn Sie MSN nicht nutzen, dann ist es offensichtlich, dass die E-Mail unseriös ist. Grundsätzlich sollten Sie bei allen E-Mails, bei denen Sie aufgefordert werden, auf einen Link zu klicken, vorsichtig sein und prüfen, wohin der Link führt. Wenn es darum geht, dass Sie Einstellung in einem von Ihnen genutzten Online-Dienst vornehmen, ist es immer ratsam, auf dem üblichen Weg in den Dienst einzusteigen und nicht einem Link in einer E-Mail zu folgen.
Die E-Mail mit dem Link zu YouTube kann, insbesondere wenn Sie den Absender kennen, durchaus seriös sein. Prüfen Sie vor dem Klick auf den Link, dass er auch tatsächlich dorthin führt.



Bei welchen E-Mails können Sie die Anhänge ohne grosses Risiko öffnen, welche sollten Sie besser vorher mit einem Antivirenprogramm prüfen und welche Anhänge sollten Sie sicher nicht öffnen? Begründen Sie Ihre Antwort.

Der Anhang der ersten Mail ist ganz sicher gefährlich. Keine seriöse Organisation verschickt solche E-Mails. Es fehlen jegliche Angaben darüber, auf welche Dienstleistung oder welches Produkt sich die Kosten beziehen und von welchem Konto der Betrag abgezogen wurde. Ausserdem ist es sehr unwahrscheinlich, dass eine Auflistung als .zip Datei angehängt wird.
Der Anhang der zweiten Mail ist höchst wahrscheinlich ungefährlich. Einerseits ist der Inhalt der E-Mail sinnvoll und andererseits ist der Anhang eine .pdf Datei, die in den allermeisten Fällen ungefährlich sind.

Auch die dritte E-Mail ist sehr wahrscheinlich seriös. Da der Anhang jedoch eine Word-Datei ist, die Makroviren enthalten kann, sollten Sie sicherstellen, dass die Datei vor dem Öffnen von einem Virenscanner geprüft wird.

Lösungen zu den Kontrollfragen Kapitel 3

1) Die Aussage von Linda ist etwas gar zuversichtlich. Obwohl ein aktuelles Antivirenprogramm, sofern es auch so konfiguriert ist, dass es E-Mails prüft, bereits einen guten Schutz bietet, kann das Verhalten von Linda trotzdem noch unerwünschte Konsequenzen haben. Zum einen könnte ein Anhang Sicherheitslücken in einem Programm ausnützen, die ein Antivirenprogramm (noch) nicht erkennt, andererseits kann ein Spammer so herausfinden, dass Lindas E-Mail Konto ein aktives Konto ist, das benützt wird.

   Marcos Aussage ist in der Praxis einerseits schwierig umzusetzen und andererseits schützt sie nicht unbedingt vor Gefahren. Es ist sicher sinnvoll, E-Mails von unbekannten Absendern tendenziell zu löschen, insbesondere, wenn auch der Betreff nicht seriös erscheint. Da aber auch hinter einem scheinbar bekannten Absender ein Übeltäter stecken könnte, schützt dieses Vorgehen nicht vor jeder Gefahr. Ausserdem verwenden die meisten Benutzer von Gratis E-Mail Adressen, wie beispielsweise Hotmail, Pseudonyme, sodass auch hinter einem unbekannten Absender unter Umständen ein Bekannter stecken könnte. Auf alle Fälle ist es ratsam, nicht nur den Absender, sondern auch den Betreff einer E-Mail in die Überlegungen einzubeziehen, ob man eine E-Mail öffnen will oder nicht.

2) Word Dokumente können Makroviren enthalten. Wenn Ihr Antivirenprogramm E-Mails nicht überprüft (oder Sie nicht sicher sind, ob der Anhang geprüft wird), ist eine manuelle Prüfung der Datei mit einem Antivirenprogramm immer ratsam. Eine solche Prüfung dauert vielleicht 15 Sekunden und kann Ihnen je nach dem einigen Ärger ersparen.

3) Einer solchen Aufforderung sollten Sie nie nachkommen. Bevor Sie auf “Abbrechen” klicken, empfiehlt es sich, dass Sie sich merken, um welche Komponente es sich handelt. Nun können Sie im Internet die entsprechende Komponente suchen, und falls es sich um etwas Seriöses handelt, die Komponente herunterladen und installieren.

