orell füssli

Norbert Pohlmann / Markus Linnemann

Sicher im Internet

Tipps und Tricks für das digitale Leben

Sicher im Internet
Norbert Pohlmann
Markus Linnemann
orell füssli

Ein Projekt vom Institut für Internet-Sicherheit:

securityNews: Kostenlose App für mehr Sicherheit im Netz

- Kostenlose App vom Institut für Internet-Sicherheit
- Aktuelle Sicherheitshinweise für Smartphone, Tablet, PC und Mac
- Warnung vor Sicherheitslücken in Standardsoftware, dank BSI-Schwachstellenampel
- Konkrete Anweisungen für Privatanwender und Unternehmen

» www.it-sicherheit.de

Available on the App Store

ANDROID APP ON Google play

Mit freundlicher Unterstützung

Bundesamt für Sicherheit in der Informationstechnik

Norbert Pohlmann/Markus Linnemann

Sicher im Internet
Tipps und Tricks
für das digitale Leben

Teil 2: Basisschtutz – das 1 x 1
für einen sicheren Computer

orell füssli Verlag AG

Basisschutz – das 1 x 1 für einen sicheren Computer

Ein intelligenter Mann namens Albert Einstein sagte einmal: «Die Welt wird nicht bedroht von Menschen, die böse sind, sondern von denen, die das Böse zulassen.» Ein Angreifer geht in der Regel den Weg des geringsten Widerstands – auch im Internet. Das bedeutet, dass ein pauschaler Angriff als Erstes bei solchen Computern gelingt, die gar nicht oder nur unzureichend geschützt sind. Doch bereits ein Basisschutz genügt, um die meisten Angriffe aus dem Internet erfolgreich abzuwehren und seinen «Verbraucherpflichten» (siehe Seite 170 ff.) als Internetnutzer Genüge zu tun. Vergleichen können Sie den Basisschutz mit Ihrem Verhalten im realen Leben, wenn Sie das Haus verlassen: Sie lassen die Rollläden herunter, schließen Fenster und Türen und schalten – soweit vorhanden – die Alarmanlage ein. Im digitalen Leben ist der Basisschutz genauso leicht herzustellen. Zum Basisschutz gehören der aktive Einsatz von einem Anti-Malware-Programm und einer Personal Firewall sowie die Nutzung des automatischen Updates von dem Betriebssystem und den Anwendungsprogrammen. Außerdem sind die Verwendung von Anti-Spyware-Programmen, die Durchführung von regelmäßigen Back-ups und der gesunde Menschenverstand Sicherheitsmechanismen des Basisschutzes. Die in diesem Kapitel beschriebenen Regeln bilden die Grundlage für alle folgenden Tipps und sollten daher unbedingt beachtet werden.

Grundlegende Sicherheitseinstellungen – Malware-Scanner & Co.

Das Leben eines Computers beginnt mit der Installation. Das Betriebssystem ist normalerweise vollständig frei von Viren, Würmern, Trojanischen Pferden, Spyware und anderer Schadsoftware, aber nur unzureichend geschützt. Als Nutzer müssen Sie deshalb einige Sicherheitsmechanismen installieren, bevor Sie den Computer mit dem Netzwerk – dem Internet – verbinden. Anderenfalls ist er vielleicht schon manipuliert oder unter der Kontrolle von Angreifern, bevor das eigentliche «Abenteuer Internet» beginnt.

Anti-Malware-Programme

Der erste Schritt besteht immer darin, ein aktuelles Sicherheitsprogramm auf dem Computer zu installieren, das Schadsoftware wie Viren, Würmer und Trojanische Pferde abwehrt. Es ist das effizienteste Mittel gegen Gefahren aus dem Internet. Die bekanntesten Vertreter der Schadsoftware sind:

- *Viren* können sich selbst unbemerkt in andere Programme kopieren und zu einem definierten Zeitpunkt meist zerstörerische Aktivitäten im Computer ausführen.
- *Würmer* nutzen Schwachstellen in der Software oder Konfiguration eines Computers aus und verbreiten sich selbstständig im Internet von Computer zu Computer.
- Ein *Trojanisches Pferd* gibt vor, ein legitimes Programm zu sein oder versteckt sich möglichst geschickt im Computer, um dann schädliche Funktionen auszuführen.
- Unter einem *Bot* wird unter anderem eine flexible, meist ferngesteuerte Schadsoftware verstanden, die durch Viren

> oder Würmer auf einem Computer installiert wurde. Die mit «böswilligen» Bots infizierten Computer werden unter der Kontrolle eines Angreifers in Botnetzen zusammengefasst. Diese Botnetze werden beispielsweise für den Versand von Spam oder für zielgerichtete Angriffe benutzt und stellen eine sehr große Gefahr dar (Softlink 210).

Für die notwendigen Sicherheitsprogramme wurde der Name «Anti-Virus» geprägt. Ein veralteter Begriff, da zu den Angreifern – wie gerade gezeigt – nicht nur die erwähnten Viren, sondern auch andere Schadprogramme zählen, die als «Malware» bezeichnet werden. Daher ist es besser, von Anti-Malware-Programmen zu sprechen.

Das Anti-Malware-Programm prüft im Hintergrund fortlaufend die Kommunikation mit dem Internet und die Aktivitäten des Computers im Hinblick auf besagtes Ungeziefer. In regelmäßigen Abständen kontrolliert es mit einem sogenannten Scan die Festplatte. Anti-Malware-Programme müssen täglich aktualisiert werden, da sie sich in einem ständigen Wettlauf mit den Angreifern befinden. Wird eine neue Art von Schadsoftware gefunden, entwickeln die Anti-Malware-Hersteller ein «Gegenmittel» (Virensignaturen) und stellen es zum Download bereit. Per Update gelangt es dann auf den Computer. Das passiert zum Teil mehrmals täglich. Die automatischen Updates für das Anti-Malware-Programm müssen daher immer eingeschaltet beziehungsweise zugelassen sein. Berücksichtigen Sie das unbedingt bei der Grundinstallation des von Ihnen verwendeten Anti-Malware-Programms.

Bevor ein Computer erstmals mit dem Internet verbunden wird, sollte bereits ein Anti-Malware-Programm installiert sein. Neue Computer enthalten meist eine Testversion, die

Sie für den Anfang nutzen können. Falls nicht, sind die 20 bis 40 Euro, die ein entsprechendes Programm derzeit pro Jahr kostet, gut angelegt. Meist erhalten Sie dafür eine Security Suite, in der ein ganzes Programmpaket enthalten ist – in der Regel ein Anti-Malware–, Firewall- und Anti-Spyware-Programm sowie Anti-Spam-Programme und weitere direkt integrierte Sicherheitsfunktionen. Hier ist nur ein einziger Installationsvorgang notwendig (Softlink 225).

Aber im Internet sind auch freie Anti-Malware-Programme, wie beispielsweise die Sicherheitslösung AntiVir (Softlink 211), erhältlich. Dafür sollten Sie jedoch durchaus über ein gewisses Maß an fundierten Computerkenntnissen verfügen, da Sie die verschiedenen Anti-Malware-Programme einzeln installieren, zusammenstellen und konfigurieren müssen. AntiVir ist nur die Anti-Viren-Lösung, aber beispielsweise keine Firewall.

TIPP: Anti-Malware-Programme

- Gehen Sie niemals ohne Anti-Malware-Programm ins Internet.
- Einen guten Anhaltspunkt, welches Programm beziehungsweise welche Sicherheitslösung für Sie geeignet ist, bieten die jährlichen Tests der diversen Fachzeitschriften.
- Gehören Sie eher zu den Computer-Neulingen, ist ein kostenpflichtiges Anti-Malware-Programm (Security Suite) für Sie die bessere Wahl (Liste von Anti-Malware-Programmen, siehe Softlink 212).
- Installieren Sie das Anti-Malware-Programm auf Ihrem Computer, bevor Sie ihn das erste Mal mit dem Internet verbinden.
- Wollen Sie ein kostenloses Programm aus dem Internet verwenden, laden Sie es mit einem anderen, geschützten Computer herunter.

- Führen Sie unmittelbar nach der Installation des Anti-Malware-Programms ein Update durch (häufig per Rechtsklick auf das entsprechende Programmsymbol), um gleich auf dem neusten Stand zu sein.

