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 des Instituts für Internet-Sicherheit

securityNews

securityNews: Kostenlose App für mehr Sicherheit im Netz



- 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/sn

Available on the App Store | ANDROID APP ON Google play | Windows Store

Mit freundlicher Unterstützung von: Bundesamt für Sicherheit in der Informationstechnik

Norbert Pohlmann/Markus Linnemann

Sicher im Internet

Tipps und Tricks für das digitale Leben

Norbert Pohlmann/Markus Linnemann

Sicher im Internet
Tipps und Tricks
für das digitale Leben

orell füssli Verlag AG

© 2010 Orell Füssli Verlag AG, Zürich
www.ofv.ch
Alle Rechte vorbehalten

Dieses Werk ist urheberrechtlich geschützt. Dadurch begründete Rechte, insbesondere der Übersetzung, des Nachdrucks, des Vortrags, der Entnahme von Abbildungen und Tabellen, der Funksendung, der Mikroverfilmung oder der Vervielfältigung auf anderen Wegen und der Speicherung in Datenverarbeitungsanlagen, bleiben, auch bei nur auszugsweiser Verwertung, vorbehalten. Vervielfältigungen des Werkes oder von Teilen des Werkes sind auch im Einzelfall nur in den Grenzen der gesetzlichen Bestimmungen des Urheberrechtsgesetzes in der jeweils geltenden Fassung zulässig. Sie sind grundsätzlich vergütungspflichtig.

Konzeption und Realisation: Ariadne-Buch, Christine Proske, München
Redaktion: Andreas Ehrlich
Umschlagabbildung: © Institut für Internet-Sicherheit, Andrej Elbers
Umschlaggestaltung: Andreas Zollinger, Zürich
Druck: fgb • freiburger graphische betriebe, Freiburg

ISBN 978-3-280-05375-1

———

Bibliografische Information der Deutschen Nationalbibliothek:
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Inhalt

Einleitung: Erfolgsgeschichte Internet – Chancen und Risiken 7
Ihr bester Schutz: IT-Sicherheit und Internetkompetenz **8**
Über dieses Buch – ein kurzer Leitfaden **8**

Basisschutz – das 1 x 1 für einen sicheren Computer 10
Grundlegende Sicherheitseinstellungen – Malware-Scanner & Co. **11**
Der Internetbrowser – sinnvoll einstellen, sinnvoll nutzen **26**

Sicher bewegen im Internet – So geht's 49
Passwörter – von gestern bis morgen **49**
E-Mail – von digitalen Postkarten und falschen Absendern **63**
Web 2.0 – das Mitmach-Web **85**
Onlinebanking – Sicher, wenn's ums Geld geht **98**
E-Commerce – Shoppen «hoch n» **113**
Auktionshäuser im Internet – 3, 2, 1 … Falle **122**
Internettelefonie & Chatten – Kommunikation total **126**
Kindersicherung fürs Internet – keine Sorge um den Nachwuchs **135**

Antennen ausfahren – Zugang zum Internet 141
DSL und WLAN – sicher einrichten und sicher nutzen **142**

Bluetooth – der «Blauzahn» **156**
UMTS – State of the Art beim mobilen Internet **160**

Ihre Rechte und Pflichten als Internetnutzer – der aktuelle Stand 162
Der Rechtsrahmen im Internet – Der Klügere denkt nach **163**
Die Verbraucherpflichten – Das fordert der Gesetzgeber von Ihnen **170**

Dringend nötig: die Schaffung einer Internet-Sicherheitskultur 174
Vom realen zum digitalen Leben – Sicherheit und Vertrauenswürdigkeit im Internet **174**
Hilfe zur Selbsthilfe – Probleme managen **180**

Glossar 183

Danksagung 191

Einleitung: Erfolgsgeschichte Internet – Chancen und Risiken

Das Internet ist aus unserem Leben nicht mehr wegzudenken! Surfen, E-Mails schreiben und Onlinebanking haben mittlerweile ebenso in unseren Alltag Einzug gehalten wie die rasant wachsenden sozialen Netzwerke Xing, Facebook oder Twitter. Riesig und komplex überwindet das Internet alle geografischen, politischen und administrativen Grenzen sowie kulturellen Unterschiede. Es schafft somit neue Wege, Demokratie und Bürgerbeteiligung zu gestalten – eine neue und ungewohnte Herausforderung für die internationale Gesellschaft und jeden einzelnen Nutzer.