Lösungen zu den Kontrollfragen Kapitel 4

1) Eine solche Meldung kann zwei Ursachen haben. Entweder ist die Webseite seriös und es fehlt tatsächlich eine entsprechende Softwarekomponente, beispielsweise ein Plugin, ein Codec zum Abspielen eines Videos oder eine ActiveX Komponente, oder die Webseite ist infiziert und versucht auf diese Art ein bösartiges Programm auf Ihrem Computer zu platzieren. Um herauszufinden, was der Fall ist, können Sie folgendermassen vorgehen:

- Schauen Sie die URL genau an. Wenn sie fast wie eine bekannte URL lautet, beispielsweise *www.faecbook.com*, können Sie relativ sicher sein, dass Sie auf einer unseriösen Webseite gelandet sind.
- Überprüfen Sie, ob sich die angeblich fehlende Komponente tatsächlich nicht auf Ihrem Computer befindet. Falls doch, so besteht eine relativ hohe Wahrscheinlichkeit, dass die Meldung nicht seriös ist.
- In der Regel erscheint zusätzlich zur Meldung ein Link, den Sie anklicken sollen. Prüfen Sie, was passieren würde, wenn Sie auf den Link klicken. Bei seriösen Webseiten führt der Link (fast) immer auf die Webseite des Herstellers der fehlenden Software. Wenn der Link direkt einen Download auslöst, so ist die Wahrscheinlichkeit gross, dass Sie damit eine bösartige Software herunterladen.

2) Social Engineering bezeichnet das Sammeln von Informationen aus dem Umfeld einer Person, mit dem Ziel, diese Informationen zum Aufbau eines Vertrauensverhältnisses zu nutzen. Ist das Vertrauen einmal aufgebaut, so missbraucht es ein Angreifer, um an vertrauliche Informationen zu kommen.

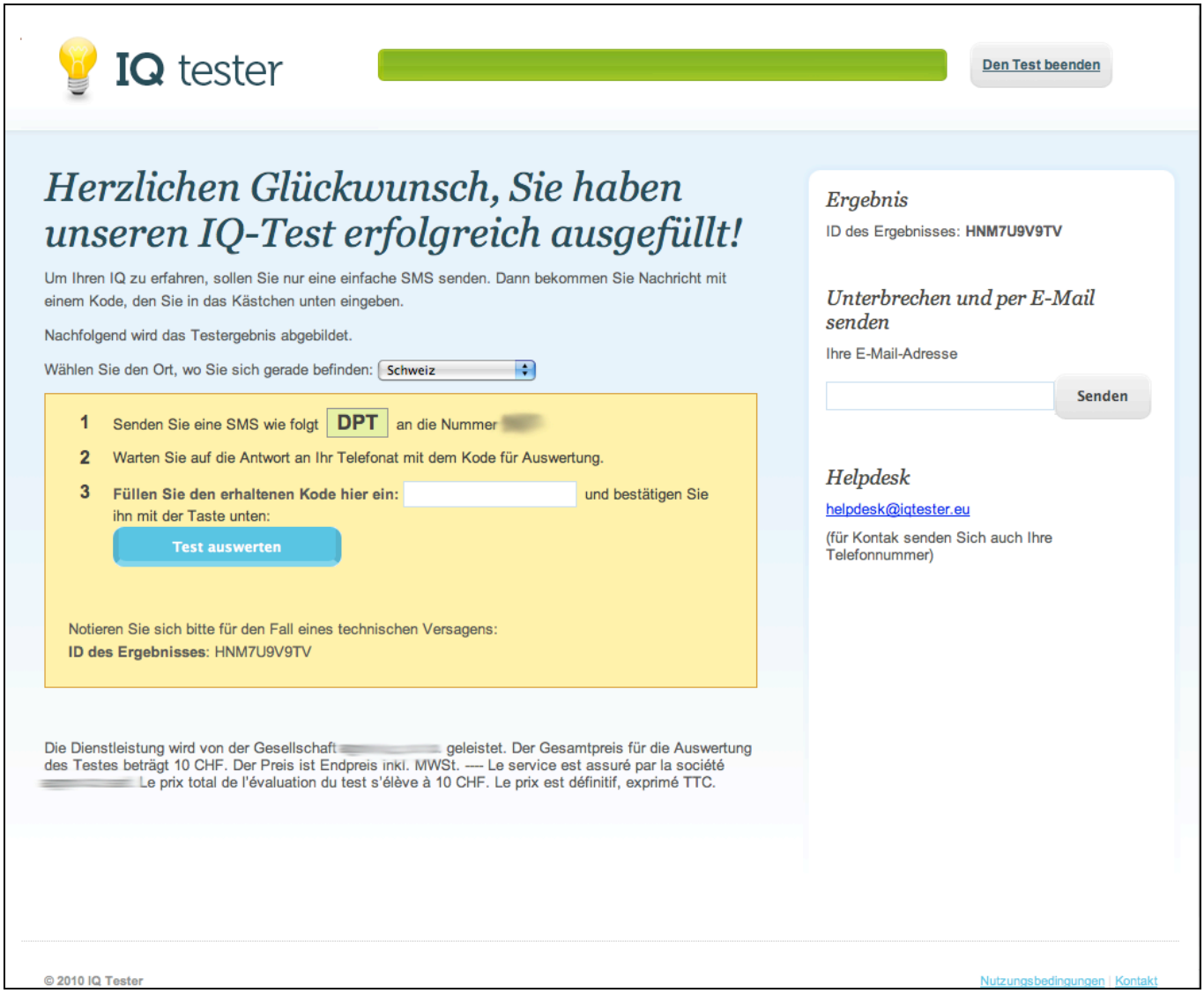
3) So allgemein, wie das Vorgehen beschrieben ist, muss man zuerst eine Unterscheidung treffen. Es gibt viele kostenlose Software im Internet, deren Download legal und unproblematisch ist. Besonders vorsichtig sollten Sie sein, wenn kostenpflichtige Software zu unrealistisch billigen Preisen oder sogar ganz kostenlos angeboten wird. In der Regel sind solche Angebote illegal, weil es sich meistens um gestohlene, beziehungsweise geknackte, Software handelt. Das heisst, Sie befinden sich bereits auf einer Webseite mit unseriösen Inhalten. Dass dabei die Gefahr, dass Sie eine bösartige Software herunterladen, besonders gross ist, sollte offensichtlich sein. Wenn es sich auf der Webseite beispielsweise um geknackte Programme handelt, so ist es ohne weiteres denkbar, dass die Betreiber der Webseite nicht nur den Kopierschutz entfernt, sondern auch noch bösartigen Code ins Programm eingebaut haben.