Personal Firewall

Zur Veranschaulichung der Funktionsweise einer Firewall kann der Computer mit einem Haus, das viele Türen und Fenster hat, verglichen werden. Nicht jeder Zugang zum Haus wird die ganze Zeit benötigt: Die Haustür steht nicht ständig offen, sondern wird nur geöffnet, wenn jemand das Haus betreten oder verlassen möchte. Die Tür zum Garten wird verschlossen, wenn der Garten nicht benutzt wird. Beim Computer ist das ähnlich. Hier sollten ebenfalls nicht alle Türen zum Netzwerk beziehungsweise Internet, hier Ports genannt, die ganze Zeit uneingeschränkt zugänglich sein. Es wird also ein Wächter benötigt, der sich um den Datenverkehr vom und zum Internet kümmert. Diesen Job übernimmt die Personal Firewall. Sie sorgt dafür, dass nur bestimmte Ports geöffnet werden und sie kontrolliert auch, welche Programme auf dem Computer diese Ports nutzen. Viele dieser Sicherheitsaufgaben erledigen aktuell verfügbare Firewalls nach der Installation ganz selbstständig, aber in einigen Bereichen ist menschliche Hilfe notwendig.

Die Firewall hat die Angewohnheit, bei ihr unbekannten Aktivitäten nachzufragen, ob diese Aktivität – die eine Verbindung mit dem Internet herstellen möchte – erlaubt werden soll. Diese Fragen sollten Sie nicht einfach wegklicken, sondern sich die Zeit nehmen sie zu lesen, auch wenn es manchmal lästig ist. Dieses Vorgehen ist entschei-

dend für die Sicherheit. Wenn die Firewall beispielsweise beim Öffnen des Browsers fragt, ob sie das Programm zur Kommunikation mit dem Internet freigeben kann, ist das kein Problem, denn was bringt ein Browser ohne Internetzugang. Diese Berechtigung können Sie auch ohne Bedenken dauerhaft vergeben, indem Sie Ihre Antwort speichern (siehe Abbildung 1). Auf diese Weise werden die Nachfragen mit der Zeit immer weniger, weil die Firewall durch die Angaben «lernt». Meldet die Firewall hingegen beim Schreiben eines Briefes plötzlich, dass ein Programm auf dem Computer mit dem Internet kommunizieren möchte, sollten Sie genauer hinschauen. Denn abgesehen von einem automatischen Update, wie beispielsweise dem des Anti-Malware-Programms, gibt es hier eigentlich keinen nachvollziehbaren Grund für eine solche Verbindung.

Abbildung 1: Beispiele für Firewall-Meldungen

Allerdings sind die Nachfragen der Firewall manchmal leider sehr kryptisch und nicht so klar wie in Abbildung 1. Wenn die Meldung zum Beispiel darauf hinweist, dass «lsass.exe» eine Verbindung zum Internet herstellen möchte, weiß nicht jeder, was sich dahinter verbirgt. Um Klarheit zu schaffen, geben Sie die Meldung bei einer Suchmaschine wie bing oder Google ein. Im Regelfall haben auch schon andere Nutzer diese Meldung erhalten und wissen Rat. Können Sie nicht klären, was die Meldung zu bedeuten hat, verweigern Sie den Zugriff.

Die optimale Nutzung einer Firewall erfordert also schon etwas Fachwissen. Aber auch als Laie ist es möglich, eine Firewall wirkungsvoll zu betreiben. Denn fast alle Programme bieten einen Modus, der dem Nutzer viele Entscheidungen, die Fachwissen erfordern, abnimmt und zusätzliche Hilfestellung gibt. Eine einfache Firewall wird mit den Betriebssystemen Windows, Mac OS X und auch bei den Linux-Distributionen direkt mitgeliefert. Diese sind allerdings recht rudimentär gehalten. Daher ist es ratsam, eine zusätzliche Software zu verwenden. Es gibt auch kostenlose Personal-Firewall-Lösungen im Internet, zum Beispiel ZoneAlarm oder Comodo (Firewalls, siehe Softlink 213) – beide für Windows. Außerdem sind in den meisten Security Suiten Firewalls bereits enthalten.

TIPP: Personal Firewalls

- Verwenden Sie immer eine Personal Firewall auf Ihrem Computer.
- Bei Firewall-Meldungen, die Sie nicht einschätzen können oder bei plötzlichen Meldungen ohne eine vorherige Aktion von Ihnen, sollten Sie den Zugriff verweigern.

- Updates der Anti-Malware-Programme, des Browsers und des Betriebssystems sollten Sie auf jeden Fall (dauerhaft) zulassen.
- Anfragen, die Sie einem von Ihnen verwendeten Programm zuordnen können, sind in der Regel unproblematisch. Diese erscheinen oft in dem Moment, in dem Sie das entsprechende Programm starten, wie beispielsweise den Browser oder das E-Mail-Programm.

Automatische Updates

Eine effiziente Abwehr von Angriffen aus dem Internet ist nur möglich, wenn sich die Software auf dem Computer, also das ganze Softwaresystem mit allen Programmen, auf dem aktuellsten Stand befindet. Das gilt nicht nur für die Anti-Malware-Programme, sondern auch das Betriebssystem sollte stets up to date sein. Das bedeutet jedoch nicht, dass Sie immer gleich das allerneuste Betriebssystem kaufen müssen. Jedoch sollte das von Ihnen verwendete Betriebssystem vom Hersteller noch unterstützt werden, das heißt, es sollten regelmäßige Updates verfügbar sein. So gibt es bei Erscheinen dieses Buches beispielsweise noch Updates für Windows XP, Vista und natürlich Windows 7, aber nicht mehr für Windows 98. Und ab Juli 2010 wird auch Windows 2000 nicht mehr mit Sicherheitsupdates unterstützt. Windows 98 sollte für einen internetfähigen Computer deshalb auf keinen Fall mehr verwendet werden. Das gilt auch für ältere Versionen von Mac OS (unter Mac OS 9) und Linux (abhängig von der jeweiligen Distribution). Der Hintergrund ist folgender: Ein Softwareprogramm besteht aus Codezeilen. Windows als Betriebssystem zum Beispiel enthält mehrere Millionen Zeilen Programmcode. Da ist es ganz normal, dass sich die Program-

mierer auch einmal «verschreiben» und sich so Fehler einschleichen – das trifft in gleichem Maße auch auf Linux oder ein Apple-Betriebssystem zu. Und eben diese Fehler sind in der Regel die Einfallstore für Angreifer. Daher programmieren die Entwickler der Softwarehersteller sogenannte «Patches», um gefundene Fehler zu beheben, und der Computer bekommt diese regelmäßig über die automatischen Updates. Diese sollten also unbedingt aktiviert sein! Bei Windows XP zeigt das Sicherheitscenter an, ob sie eingeschaltet sind, bei Windows 7 findet sich diese Einstellung unter «Windows Update»(Einstellungen von Ubuntu und Mac OS X, siehe Softlink 214). Beides finden Sie jeweils in der Systemsteuerung. In Abbildung 2 sind die automatischen Updates nicht aktiviert. Diese Einstellung sollte umgehend mit der Auswahl «Updates automatisch installieren» korrigiert werden.

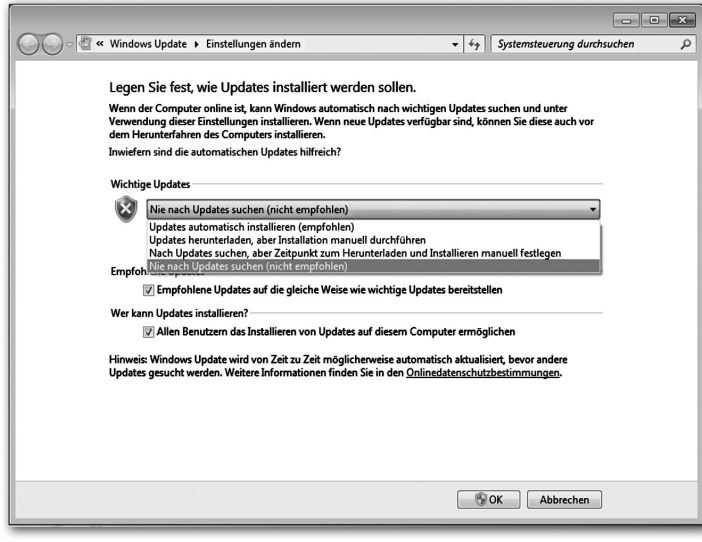

Abbildung 2: Sicherheitscenter unter Windows, das nicht optimal konfiguriert ist

Bei einer potenziellen Gefährdung weist Windows mit einer Warnmeldung auf das Sicherheitsproblem hin, wie in Abbildung 3 zu sehen ist. Das Warnsymbol befindet sich in der Taskleiste. Hier sollten Sie immer sofort reagieren!

Abbildung 3: Warnsymbol von Windows, das auf ein Sicherheitsproblem hinweist

Ein Doppelklick auf das Warnsymbol (bei Windows XP ein rotes Schild) bringt Sie direkt in die Sicherheitseinstellungen (siehe Abbildung 2), wo Sie alle notwendigen Schutzmaßnahmen aktivieren und optimieren können (Firewall, automatische Updates und Virenschutz).