Als Teil einer vernetzten Informations- und Wissensgesellschaft verlagern immer mehr Menschen ihr Berufs-, aber auch ihr Privatleben ins Internet. Die Risiken, denen sie sich dabei aussetzen, sind vielen jedoch unbekannt. Das Internet ist ein gewaltiger Datenspeicher, der begierig alles aufsaugt und nichts vergisst. Dazu gehören auch Informationen und Bilder, von denen wir nicht wollen, dass sie jedem Nutzer des World Wide Web zur Verfügung stehen. Sicherheitskritische Daten wie unsere Kontodaten geben wir im realen Leben nur ungern einem Fremden preis. Sollten wir dann nicht auch in der virtuellen Welt Vorkehrungen treffen, um unsere Daten zu schützen? Die Bedeutung des Themas Sicherheit hat im Internet in den letzten Jahren erheblich zugenommen, denn das Vertrauen der Nutzer in das Medium sinkt aufgrund

negativer Erfahrungen und sich häufender Nachrichten über Datenmissbrauch sowie immer neue Betrugsmaschen zwangsläufig. Sicherheitslücken schließen und die eigene Internetkompetenz stärken – diese Herausforderungen gilt es zu meistern, um die vielfältigen Möglichkeiten des Internets sicher nutzen zu können.

Ihr bester Schutz: IT-Sicherheit und Internetkompetenz

Ob Diebstahl von Identitätsdaten, Passwort-Fishing oder Viren, Würmer und Trojanische Pferde – die Angriffsmöglichkeiten auf unsere Daten werden immer raffinierter und professioneller. IT-Sicherheitsmaßnahmen wie Viren- beziehungsweise Malware-Scanner und Personal Firewalls helfen, diese Risiken zu minimieren, doch 100-prozentige Sicherheit kann es im Internet nicht geben – so wie es sie auch im realen Leben nicht gibt. Wir sind daher ergänzend auf die eigene Internetkompetenz angewiesen, die es uns ermöglicht, uns gefahrlos darin zu bewegen. Denn erst wenn uns die Gefahren bei der Nutzung des Internets bewusst sind, können wir unser Verhalten anpassen und unsere Daten schützen.

Über dieses Buch – ein kurzer Leitfaden

Dieses Buch verschafft Ihnen einen Überblick über die derzeitige Situation des digitalen Lebens und beantwortet all Ihre Fragen rund um das Thema «Sicher im Internet». Zahlreiche Tipps und Tricks helfen Ihnen, die Herausforderungen im

Umgang mit den modernen Medien souverän zu meistern – auch ohne vorher ein Informatikstudium absolviert zu haben.

Auf der Webseite *www.sicher-im-internet.de* erhalten Sie zudem aktuelle Informationen zu bestimmten Themen und Linksammlungen. Außerdem finden Sie dort ergänzende beziehungsweise vertiefende Hintergrundinformationen, Zusatztexte, Hilfen sowie Workshops zu speziellen Fragestellungen – darunter auch einige Screenvideos, welche die wichtigsten Einstellungen und Technologien Schritt für Schritt erklären.

Mithilfe der Softlinks in diesem Buch können Sie bequem den im Text befindlichen Verweisen auf die Webseite folgen, ohne jeweils die komplette Webadresse abtippen zu müssen. Unter *www.sicher-im-internet.de/softlinks/* können Sie den Softlink (dreistellige Nummer) in das Formular eintragen und gelangen dann direkt zum gewünschten Ziel.

Wir wünschen Ihnen bei der Lektüre dieses Ratgebers viele hilfreiche Einsichten und fordern Sie auf, uns unter der E-Mail-Adresse *feedback@sicher-im-internet.de* Feedback zu geben. Wir werden dann entsprechende Updates zur Verfügung stellen (Softlink 101).