4) Der Grundgedanke, Anmeldeinformationen nur über verschlüsselte Verbindungen einzugeben, ist richtig. Es ist nun leider so, dass es nicht bei allen Webseiten erkennbar ist, dass die Übertragung tatsächlich verschlüsselt passiert. Wenn Sie bei einer Webseite eine Eingabe machen können oder müssen, so füllen Sie ein Formular aus. Sobald Sie die Eingabe mit einem Klick abschliessen, werden die eingegeben Informationen an den entsprechenden Server übermittelt. Dies geschieht, indem eine URL aufgerufen wird, der die Informationen beigefügt werden. Wichtig ist, dass diese Übermittlung verschlüsselt geschieht. Sie können das überprüfen, indem Sie in Ihrem Browser den *Quelltext* der Seite anzeigen lassen und darin nach *https://* suchen. Wird der Suchtext gefunden, so geschieht die Übertragung verschlüsselt und Sie können Ihre Daten beruhigt eingeben.

Lösungen zu den Kontrollfragen Kapitel 5

1) Die Seite enthält keine Hinweise darauf, dass Sie sich zu irgendwelchen Zahlungen verpflichten. Sie müssen auch keine privaten Daten eingeben. Insofern ist das Starten des IQ-Test unbedenklich.

   Etwas anders sieht es aus, wenn Sie die Fragen beantwortet haben. Dann erscheint nämlich folgende Seite:



   Hier werden Sie aufgefordert, ein SMS an eine bestimmte Nummer zu schicken. Erst dann erhalten Sie einen Code, um die Auswertung des Tests anzuzeigen. Im Kleingedruckten steht ausserdem, dass Sie das Ganze 10.- Franken kostet.

2) nItRaMrEiEm Dieses Passwort kann nicht als sicher angesehen werden. Es ist zwar ausreichend lang, entspricht aber dem Namen *Martin Meier*.

   5Z=3.r4 Dieses Passwort ist ebenfalls nicht sicher. Die Zeichenfolge ist zwar schwierig zu erraten, aber mit nur 7 Zeichen ist es zu kurz.

   iwi3.S,gdaK Dieses Passwort ist ziemlich sicher. Mit 11 Zeichen ist es genügend lang, die Zeichenfolge ist schwierig zu erraten, aber leicht zu merken;

sie besteht aus den Anfangsbuchstaben und den Satzzeichen des Satzes "*ich wohne im 3. Stock, gegenüber der alten Kirche*".