TIPP: Automatische Updates

- Schalten Sie die automatischen Updates Ihres Betriebssystems immer ein.
- Verwenden Sie, soweit es angeboten wird, auch bei allen anderen installierten Programmen die Updatefunktion, zum Beispiel beim Browser (besonders wichtig!).

Anti-Spyware-Programme

Sicherheitstechnisch noch besser aufgestellt ist, wer Anti-Spyware-Programme einsetzt. Diese verhindern, dass Informationen vom eigenen Computer an Dritte gesendet werden. Denn auch einige «normale» Programme haben die Ange-

wohnheit – zum Beispiel zu Werbezwecken –, Informationen an ihre Hersteller zu senden. Dass das natürlich auch für Schadsoftware gilt, versteht sich von selbst. Daher sind diese Anti-Spyware-Programme eine sinnvolle Ergänzung zum Basisschutz. Auch hier gibt es freie Software für den Heimanwender im Internet wie Spybot – Search & Destroy (Softlink 215) oder Ad-Aware (Softlink 216). Die Programme verrichten ihren Dienst größtenteils vollkommen selbsttätig. In den meisten Security Suiten sind Anti-Spyware-Programme ebenfalls enthalten.

Regelmäßige Back-ups

Alle Daten weg? Alle Filme, Fotos, Lieder und persönlichen Dokumente im Computer-Nirvana? Eine Horrorvorstellung für jeden Nutzer, denn die Dateien auf dem Computer sind in der Regel ein wertvolles Gut, und ihr Verlust kann einen hohen ideellen und auch finanziellen Schaden bedeuten. Nicht selten löst sich so die Arbeit von Stunden, Tagen oder sogar Monaten innerhalb von wenigen Sekunden in Luft auf. Das haben schon viele Studenten beim Schreiben der Abschlussarbeit leidvoll erleben müssen.

Datenverluste können zum Beispiel durch einen Defekt der Festplatte auftreten, da diese nur eine begrenzte Lebensdauer besitzt. Aber auch Fehler in Anwendungsprogrammen, Malware oder eine Fehlbedienung können der Grund für einen solchen Verlust von Dateien sein. Aber dieses Horrorszenario können Sie sehr einfach verhindern – mit regelmäßigen Back-ups!

Ein Back-up ist eine Kopie von bestimmten, auf der internen Festplatte gespeicherten Dateien auf einem anderen

Speichermedium. Tritt dann ein Defekt auf, können verloren gegangene Dateien vom Back-up wieder zurückgespielt und verfügbar gemacht werden. Und das Beste: Es ist gar nicht schwierig, ein Back-up zu erstellen, und der Vorgang kann sogar automatisiert werden.

Die einfachste Möglichkeit ist die Verwendung einer externen Festplatte oder eines USB-Sticks mit genügend freiem Speicherplatz. Perfekt ist, wenn das Back-up-Medium nur während des Back-up-Vorgangs an die Stromversorgung angeschlossen ist. So stellen Sie sicher, dass das Back-up auch dann noch funktioniert, wenn beispielsweise ein elektronischer Schaden durch einen Blitz oder eine Spannungsspitze entsteht. Zusätzlich schützt es Sie vor Erpressung. Es gibt Angreifer, die eine Malware installieren, welche die Festplatte des betroffenen Computers verschlüsselt, und dann Geld fordern, damit sie die Daten wieder lesbar machen. Auf dem Back-up-Medium wären die Daten nach wie vor für Sie verfügbar, und Sie könnten den befallenen Computer problemlos neu installieren.

Darüber hinaus ist es möglich, Back-ups im Internet anzulegen, auf sogenannten Onlinefestplatten. Dafür ist allerdings eine schnelle Internetverbindung nötig. Zudem stellt sich hierbei immer die Vertrauensfrage, da die Anbieter theoretisch jederzeit Einblick in die gespeicherten Dateien nehmen können. Eine mit SSL/TLS verschlüsselte Verbindung zur Datenübertragung sollte bei solchen Angeboten eine Selbstverständlichkeit sein (siehe Seite 36 ff.). Sie sehen, auch hier ist Vorsicht geboten!

In den aktuellen Betriebssystemen wie Mac OS X (Time Machine) und Windows Vista beziehungsweise Windows 7 sind bereits Back-up-Programme enthalten – ebenso wie in

den meisten Security Suiten –, sie können jedoch auch extra erworben werden. Freie Programme, wie beispielsweise Cobian Backup (Softlink 217), leisten aber genauso zuverlässige Dienste. Außerdem sind im Handel externe Festplatten erhältlich, denen ebenfalls ein Back-up-Programm beiliegt, sodass Sie Ihre Daten teilweise per Knopfdruck sichern können. Sind auf Ihrem Computer sensible Daten gespeichert, sollten Sie USB-Sticks oder Festplatten benutzen, die Ihre Dateien automatisch verschlüsseln. Das hat den Vorteil, dass bei einem Diebstahl die Daten nicht ohne Weiteres von jedem gelesen werden können («Datenverschlüsselung mit TrueCrypt» – Fortgeschrittenen-Workshop, siehe Softlink 218).

TIPP: Back-ups

- Führen Sie regelmäßig(!) Back-ups auf externe Speichermedien (zum Beispiel externe Festplatten, USB-Sticks, DVDs, CDs) durch.
- Ein Back-up-Medium gehört genauso zum Computer wie der Monitor. Planen Sie es deshalb bereits beim Kauf mit ein und sparen Sie nicht am falschen Ende – dem Schutz Ihrer Daten.
- Die zeitlichen Abstände richten sich nach der Menge und der Wichtigkeit der hinzukommenden Dateien. Bei regelmäßigem privatem Gebrauch ist einmal pro Woche eine sinnvolle Frequenz.
- Bewahren Sie die externen Back-up-Speichermedien an einem sicheren Ort auf.
- Bei besonders wertvollen Daten sollten Sie zwei Back-ups pflegen und örtlich getrennt aufbewahren.
- Bei sicherheitskritischen Daten empfiehlt es sich, die Back-up-Daten auf externen Medien zu speichern, die diese automatisch verschlüsseln.

Surfen als eingeschränkter Nutzer

Malware kann besonders großen Schaden anrichten, wenn sie die Berechtigung hat, auf viele Dateien im Computer zuzugreifen. Alle aktuellen Betriebssysteme bieten nicht zuletzt deshalb die Möglichkeit, die Rechte des Nutzers einzuschränken – und verwenden diese Einstellung standardmäßig. Das sollten Sie auf jeden Fall so handhaben (insbesondere wenn Sie im Internet surfen), da dieser Modus des «eingeschränkten Nutzers» die Angriffsfläche für Malware erheblich verringert. Administrator-Rechte – je nach Betriebssystem auch Root-Rechte genannt –, die es dem Nutzer erlauben, alle Einstellungen zu verändern und auf alles zuzugreifen, benötigen Sie nur zur Installation oder anderen systemrelevanten Vorgängen. Und für diesen Fall können Sie vom eingeschränkten Nutzer mittels einer entsprechenden Bestätigung jederzeit kurzfristig zum Administrator werden (Administrator

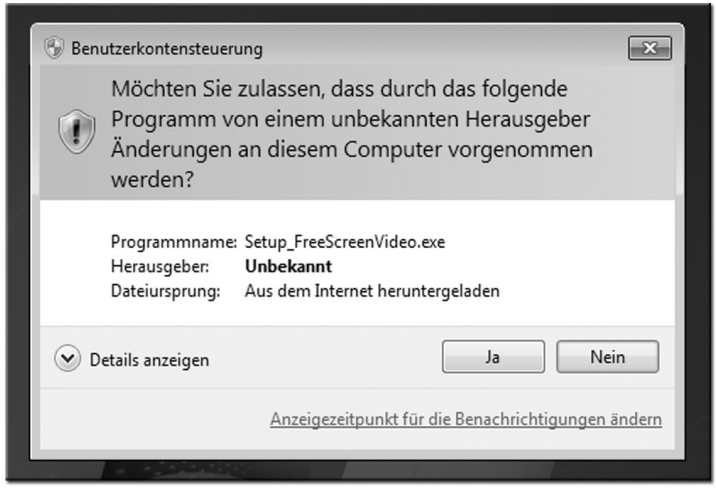

Abbildung 4: Windows-Dialogfeld, das nach Administrator-Rechten fragt

vs. eingeschränkter Nutzer, siehe Softlink 219). Windows 7, Windows Vista, Ubuntu und Mac OS X behandeln den Anwender grundsätzlich als eingeschränkten Nutzer. Wenn Administrator- oder Root-Rechte erforderlich sind, öffnet sich ein Dialog, der eine Bestätigung und je nach Betriebssystem und Einstellung ein Passwort erwartet (siehe Abbildung 4). Wird also die Nachfrage nach Administrator-Rechten gestellt, sollten Sie dies nur zulassen, wenn auch ein Grund dafür vorliegt, wie zum Beispiel die aktive und bewusste Installation eines Programms.