Und noch ein Hinweis zum Schluss: Grundsätzlich bestehen Gefahren für alle Betriebssysteme, egal ob Mac OS, Linux oder Windows. Allerdings ist das Risiko eines Angriffs auf einen Mac-OS- und Linux-Rechner momentan noch geringer, weil sich die Angreifer wegen der hohen Verbreitung von Windows-Systemen auf diese konzentrieren. Deshalb gehen wir bei den Beschreibungen auch grundsätzlich von einem Windows-System aus, wobei die meisten Tipps für alle Betriebssysteme gleichermaßen gelten, da das Internet plattformunabhängig ist. Ist das einmal nicht der Fall, werden die Unterschiede an der jeweiligen Stelle kurz erläutert.

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.

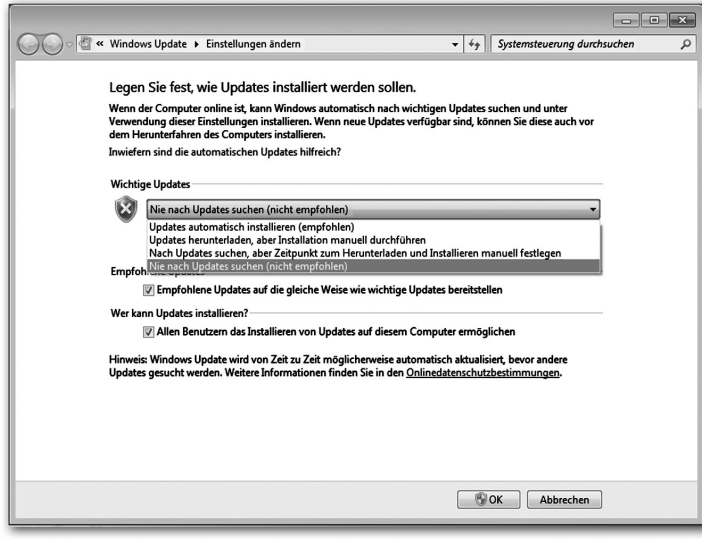


Abbildung 2: Sicherheitscenter unter Windows, das nicht optimal konfiguriert ist

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

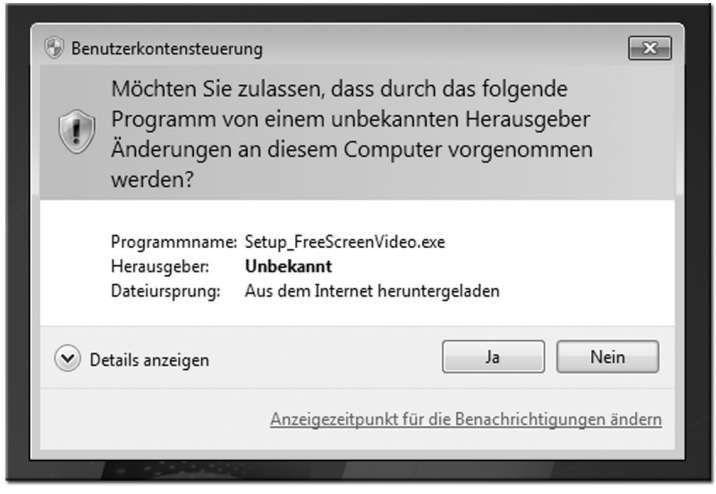


Abbildung 4: Windows-Dialogfeld, das nach Administrator-Rechten fragt

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.

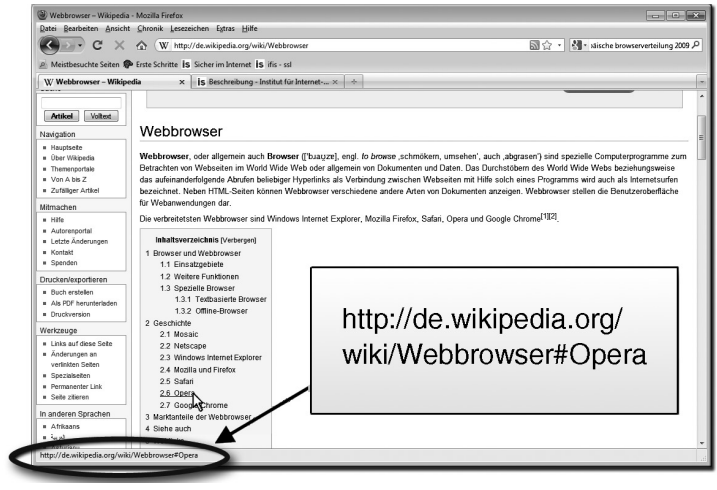


Abbildung 6: Die Statusleiste zeigt die Webadresse an, zu welcher der Link führt. Sie scheint in diesem Fall korrekt zu sein.