&.rg:67?rKD Dieses Passwort ist ebenfalls ziemlich sicher. Mit 11 Zeichen ist es ausreichend lang und die Zeichenfolge ist schwierig zu erraten. Leider ist es auch schwierig, sich die Folge zu merken. Damit ist die Gefahr gross, dass man sich das Passwort aufschreibt, wodurch es wieder deutlich weniger sicher wird.

3) Der Hauptvorteil dieser Massnahmen ist, dass ihr Browser weniger Informationen über Ihr Surfverhalten preisgeben kann. Dadurch dass der Browser keine Kopien von (Teilen von) Webseiten speichert, verringern Sie das Risiko, dass bösartiger Code auf ihren Computer gelangt.

   Ein Nachteil ist, dass Sie auch bei besuchten Webseiten (sofern Sie sie nicht zu den Lesezeichen hinzugefügt haben) die URL immer wieder vollständig eintippen müssen und der Browser Ihnen keine Vorschläge machen kann. Das Löschen der Cookies bewirkt, dass sich eine Webseite nicht an Sie erinnert und Sie somit jedes Mal wie einen neuen Besucher behandelt.

   Beachten Sie, dass sich die meisten Browser auch merken können, bei welchen Seiten Sie sich mit welchem Benutzernamen angemeldet haben. Diese Informationen werden mit den erwähnten Massnahmen nicht gelöscht.

Lösungen Kapitel 6

1) Eine Firewall auf dem Computer zu installieren ist sinnvoll, aber nicht immer unbedingt nötig. Wenn Ihr Computer über einen DSL Router mit dem Internet verbunden ist und sich im gleichen Subnetz keine weiteren Computer befinden, so genügt in der Regel die im Betriebssystem integrierte Firewall. Diese sollte aber unbedingt eingeschaltet sein. Wenn Sie über ein Kabelmodem ins Internet gehen oder mehrere Computer im selben Subnetz sind, ist eine Firewall nötig.

2) Wenn eine Firewall gar keine eingehenden Verbindungen erlaubt, können Sie mit Ihrem Computer nicht mehr in Internet, weil alle Antworten blockiert werden. Eine Firewall sollte so konfiguriert sein, dass nur eingehende *Verbindungsanfragen* blockiert werden. Ausgehende Verbindungen können grundsätzlich erlaubt werden, es ist aber ratsam auch hier eine gewisse Kontrolle zu führen und Verbindungen nur für bekannte Programme zu erlauben.

3) Wenn Ihre Firewall so eingestellt ist, dass Sie zuerst einwilligen müssen, wenn ein unbekanntes Programm eine Verbindung mit dem Internet herstellen will, kann eine Firewall tatsächlich bei der Entdeckung von Malware helfen.

Lösungen Kapitel 7

Base64 Entschlüsselung

Zeichen	**<Nullbyte>**								**c**								**l**							
ASCII	0								99								108							
Byte	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	0	1	1	0	1	1	0	0
Binär	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	1	0	1	1	0	1	1	0	0
Zahl	0								6				13				44							
Code	**A**								**G**				**N**				**s**							

Zeichen	**a**								**u**								**d**							
ASCII	97								117								100							
Byte	0	1	1	0	0	0	0	1	0	1	1	1	0	1	0	1	0	1	1	0	0	1	0	0
Binär	0	1	1	0	0	0	0	1	0	1	1	1	0	1	0	1	0	1	1	0	0	1	0	0
Zahl	24								23				21				36							
Code	**Y**								**X**				**V**				**k**							

Zeichen	**i**								**a**								**@**							
ASCII	105								97								64							
Byte	0	1	1	0	1	0	0	1	0	1	1	0	0	0	0	1	0	1	0	0	0	0	0	0
Binär	0	1	1	0	1	0	0	1	0	1	1	0	0	0	0	1	0	1	0	0	0	0	0	0
Zahl	26								22				5				0							
Code	**a**								**W**				**F**				**A**							

Zeichen	**s**								**c**								**h**							
ASCII	115								99								104							
Byte	0	1	1	1	0	0	1	1	0	1	1	0	0	0	1	1	0	1	1	0	1	0	0	0
Binär	0	1	1	1	0	0	1	1	0	1	1	0	0	0	1	1	0	1	1	0	1	0	0	0
Zahl	28								54				13				40							
Code	**c**								**2**				**N**				**o**							

Zeichen	**u**								**l**								**e**							
ASCII	117								108								101							
Byte	0	1	1	1	0	1	0	1	0	1	1	0	1	1	0	0	0	1	1	0	0	1	0	1
Binär	0	1	1	1	0	1	0	1	0	1	1	0	1	1	0	0	0	1	1	0	0	1	0	1
Zahl	29								22				49				37							
Code	**d**								**W**				**x**				**l**							