TIPP: Eingeschränkter Nutzer

- Surfen Sie nicht als Administrator beziehungsweise mit Root-Rechten.
- Nutzen Sie die Funktion des eingeschränkten Nutzers.

Gesunder Menschenverstand

Der wichtigste Schutz im digitalen Leben ist aber der gesunde Menschenverstand. Im realen Leben sagt uns dieser, dass wir die Haustür beim Verlassen des Hauses besser abschließen, unseren Geldbeutel nicht offen herumtragen, uns von dunklen Ecken fernhalten und uns beim Autofahren anschnallen. Im Umgang mit Computer und Handy müssen wir vergleichbare Verhaltensweisen erst entwickeln – doch das braucht Zeit. Zeit, die Sie sich aber unbedingt nehmen sollten, da das Wissen um die Gefahren und die daraus abgeleiteten Automatismen für Ihren Schutz im Internet entscheidend sind.
Als Internetnutzer dürfen Sie nicht «blind» surfen. Stellen Sie sich vor, ein Fremder kommt auf der Straße auf Sie zu und bietet Ihnen 1.000 Euro als Geschenk an – da werden Sie

doch misstrauisch. Wenn Ihnen ein Link im Internet verspricht, dass Sie mit einem Klick 1.000 Euro gewinnen können, sollten Sie ebenso misstrauisch werden. Denn niemand verschenkt einfach so 1.000 Euro!

Das größte Sicherheitsproblem eines Computers ist oftmals der Mensch, der davor sitzt. Die Ausnutzung «menschlicher Schwächen» wird in Fachkreisen «Social Engineering» oder «Social Hacking» genannt. Wenn Ihnen also jemand ohne Grund einen USB-Stick schenkt, seien Sie besser auf der Hut. Denn entweder handelt es sich um einen außergewöhnlich netten Menschen oder aber – was sehr viel wahrscheinlicher ist – um einen Betrüger, der darauf hofft, dass Sie das von ihm auf dem USB-Stick platzierte Trojanische Pferd auf Ihrem Computer ausführen und ihm so Zugriff auf Ihre Daten ermöglichen. Der Einsatz Ihres gesunden Menschenverstandes ist Ihre beste Waffe im Kampf gegen «das Böse» und damit Ihr bester Schutz.

Das gilt insbesondere auch bei Scareware. Als Scareware werden Programme bezeichnet, die darauf abzielen, den Nutzer zu verunsichern, sodass er aus Angst eine bestimmte Handlung vornimmt. Beispielsweise werden im Internet falsche Anti-Malware-Tools angeboten, die ganz viele Probleme auf Ihrem Computer melden, die Sie mit einer entsprechenden Software – die Ihnen gleich zum Kauf angeboten wird – beheben könnten. In Wahrheit werden aber einfach nur die falschen Warnungen abgestellt. Eine andere Masche der Betrüger sind Online-Malware-Scanner, die fälschlicherweise behaupten, dass sich Malware auf dem Computer befindet. Um das zu beheben, wird dazu aufgefordert, einen bestimmten Link anzuklicken. Dieser führt dann zu einer infizierten Webseite und bringt so die Malware auf den Com-

puter. Das Gleiche wird auch mit Programmen versucht, die vom Nutzer direkt aus dem Internet heruntergeladen werden sollen, um die angeblich gefundene Malware zu neutralisieren. Doch genau das Gegenteil ist der Fall: Die Malware wird von diesen Programmen erst installiert.

TIPP: Gesunder Menschenverstand

- Fallen Sie nicht auf unrealistische Sonderangebote und Versprechungen im Internet herein.
- Deinstallieren Sie Programme, die Sie nicht mehr benötigen. Weniger Programme bedeuten weniger Angriffsfläche für Malware.
- Verwenden Sie fremde USB-Sticks (und andere Speichermedien) nur, wenn Sie aus einer vertrauenswürdigen Quelle stammen.
- Lassen Sie sich von Scareware nicht zu voreiligen Handlungen verleiten. Im Zweifelsfall tun Sie besser nichts und holen den Rat eines Experten ein. Generell gilt im Internet: Sind Sie sich nicht sicher, unterlassen Sie die jeweilige Aktivität besser!
- Überprüfen Sie einen angebotenen Link im Web, bevor Sie einfach darauf klicken (siehe Seite 29f.).

Der Internetbrowser – sinnvoll einstellen, sinnvoll nutzen

Der Internetbrowser ist Ihr Tor zur digitalen Welt und das wichtigste Hilfsmittel, um im World Wide Web Informationen zu sammeln, Bankgeschäfte zu erledigen, einzukaufen, mit Freunden zu chatten, Zeitung zu lesen oder zu spielen. Diese Liste ließe sich fast endlos weiterführen. Gerade deshalb ist es

so wichtig, dass Sie einerseits einen sicheren Browser verwenden, andererseits aber auch wissen, wie dieser funktioniert und wie Sie ihn zu bedienen haben.

Erhältlich sind derzeit mehrere Browser von verschiedenen Herstellern. Von Vorteil ist, dass sie im Normalfall kostenlos angeboten werden. Sie haben also die Qual der Wahl, welchen Browser Sie verwenden wollen, oder Sie nutzen mehrere im Wechsel. Die bekanntesten und am häufigsten verwendeten Browser sind (in alphabetischer Reihenfolge):

- Google Chrome
- Mozilla Firefox
- Opera
- Safari
- Windows Internet Explorer

In der Linux-Welt gibt es noch zusätzliche Ableger, beispielsweise den Konqueror.

Der Begriff Browser kommt, wie die meisten Begriffe in der Informatik, aus dem Englischen und heißt so viel wie «umschauen» oder «schmökern». Und genau das lässt sich mit allen genannten Vertretern wunderbar erledigen. Das Anzeigen von Webseiten ist die wichtigste Funktion des Browsers. Früher gab es hier bereits die ersten Probleme, da die unterschiedlichen Browser die Webseiten auf verschiedene Arten darstellten, um sich voneinander abzuheben. Heute halten sich die Browserhersteller im Großen und Ganzen an die Vorgaben des W3C (**W**orld **W**ide **W**eb **C**onsortium). In diesem Konsortium sind alle wichtigen Firmen vertreten, um Standards für das Web zu erarbeiten und umzusetzen.

Mittlerweile gehen die Fähigkeiten eines Browsers aber weit über das reine Darstellen von Webseiten hinaus. Mit unterschiedlichen Technologien können die Browser auch PDF-Dateien anzeigen, Musik abspielen und animierte Inhalte darstellen.

Dieser Abschnitt stellt einen typischen Browservertreter mit seinen wichtigsten Funktionen vor und erläutert die sicherheitsrelevanten Aspekte bei der Nutzung im Internet. Anhand des flexiblen Open-Source-Browsers Firefox der Mozilla Foundation wird gezeigt, wie Sie Ihren Browser schon mit kleinen Eingriffen sehr gut absichern können, beziehungsweise wie der Browser Sie in Sicherheitsthemen unterstützen kann. Firefox wird gleichermaßen für Windows, Mac OS und Linux angeboten. Open Source bedeutet, dass die Programme, genauer gesagt deren Programmcodes, offen einsehbar sind und dass die Software kostenfrei genutzt werden kann.

Der Aufbau eines Browsers

Jeder Internetnutzer kennt einen Browser. Doch um die richtigen (Sicherheits-)Einstellungen genauer erläutern zu können, ist es sinnvoll, vorab kurz einige Begrifflichkeiten zu klären. Abbildung 5 zeigt auf einen Blick, in welche verschiedenen Anzeigebereiche das Fenster des Browsers aufgeteilt ist.

- Im Inhaltsbereich werden die Webseiten dargestellt.
- Die Bedienelemente und die Adresszeile dienen in erster Linie dazu, Webseiten aufzurufen, zu aktualisieren und zwischen einzelnen Seiten hin und her zu springen.
- Die Komfortfunktion Lesezeichen bietet Ihnen die Möglichkeit, einen direkten Link zu einer Webseite anzulegen, um so mit nur einem Klick – ohne die Internetadresse per

Hand eingeben zu müssen – zu der gespeicherten Internetadresse zu kommen.

- Die Statusleiste befindet sich im Allgemeinen unter dem Anzeigebereich. Sie kann über das Menü «Ansicht» aufgerufen werden und zeigt zusätzliche wichtige Informationen an.