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.

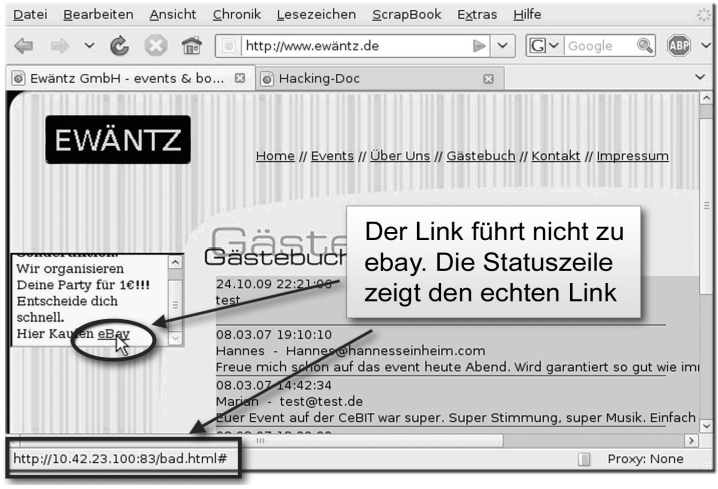


Abbildung 7: Webseite, die einem Cross-Site-Scripting-Angriff zum Opfer gefallen ist

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.

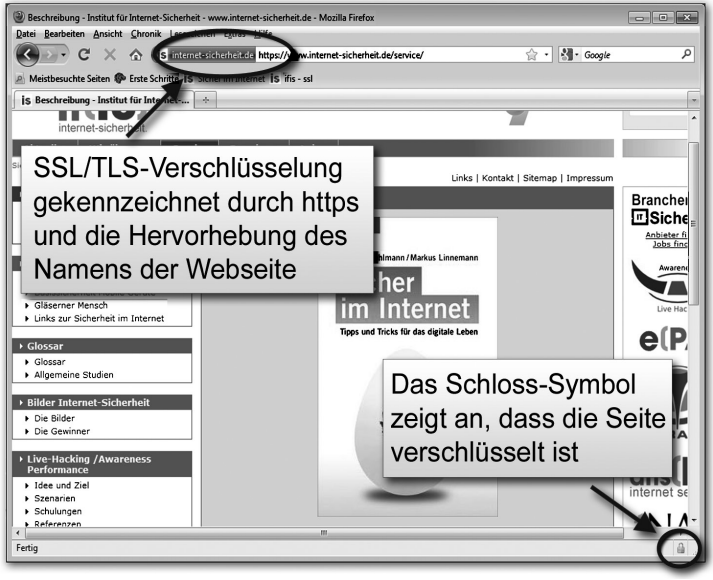


Abbildung 8: Webseite, die Daten verschlüsselt per SSL/TLS überträgt

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

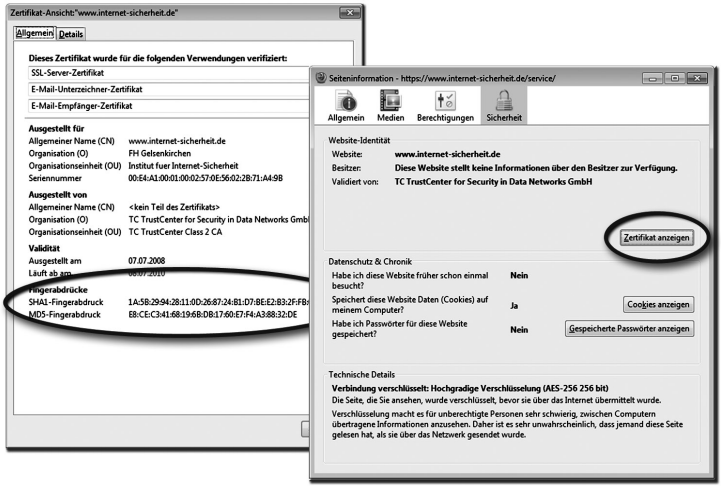


Abbildung 9: Zertifikat mit den beiden Fingerabdrücken

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.