Zeichen	**.**								**c**								**h**							
ASCII	46								99								104							
Byte	0	0	1	0	1	1	1	0	0	1	1	0	0	0	1	1	0	1	1	0	1	0	0	0
Binär	0	0	1	0	1	1	1	0	0	1	1	0	0	0	1	1	0	1	1	0	1	0	0	0
Zahl	11								38				13				40							
Code	**L**								**m**				**N**				**o**							

Zeichen	**<Nullbyte>**								**t**								**r**							
ASCII	0								116								114							
Byte	0	0	0	0	0	0	0	0	0	1	1	1	0	1	0	0	0	1	1	1	0	0	1	0
Binär	0	0	0	0	0	0	0	0	0	1	1	1	0	1	0	0	0	1	1	1	0	0	1	0
Zahl	0								7				17				50							
Code	**A**								**H**				**R**				**y**							

Zeichen	**s**								**8**								**0**							
ASCII	115								56								48							
Byte	0	1	1	1	0	0	1	1	0	0	1	1	1	0	0	0	0	0	1	1	0	0	0	0
Binär	0	1	1	1	0	0	1	1	0	0	1	1	1	0	0	0	0	0	1	1	0	0	0	0
Zahl	28								51				32				48							
Code	**c**								**z**				**g**				**w**							

Zeichen	**C**								**6**								**4**							
ASCII	67								54								52							
Byte	0	1	0	0	0	0	1	1	0	0	1	1	0	1	1	0	0	0	1	1	0	1	0	0
Binär	0	1	0	0	0	0	1	1	0	0	1	1	0	1	1	0	0	0	1	1	0	1	0	0
Zahl	16								51				24				52							
Code	**Q**								**z**				**Y**				**0**							

Wir erhalten die E-Mail Adresse *claudia@schule.ch* und das Passwort *trs80C64*.

Reaktion eines Antiviren Programms, wenn die Testfolge direkt im Mailinhalt steht

Da der Mailinhalt als reiner Text aufgefasst wird (unabhängig davon, ob er als normaler Text oder in HTML Code eingebettet erscheint) wird die E-Mail als unbedenklich eingestuft.

Anhang B

Eicar - Eine harmlose Virentest–Datei

Vielleicht haben Sie sich schon gefragt, ob Ihr Antiviren Programm auch tatsächlich eingreifen würde, wenn ein Virus auf Ihren Computer gelangen möchte. Da diese Frage auch für professionelle Systembetreuer wichtig ist, gibt es eine Organisation, die eine Zeichenfolge definiert hat, die harmlos ist, aber von Herstellern von Antiviren Programmen als Virus identifiziert wird. Speichert man diese Zeichenfolge in einer Datei, so sollte ein Antiviren Programm diese Datei wie eine tatsächlich infizierte Datei behandeln.

Die Antiviren Testdatei findet man unter http://www.eicar.org/anti_virus_test_file.htm

Die Zeichenfolge besteht aus genau 68 Zeichen (68 Bytes) und lautet

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

Auf der angegebenen Webseite stehen Testdateien in verschiedenen Formaten zum Herunterladen bereit. Das Herunterladen kann allerdings unter Umständen schwierig sein. Da die Dateien von einem Antiviren Programm ja als infizierte Dateien angeschaut werden, sollte Ihr Antiviren Programm Alarm schlagen, wenn Sie versuchen die Datei herunter zu laden.

Als Ausweg steht Ihnen die Möglichkeit offen, eine Testdatei selbst zu erstellen, indem Sie in einem einfachen Texteditor die entsprechende Zeichenfolge eingeben und die Datei speichern. Beachten Sie, dass Sie einen Editor verwenden, der keine zusätzlichen Informationen speichert. Die Datei sollte wirklich nur gerade aus diesen 68 Bytes bestehen.

Es empfiehlt sich auch, den Begleittext auf der Webseite zu lesen.

Die Datei eignet sich gut um zu testen, ob und wann ein Antivirenprogramm reagiert. Wenn man beispielsweise die oben abgebildete Zeichenfolge in einem Editor eintippt und das Dokument mit der Endung ".exe" speichert, so sollte ein Antivirenprogramm Alarm schlagen. Speichert man das Dokument mit der erweiterung ".txt", so reagieren Antivirenprogramme unterschiedlich. Man kann auch versuchen, ein E-Mail mit der Datei im Anhang zu verschicken und prüfen, ob die Mail ankommt oder schon vorher vom Antivirenprogramm des Providers entfernt wird.