Abbildung 5: Die Anzeigebereiche eines Browsers

Die Funktion «Statusleiste» sollten Sie unbedingt nutzen, denn damit können Sie sich unter anderem die Zieladresse eines Links ansehen (Aufbau von Links beziehungsweise einer URL, siehe Softlink 220). Diese wird automatisch angezeigt, wenn Sie den Mauszeiger auf den fraglichen Link bewegen, ohne ihn anzuklicken (siehe Abbildung 6). Steht hier statt der zu erwartenden eine völlig andere Webadresse, ist Vorsicht geboten, da der Link eventuell manipuliert wurde, um einen Angriff vorzubereiten. Im Zweifelsfall ist es daher immer ratsam, den fraglichen Link nicht zu benutzen.

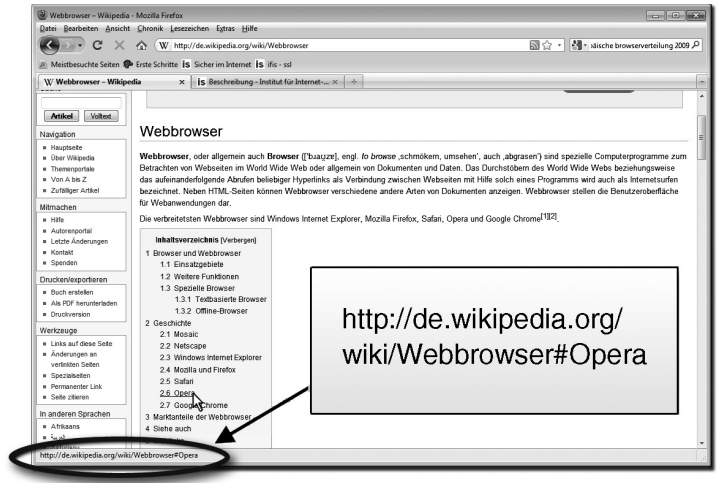

Abbildung 6: Die Statusleiste zeigt die Webadresse an, zu welcher der Link führt. Sie scheint in diesem Fall korrekt zu sein.

TIPP: Statusleiste

Gewöhnen Sie sich an, eine Webadresse immer erst in der Statuszeile genau zu betrachten, ehe Sie sie anklicken. Zeigt die Statuszeile nicht das gewünschte Ziel, meiden Sie den Link. So lässt sich beim täglichen Surfen so mancher Angriff von vornherein vermeiden.

Angriffsfläche Browser – von aktiven Inhalten und anderen Gefahren

Als Tor zur digitalen Welt ist der Browser auch ganz dicht an den Gefahren des Internets dran. Für Angreifer ist er Angriffsziel Nummer eins. Und je vielseitiger die Funktionen und Möglichkeiten des Browsers werden, umso mehr Angriffsmöglichkeiten werden auch eröffnet. Aber Sie können sich gegen viele dieser Angriffe schützen, indem Sie sich richtig verhalten. Wie das geht, zeigen die folgenden Abschnitte.

Risikofaktor aktive Inhalte

Webseiten werden mit der Auszeichnungssprache HTML (HyperText Markup Language) erstellt. Diese lässt jedoch zunächst keine Interaktion beziehungsweise Animation zu. Das ist nur mit zusätzlichen sogenannten aktiven Inhalten möglich. Dabei handelt es sich um kleine «Softwareprogramme», die mithilfe von Werkzeugen wie JavaScript beziehungsweise JScript, Flash, ActiveX-Controls, VBScript, Java-Applets sowie AJAX erstellt und in den HTML-Code eingebettet werden. Aktive Inhalte machen eine Webseite dynamisch (zum Beispiel durch Spiele, Filme und animierte Sequenzen) und ermöglichen eine direkte Interaktion zwischen den Anwendungen auf Ihrem Computer und dem Webserver, um beispielsweise auf eine Datenbank zugreifen zu können. Sie werden automatisch aktiv, sobald die entsprechende Webseite angesurft wird.

Aktive Inhalte bieten also viele Vorteile, stellen aber auch ein großes Sicherheitsrisiko dar. Denn heutzutage wird Malware zum größten Teil über Webseiten mit aktiven Inhalten verbreitet. Dieser Angriff wird Drive-by-Download genannt. Dabei wird eine Schwachstelle des Browsers oder eines Browser-Plugins ausgenutzt, um beim Besuch einer infizierten Webseite im Hintergrund eine Malware auf den Computer herunterzuladen. Allein der Besuch einer solchen Webseite kann ausreichen, um Ihren Computer – ohne dass Sie es merken – zu infizieren.

Aktuelle Browser weisen deshalb mithilfe verschiedener Anzeigen den Nutzer darauf hin, dass aktive Inhalte in einer Webseite enthalten sind und fragen, ob diese zugelassen werden sollen. Erste Reaktion: «Na klar, sonst kann ich ja nicht alle Funktionen der Webseite nutzen!» Doch Vorsicht: Über die vielen flexiblen Möglichkeiten der aktiven Inhalte ist es ver-

gleichsweise einfach, Schwachstellen im Computer für einen Angriff zu nutzen. Sie sollten also deren Einsatz wann immer möglich vermeiden. Allerdings sind aktuelle Webseiten im Web 2.0 fast immer mit aktiven Inhalten ausgestattet – eine Videoplattform ohne Videos ergibt schließlich nicht viel Sinn. Hier ist wiederum Ihr gesunder Menschenverstand gefragt und die Fähigkeit, die Vertrauenswürdigkeit einer Webseite einzuschätzen. Die folgenden Punkte helfen Ihnen dabei:

- Sind der Aufbau und die Inhalte der Webseite für Sie klar nachvollziehbar und machen sie einen vertrauenswürdigen Eindruck?
- Haben Sie mit der Webseite bereits in der Vergangenheit gute Erfahrungen gemacht?
- Ist Ihnen die Webseite von einer vertrauenswürdigen Person empfohlen worden?
- Werden Sie aufgefordert Daten einzugeben, die aus Ihrer Sicht nichts mit Ihrem eigentlichen Anliegen zu tun haben?
- Werden Eingaben verschlüsselt übertragen (siehe Seite 36 ff.)?
- Ist Werbung – sofern vorhanden – klar als solche zu erkennen?
- Steht im Impressum genau, wer für die Webseiten verantwortlich ist? Sind eine Adresse und eine Telefonnummer angegeben?

Um den Anwender in eine Falle zu locken, lassen sich die Angreifer durchaus etwas einfallen. Die Webseite in Abbildung 7 ist von einem Angreifer verändert worden. Der Link in dem kleinen Kasten führt in diesem Fall nicht zu ebay, sondern zu einer gefälschten ebay-Seite, um an die Zugangsdaten des Benutzers zu kommen.

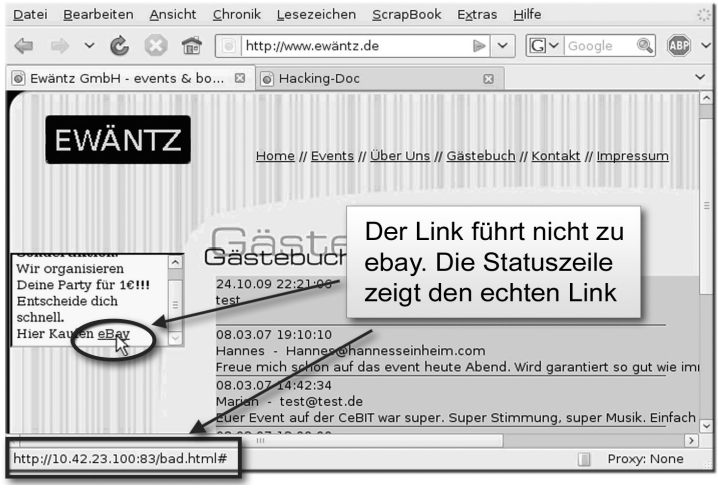

Abbildung 7: Webseite, die einem Cross-Site-Scripting-Angriff zum Opfer gefallen ist

Der in diesem Beispiel vollzogene Angriff nennt sich Cross Site Scripting (XSS). Er nutzt sicherheitstechnisch schwach programmierte Webseiten mit aktiven Inhalten aus – hier eine Webseite mit einem Eingabefeld (Gästebuch), die sicherheitstechnisch nicht sauber programmiert wurde. Gegen den Fehler selbst können Sie als Internetnutzer nichts tun. Aber Sie können durch Achtsamkeit die Manipulation erkennen (wäre der Link echt, würde in der Statuszeile die Webadresse www.ebay.de stehen) und sich dementsprechend schützen (siehe Seite 29f.).

Das in dem Beispiel versuchte «Phishen» (Phishing = Password + Fishing) der Zugangsdaten ist eine gängige Art des Angriffs im Internet. Ein Klick auf den Link im markierten Kasten würde den Nutzer auf eine Webseite führen, die nur so aussieht wie die von ebay. Wenn sich der Nutzer dann auf der falschen ebay-Seite einloggt, gibt er dem Angreifer seine Iden-

tität und das Passwort preis. Dieser Angriff wird «Phishing» genannt, weil nach dem Passwort des Nutzers gefischt wird (siehe Abschnitt «Onlinebanking»).