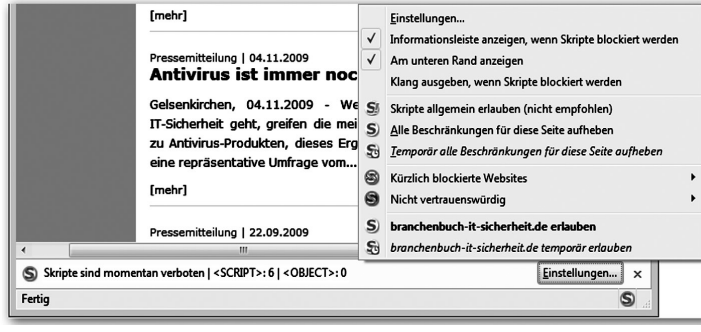


Abbildung 11: Hier können Sie wählen, wie Sie mit den jeweiligen Skripten verfahren wollen.

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.

Sicher bewegen im Internet – So geht's

Im vorangegangenen Kapitel haben Sie bildlich gesprochen den Reifendruck Ihres Autos überprüft, die Scheinwerfer kontrolliert und den Sicherheitsgurt angelegt. Nun geht es darum, das Fahren auf der Autobahn, bei Nacht und in engen Gassen zu üben, damit Sie für alle Situationen gerüstet sind und stets sicher an Ihr Ziel gelangen. Auf das Internet übertragen heißt das, dass Sie in diesem Kapitel alles Wissenswerte zum richtigen Umgang mit den wichtigsten Internetdiensten und Sicherheitstechnologien erfahren.

Passwörter – von gestern bis morgen

Im Jahr 2008 wurde in einem britischen Unternehmen ein interessanter Versuch durchgeführt: Den Mitarbeitern wurde Schokolade im Tausch gegen ihr Zugangspasswort für das Firmennetz angeboten. Das Ergebnis: Je nach Geschlecht gingen 10 Prozent (Frauen) beziehungsweise 45 Prozent (Männer) der Befragten auf dieses Angebot ein. Die Mitarbeiter des Instituts für Internet-Sicherheit konnten das kaum glauben und beschlossen daher im Frühjahr 2009, ein ähnliches Experiment durchzuführen. Sie fragten unter einem Vorwand verschiedene Passanten in einer Fußgängerzone in Gelsenkirchen nach ihren Internetpasswörtern. Auch dieses

Ergebnis ist aus sicherheitstechnischer Sicht erschütternd: Mehr als 90 Prozent der Befragten gaben ihre persönlichen Passwörter preis, und mehr als 50 Prozent verrieten dazu sogar noch ihren (Benutzer-)Namen und die Internetdienste, für die sie ihre Passwörter verwenden. Dabei ist ein Passwort Ihr Schlüssel für die jeweilige Webseite. Und Sie würden Ihren Wohnungs- oder Autoschlüssel doch auch nicht gegen Schokolade tauschen, oder? Sicher nicht, wie das Ergebnis eines nachfolgenden Tests beweist: Bei der Frage nach dem Autoschlüssel war nämlich niemand bereit, diesen herauszugeben.

Passwörter und ihre Schlüsselfunktion

Damit ein Internetdienst, zum Beispiel ein E-Mail-Anbieter oder ein Onlineshop, feststellen kann, ob der anfragende Nutzer Zugang zu dem jeweiligen Dienst erlangen darf, muss sich dieser identifizieren und authentisieren. Die Identifikation ist die Überprüfung eines vorgelegten kennzeichnenden Merkmals, zum Beispiel des Benutzernamens oder der E-Mail-Adresse.

Der Begriff Authentikation bezeichnet einen Prozess, bei dem überprüft wird, ob jemand «echt» ist. Authentikation bedeutet also die Überprüfung der Echtheit beziehungsweise der Identität. Um eine Vergleichsmöglichkeit zu haben, muss diesem Vorgang eine Registrierung oder Anmeldung vorausgegangen sein. Das ist vergleichbar mit einer Passkontrolle. Und diese Kontrolle wird im Internet derzeit überwiegend mithilfe eines Passwortes durchgeführt. Erst wenn der Nutzer das richtige Passwort eingegeben hat, kann er den entsprechenden Internetdienst nutzen.