Noch gefährlicher ist es, wenn Sie auf eine Webseite gelangen, die versucht, Schadsoftware auf Ihren Computer zu spielen. Damit kann der Computer vollständig übernommen und alle Dateien, inklusive Passwörter und Bankdaten, können ausgespäht werden. Diese Angriffe passieren im Internet täglich. Deshalb ist Wachsamkeit durch nichts zu ersetzen!

TIPP: Sicheres Surfen

- Wenn Sie auf eine Ihnen bekannte Webseite surfen und diese sich plötzlich verändert präsentiert, beispielsweise einen neuen Kasten enthält, wie die Webseite in Abbildung 7, dann sollten bei Ihnen die Alarmglocken läuten.
- Ebenso misstrauisch sollten Sie sein, wenn eine Ihnen unbekannte Webseite aktive Inhalte nutzen will.
- Lassen Sie aktive Inhalte nur auf vertrauenswürdigen Seiten zu, und auch nur dann, wenn sie unbedingt notwendig sind (zum Beispiel um einen Film abzuspielen).
- Seien Sie besonders wachsam, wenn Sie auf Webseiten sicherheitskritische Daten wie Passwörter, Bankdaten, Adressen, Handy-Nummer usw. eingeben.

Risikofaktor sorgloser Umgang mit persönlichen Daten

Ein großes Problem stellt der sorglose Umgang vieler Nutzer mit ihren privaten Daten dar. Dabei ist genau das Gegenteil das Gebot der Stunde: Geben Sie so wenig wie möglich von sich im Internet preis. Und wenn Sie Informationen weitergeben, dann nur solche, die für den entsprechenden Vorgang wirklich notwendig sind – ein Chatroom benötigt keine

Bankdaten und ein Onlineshop muss nicht unbedingt wissen, welche anderen Shops Sie sonst noch besuchen. Entsprechend sollten Sie Ihre Daten auch nicht wahllos in sozialen Netzwerken verteilen (siehe Seite 86 ff., Softlink 221). Denken Sie stets daran: Weniger Daten bedeutet mehr Schutz Ihrer Privatsphäre!

Risikofaktor private Surfdaten

Das Surfen hinterlässt Spuren im Browser. Dieser legt automatisch eine Chronik an, welche die besuchten Seiten, Sucheinträge, ausgeführte Downloads, Formulardaten, Cookies und temporäre Internetdateien speichert. Eigentlich handelt es sich hierbei um eine Komfortfunktion, aber es kann durchaus sinnvoll sein, private Surfdaten daraus zu löschen, beispielsweise wenn der Computer nach Ihnen noch von einem anderen Nutzer verwendet wird. Ansonsten kann dieser die genannten Daten einsehen und eventuell missbrauchen.

Ein Beispiel für private Surfdaten sind Cookies, die viele Webseiten auf dem Computer des Nutzers hinterlassen. Dabei handelt es sich um Dateien, mit deren Hilfe ein Webserver erkennen kann, ob ein Nutzer schon einmal auf der Webseite war oder ob er sich gerade in einem Einkaufsvorgang befindet. Dazu sendet der Webserver einen Cookie zum Browser, und dieser speichert den Cookie auf dem Computer. Wenn der Nutzer dann wieder auf den gleichen Webserver zugreift, erkennt das der Browser und sendet als Erstes den gespeicherten Cookie mit. Mit dem Inhalt des Cookies ist der Webserver in der Lage, Rückschlüsse auf alte Vorgänge zu ziehen, wie zum Beispiel das Nutzerverhalten. Damit der Webserver aber die Aktivitäten einem bestimmten Nutzer zu-

ordnen kann, enthalten die Cookies auch die ID des Nutzers, mit der er auf der entsprechenden Webseite geführt wird. Das birgt potenziell auch die Gefahr des Datenmissbrauchs.

Um dieses Risiko zu minimieren, können Sie den Browser so einstellen, dass nach dem Schließen des Browsers alle Cookies und private Daten gelöscht werden. Allerdings kann eine Ausnahme für Seiten, die Sie regelmäßig nutzen, hier durchaus sinnvoll sein, da Cookies helfen, das Angebot von Webseiten zu optimieren. Ein Browser kann auch direkt in einem Modus gestartet werden, der von vornherein die Speicherung der genannten privaten Daten verhindert (Umgang mit privaten Surfdaten und Einstellung eines privaten Modus, siehe Softlink 222).

Risikofaktor Datenübertragung

Ein weiteres Problem im Internet ist, dass Daten bei der Übertragung grundsätzlich mitgelesen werden können. Dafür braucht der Angreifer nur Zugriff auf die Datenleitung, was zum Beispiel dann möglich ist, wenn er sich im gleichen Netzwerk befindet.

Besonders kritisch ist das natürlich bei Daten wie Passwörtern oder Kreditkartennummern. Um hier Abhilfe zu schaffen, bieten viele Internetdienste inzwischen eine sogenannte SSL/TLS-Verschlüsselung an, die alle zwischen Browser und Webserver ausgetauschten Dateien verschlüsselt und integritätsgesichert überträgt (Softlink 226).

Ob die von Ihnen besuchte Webseite eine solche Verschlüsselung verwendet, können Sie an zwei Merkmalen erkennen: In der Adresszeile (URL) des Browsers beginnt die Webadresse normalerweise mit «http://». Werden die Daten verschlüsselt übertragen, steht dort «https://». Das kleine «s»

zeigt die sichere Übertragung der Daten an. Das allein ist aber noch nicht ausreichend. Zusätzlich erscheint im Browser in der rechten unteren Ecke oder ebenfalls in der Adresszeile ein Schloss-Symbol, das ebenfalls die sichere Verbindung signalisiert (siehe Abbildung 8). Durch einen Doppelklick auf das Schloss-Symbol erhalten Sie genauere Informationen zu der Verschlüsselung und dem Zertifikat, das benutzt wird.

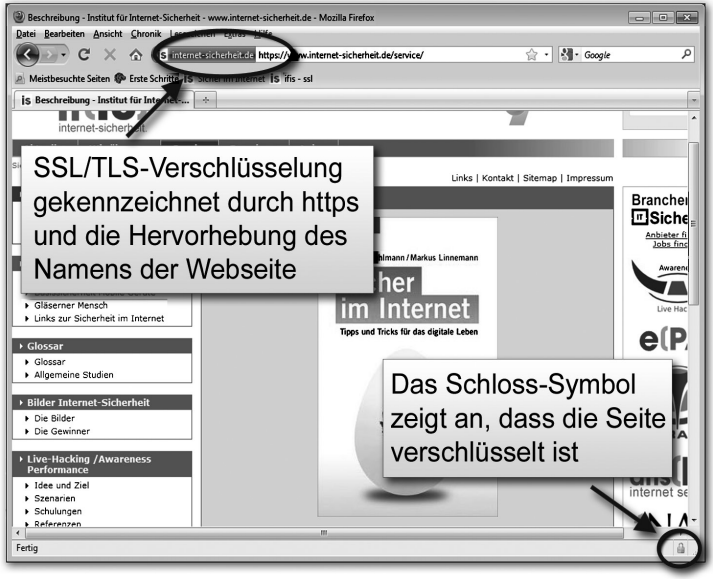

Abbildung 8: Webseite, die Daten verschlüsselt per SSL/TLS überträgt

Dieses Zertifikat lässt sich ein Webseitenanbieter von einer vertrauenswürdigen Instanz, einer Zertifizierungsstelle, ausstellen. Die Zertifizierungsstelle überprüft die Echtheit des Antragstellers, das heißt, der Nutzer kann sicher sein, dass hinter dem Namen im Zertifikat ein reales Unternehmen steht und dass die Webadresse tatsächlich zu diesem Unternehmen

gehört. Die Webadresse www.internet-sicherheit.de zum Beispiel gehört zum Institut für Internet-Sicherheit der Fachhochschule Gelsenkirchen.

Ihr Browser kann die gängigsten Zertifikate in der Regel automatisch verifizieren. Dazu sind die sogenannten Root-Zertifikate der entsprechenden Zertifizierungsstellen sicher im Browser gespeichert. Wenn Sie nun unter Verwendung einer verschlüsselten SSL/TLS-Kommunikation eine Webseite aufrufen, und es erscheint eine Warnmeldung, dass etwas mit dem Zertifikat nicht stimmt, ist höchste Vorsicht geboten! Besonders dann, wenn ein vorheriger Besuch dieser Webseite keine Warnmeldung hervorgerufen hatte. Hier handelt es sich mit großer Wahrscheinlichkeit um einen Angriff. Stoppen Sie deshalb an dieser Stelle alle Aktivitäten und überprüfen Sie das Zertifikat genauer.

Dazu führen Sie einen Doppelklick auf das Schloss-Symbol aus und klicken im Folgedialog auf «Zertifikat anzeigen». Nun können Sie vergleichen, ob die Webadresse im Zertifikat mit der Webadresse übereinstimmt, auf die Sie zugreifen möchten. Haben Sie zum Beispiel in die Adresszeile «www.internet-sicherheit.de» eingegeben, dann muss auch im Zertifikat diese Webadresse genannt sein. Aber schauen Sie lieber zweimal hin. Die folgenden Webadressen www.internet-sicherheit.de und www.intenet-sicherheit.de sehen auf den ersten Blick zwar ähnlich aus, aber im Ernstfall würde die zweite Adresse Sie auf die Webseite des Angreifers führen. Auf diese Weise können Sie ebenfalls überprüfen, wem die Webadresse gehört. In unserem Beispiel: dem Institut für Internet-Sicherheit der Fachhochschule Gelsenkirchen (siehe Abbildung 9 sowie Softlink 223 – Screenvideo «SSL/TLS und Zertifikate überprüfen»).

Der sicherste, aber sehr selten praktizierte Weg, ein Zertifikat zu überprüfen, besteht darin, den sogenannten Fingerabdruck eines Zertifikats (eine Zeichenfolge aus den Buchstaben A bis F und den Ziffern 0 bis 9) zu kontrollieren. Dafür müssen Sie den Webseitenbetreiber kontaktieren und beispielsweise per Telefon den im Zertifikat der Webseite genannten Fingerabdruck mit den Angaben des Anbieters vergleichen. Die Reaktion eines normalen Mitarbeiters auf ein solches Ansinnen ist interessant zu beobachten, da die meisten damit zunächst völlig überfordert sind. Dieses Verfahren sollten Sie also wirklich erst dann anwenden, wenn Sie den begründeten Verdacht haben, dass tatsächlich ein Angriff auf Ihren Rechner vorliegt.

In Abbildung 9 ist beispielhaft ein Zertifikat mit den genannten Angaben und den beiden Fingerabdrücken (es handelt sich dabei lediglich um zwei verschiedene Arten, den Fingerabdruck anzugeben) zu sehen. Stimmen die Daten und die

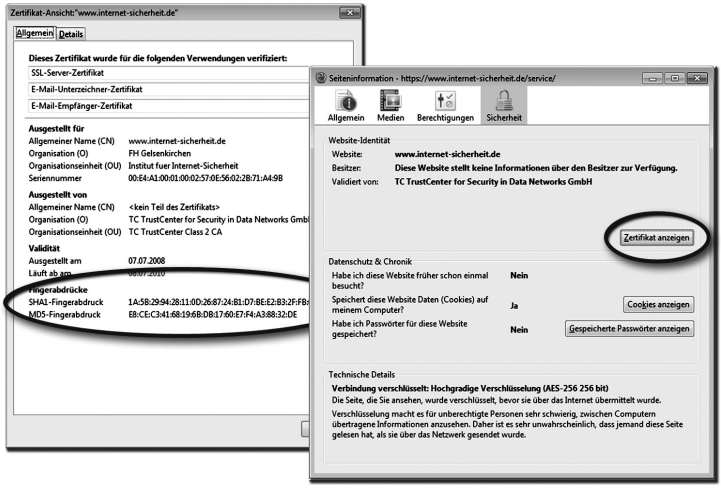

Abbildung 9: Zertifikat mit den beiden Fingerabdrücken

Fingerabdrücke mit denen überein, die der Betreiber Ihnen nennt, ist die Webseite in Ordnung. Ein Phishing-Angriff wird durch diese Art der Überprüfung quasi ausgeschlossen.

In der Realität werden Sie vermutlich jedoch nicht jedes Zertifikat prüfen, aber von Zeit zu Zeit sollten Sie doch eine Überprüfung durchführen, vor allem dann, wenn Ihnen etwas verdächtig vorkommt, Sie die Seite zum ersten Mal besuchen oder Ihr Computer mit Schadsoftware in Berührung gekommen ist.

Noch mehr Sicherheit soll das Extended-Validation-Zertifikat bieten, das von den wichtigsten Zertifizierungsstellen und Browserherstellern gemeinsam spezifiziert und umgesetzt wird. Ziel dieses neuen Sicherheitsmechanismus ist, Phishing mittels vermeintlich sicherer Webseiten zu erschweren. Durch die Einführung dieses neuen, erweiterten Zertifikats und der zusätzlichen Elemente im Browser soll das Vertrauen der Nutzer in die Sicherheit der Verbindung gestärkt werden.

Für das Extended-Validation-Zertifikat bestehen strengere Vergabekriterien. Die Zertifizierungsstellen, die dieses Zertifikat ausgeben dürfen, müssen sich einer Überprüfung hinsichtlich ihrer Verlässlichkeit und Vertrauenswürdigkeit unterziehen. Die Vergabe des Extended-Validation-Zertifikats durch die überprüften Zertifizierungsstellen ist an die folgenden Kriterien gebunden:

- Die Verifizierung der Identität, das heißt der Echtheit der Geschäftsadresse des Antragstellers, muss erfolgen.
- Es muss sichergestellt werden, dass der Antragsteller auch ausschließlicher Eigentümer der Domain (Webadresse) ist oder eine exklusive Nutzungsberechtigung hat.
- Es muss sichergestellt werden, dass der Antrag ausnahmslos von Personen gestellt wird, die dazu befugt sind, und dass

der Unterzeichner des rechtlich bindenden Dokuments zeichnungsberechtigt ist.

Ihnen als Nutzer hilft das Zertifikat, weil es zusätzliche Anzeigen im Browser generiert. Je nach Browser wird die ganze Adresszeile, Teile davon oder der neben dem Schloss-Symbol angegebene Namen des Zertifikatsbesitzers grün dargestellt. Zusätzlich wird ein Feld angezeigt, in dem der Zertifikats- und Webadresseninhaber im Wechsel mit der Zertifizierungsinstanz eingeblendet wird. So können Sie diese Angaben einfacher überprüfen und schneller erkennen, ob die von Ihnen besuchte Webseite echt ist.

TIPP: Sichere Datenübertragung

Geben Sie sicherheitskritische Daten wie Kreditkartennummern und Passwörter nur dann in einen Browser ein, wenn die Verbindung SSL/TLS-verschlüsselt ist. Sie erkennen dies an der Angabe «https» in der Adresszeile und dem geschlossenen Schloss-Symbol. Haben Sie Zweifel, doppelklicken Sie auf das Schloss-Symbol und überprüfen Sie das Zertifikat (SSL/TLS und Zertifikate überprüfen, siehe Softlink 223).

Risikofaktor Surfen mit fremden Computern

Das Surfen im Internet ist insbesondere auf Dienstreisen und im Urlaub eine gute Möglichkeit, um mit der «Heimat» in Kontakt zu bleiben. Beim Surfen mit fremden Computern, zum Beispiel im Internetcafé, ist jedoch besondere Vorsicht geboten, da Sie keinen oder nur sehr wenig Einfluss auf die getroffenen Sicherheitsmaßnahmen haben. Insofern ist die Gefahr, dass Ihre Eingaben ausgespäht werden – vom Besitzer des PCs oder von jemand anderem –, deutlich erhöht. Versu-

chen Sie deshalb, so wenig persönliche Daten wie möglich preiszugeben und löschen Sie alle Daten (Fotos, Cookies etc.), bevor Sie Ihre Internetsitzung beenden. Sicherheitskritische Vorgänge, wie Onlinebanking oder Einkäufe (hier vor allem das Bezahlen), sollten Sie generell nur mit Ihrem eigenen Computer erledigen.

TIPP: Surfen mit fremden Computern

- Versuchen Sie, so wenig persönliche Daten wie möglich einzugeben.
- Führen Sie sicherheitskritische Vorgänge nur auf dem eigenen Computer aus, wie zum Beispiel Onlinebanking, Einkaufen und Bezahlen.
- Löschen Sie alle Daten (Fotos, Cookies, Passwörter usw.), bevor Sie das Internetcafé verlassen!

Exkurs: IP-Adresse und DNS

Dieser Abschnitt erfordert etwas mehr technische Erklärungen und ist für all diejenigen relevant, die sich für die in der Politik und in der Rechtsprechung heftig diskutierte Sperrung von Internetseiten interessieren – oder einfach nur wissen wollen, was DNS und IP-Adressen sind.

Die Webadresse ist nur der Einfachheit halber als Name realisiert, und es gibt zu jedem Namen auch eine Zahlenfolge in der Form 123.123.123.123 – die sogenannte IP-Adresse (IP = Internet Protocol), welche die eigentliche Internetadresse darstellt. So verbirgt sich hinter der Webadresse www.internet-sicherheit.de aktuell die IP-Adresse 194.94.127.43. Jetzt fragen Sie sich vielleicht, wie diese IP-Adresse zustande kommt. Das erledigt der sogenannte Domain Name Service

(DNS). Seine Aufgabe ist es, die namentliche Webadresse auf die jeweilige numerische IP-Adresse zu «mappen» (abzubilden). Das heißt, wenn Sie in das Adressfeld Ihres Browsers eine Webadresse eintippen, dann übergibt dieser sie dem Domain Name Service. Der DNS holt sich dann über das Internet die IP-Adresse und gibt diese an den Browser zurück. Der Browser wiederum baut mit der IP-Adresse die Verbindung zum Webserver auf, und die Webseite kann geladen werden.

Der Vorteil dieser Methode ist, dass Sie sich keine komplizierte Ziffernfolge merken müssen, sondern Namen, die in der Regel viel eingängiger sind und auch einfacher zu raten, wie zum Beispiel www.otto.de für den Versandhändler Otto (in Deutschland). Der Nachteil ist, dass dieses Verfahren auch zum Ausspähen von Daten genutzt werden kann, zum Beispiel im Rahmen eines sogenannten Pharming-Angriffs, bei dem der Domain Name Service manipuliert wird (siehe Seite 103 ff.).

Übrigens besitzt nicht nur jede Webseite eine IP-Adresse, sondern auch jedes an das Internet angeschlossene Gerät. Das muss so sein, damit die Datenpakete, die durch das Internet sausen, genau wissen, wo sie hin müssen (analog zur Postanschrift).

So machen Sie Ihren Browser fit für die Datenautobahn

Um sich möglichst sicher im Internet zu bewegen, gibt es eine Vielzahl an technischen Hilfen. Der Browser selbst lässt sich sicherheitstechnisch optimieren und bringt bereits einige Sicherheitsfunktionen von Haus aus mit. Die entsprechenden Einstellungen können Sie beim Firefox im Menü «Extras» im Reiter «Sicherheit» vornehmen.

Abbildung 10: Sicherheitseinstellungen im Firefox Browser

Basis-Einstellungen

Wie in Abbildung 10 zu sehen ist, sollten hier bestimmte Haken gesetzt sein. Der zweite und dritte Haken erklären sich von selbst und sollten auf jeden Fall aktiviert werden, um nicht auf Webseiten zuzugreifen, die nachweislich problematisch sind. Ist der erste Haken zusätzlich gesetzt, werden sogenannte Add-ons geblockt, die automatisch installiert werden sollen, also ohne vorherige Interaktion mit dem Anwender. Add-ons sind kleine Zusatzprogramme, mit denen der Browser erweitert werden kann, ähnlich der Sonderausstattung im Auto. Im Normalfall können diese, wie noch beschrieben wird, sehr nützlich sein. Aber es könnten auch Add-ons installiert werden, welche die Sicherheit bedrohen, daher die Warnung. Der sich anschließende Bereich «Passwörter» bezieht sich auf die Speicherung von eingegebenen

Passwörtern. Der Browser merkt sich nach der ersten Eingabe auf Wunsch die Zugangsdaten und füllt die entsprechenden Felder beim nächsten Besuch automatisch aus. Diese Komfortfunktion ist jedoch mit Vorsicht zu genießen. Genauere Informationen hierzu erhalten Sie ab Seite 57.

Werbung und aktive Inhalte blocken

Wild blinkende Werbebanner versprühen nicht nur einen fragwürdigen Charme, sondern sind oftmals auch ein Hilfsmittel für kriminelle Machenschaften. Um diese Art Werbung zu blocken, sollten Sie Ihren Browser ausrüsten, indem Sie ein entsprechendes Add-on installieren – beim Firefox zum Beispiel Adblock Plus. Dazu rufen Sie die Mozilla-Add-on-Webseite (Softlink 224) auf und geben in das Suchfeld «Adblock Plus» ein. Zur Installation drücken Sie lediglich den Button

und wählen im folgenden Dialog «Jetzt installieren» aus. Nachdem das Add-on installiert wurde, müssen Sie den Browser neu starten, und es öffnet sich eine Webseite, auf der Sie aufgefordert werden, eine der angegebenen Listen auszuwählen.

Für Deutschland, Österreich und die Schweiz ist es sinnvoll, die vorgewählte «Easy List Germany + Easy List» auszuwählen und die Eingabe zu bestätigen. Fortan bleiben Sie größtenteils von lästiger und manchmal auch gefährlicher Werbung verschont.

Aktive Inhalte können, wie bereits erläutert, ebenfalls eine Gefahr darstellen. Deshalb besitzen die meisten Browser bereits einen eingebauten Warnmechanismus, wenn aktive Inhalte zur Ausführung kommen sollen. Dieser ist aber nicht sehr flexibel und reicht kaum aus. Eine deutlich bessere und komfortablere Kontrolle bietet da das Firefox-Add-on NoScript. Die Installation folgt dem Beispiel von Adblock Plus.

Danach blockt NoScript zunächst alle Skripte (aktive Inhalte) auf einer Webseite und teilt Ihnen dies mit. Sie können nun entscheiden, welche Skripte Sie – temporär oder immer – zulassen wollen und welche nicht. Der gelbe Balken am unteren Bildrand signalisiert Ihnen, dass Skripte vorhanden sind, und mit einem Klick auf den Einstellungen-Button beziehungsweise auf das  -Symbol rechts unten in der Statusleiste gelangen Sie in das entsprechende Menü (siehe Abbildung 11). Das Symbol zeigt gleichzeitig an, welche Skripte geblockt werden und welche nicht.

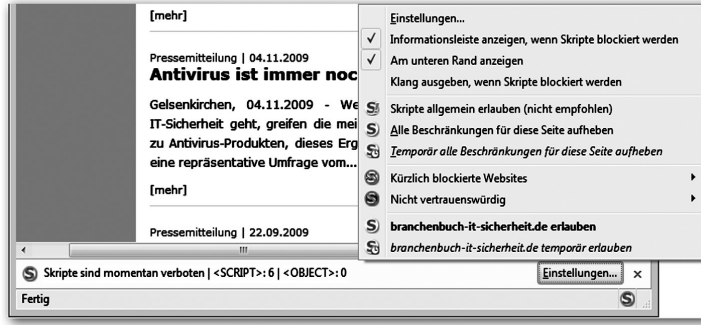

Abbildung 11: Hier können Sie wählen, wie Sie mit den jeweiligen Skripten verfahren wollen.

NoScript ist so aufgebaut, dass auch ein Internetneuling nach einer kurzen Eingewöhnungszeit problemlos damit um-

gehen kann. Einziger Wermutstropfen: Der tägliche Surfaufwand erhöht sich minimal, doch Sicherheit benötigt eben auch Zeit und Aufmerksamkeit.

Eine andere Möglichkeit ist, JavaScript über die Grundeinstellung des Browsers vollständig zu blocken (beim Firefox über das Menü «Extras» und dann im Reiter «Inhalt»). Allerdings führt das im Zeitalter von Web 2.0 dazu, dass sehr viele Webseiten nicht mehr richtig nutzbar sind. Darum ist es sinnvoller, mit Add-ons wie NoScript flexibel zu bleiben.

Ausblick: Wie sieht die Zukunft des Web aus?

Die Bedeutung des Browsers wird weiter zunehmen. Der Trend geht dahin, dass Funktionen, die heute lokal auf dem Computer ausgeführt werden, «in das Internet wandern». Das bedeutet, dass der Browser Programme wie Word, Excel, PowerPoint etc. überflüssig machen wird, da diese Anwendungen künftig als Internetdienste verfügbar sein werden und wir unsere Dokumente im Internet verfassen und abspeichern werden. Lokale Office-Installationen und große lokale Festplatten gehören dann der Vergangenheit an. Diese Entwicklung nennt sich Cloud Computing, da alle Funktionen innerhalb der «Internetwolke» angeboten werden.

Für den Nutzer stellt sich dann die Frage, welchem Cloud-Computing-Anbieter er so viel Vertrauen schenkt, dass er ihm all seine Daten anvertraut. Denn diese sollten zuverlässig zu jeder Zeit und auch in zehn Jahren noch zur Verfügung stehen …

Im Zuge dieser Entwicklung wird auch die Bedeutung der Smartphones weiter wachsen. Diese bringen jedoch

naturgemäß ein größeres Risiko mit sich, da die Wahrscheinlichkeit, dass diese kleinen und häufig mit sich herumgetragenen Geräte samt den gespeicherten Daten gestohlen werden oder verloren gehen, deutlich höher ist.

Freuen Sie sich auf Teil 3:
Sicher bewegen im Internet – Passwörter, E-Mail, Web 2.0

Ab 21.01.2013 zum kostenlosen Download auf
www.internet-sicherheit.de