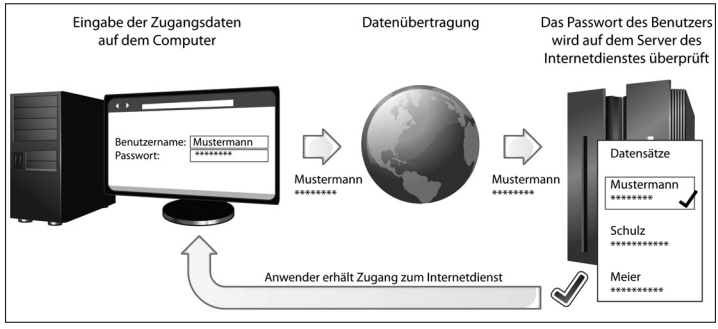


Abbildung 12: Authentikation – ein Passwort ermöglicht den Zugang zu geschützten Bereichen zum Beispiel auf einer Webseite.

In den Anfängen des Internets war noch nicht absehbar, dass irgendwann fast alle gesellschaftlichen und kommerziellen Vorgänge der realen Welt auch im Internet abgebildet sein würden. Zum Schutz personenbezogener Daten und vor dem missbräuchlichen Auslösen von Vorgängen musste daher schnell ein einfach umzusetzender Sicherheitsmechanismus gefunden werden. Und so wurde das Passwort zum Authentikationsmerkmal Nummer eins – jeder weiß, wie es funktioniert, jeder ist in der Lage, ein Passwort auszuwählen, und es bietet nahezu unendliche Variationsmöglichkeiten, solange es in der Länge nicht beschränkt ist. Aber mit ihm sind auch einige technische und gesellschaftlich begründete Schwierigkeiten verbunden, die zu Sicherheitsproblemen führen können.

Das größte Problem ist der Nutzer selbst

Traditionelle Angriffe auf Passwörter sind recht simpel: Hacker probieren alle möglichen Buchstaben- und Zahlenkombinationen aus, bis die richtige Zusammensetzung gefunden ist. Diese Art von Angriffen wird Brute-Force-Angriff

genannt und führt durch die hohe Leistungsfähigkeit heutiger Computer schnell zum Erfolg. Zusätzlich macht sich der Angreifer zunutze, dass die meisten Anwender leicht zu merkende Buchstaben- und Zahlenkombinationen verwenden, wie ihren Namen, den des Wohnorts oder ihr Geburtsdatum. Diese Möglichkeiten werden von Angreifern als Erstes unter die Lupe genommen, zum Beispiel indem alle Wörter aus dem Duden durchprobiert werden (Wörterbuchattacke).

Das Grundproblem ist also der Internetnutzer. Denn die meisten Menschen neigen dazu, einfache kurze Passwörter zu wählen. Doch gerade in Bezug auf die Sicherheit ist die Länge

Zeichenzahl eines Passwortes	Passwort bestehend aus großen und kleinen Buchstaben sowie Zahlen (68 unterschiedliche Zeichen)	Passwort bestehend aus großen und kleinen Buchstaben sowie Zahlen und Sonderzeichen (94 unterschiedliche Zeichen)
1	8,5 Mikrosekunden	11,75 Mikrosekunden
2	0,58 Millisekunden	1,10 Millisekunden
3	0,39 Sekunden	0,10 Sekunden
4	2,67 Sekunden	9,76 Sekunden
5	3,03 Minuten	15,29 Minuten
6	3,43 Stunden	23,95 Stunden
7	9,73 Tage	93,82 Tage
8	1,81 Jahre	24,14 Jahre
9	123,14 Jahre	2.260 Jahre
10	**8.370 Jahre**	**213.350 Jahre**
11	569.380 Jahre	10,05 Millionen Jahre
12	38,72 Millionen Jahre	1,89 Milliarden Jahre

Abbildung 13: Benötigte Zeit zum Knacken eines Passwortes; gilt für DualCore-Notebook (in Abhängigkeit von der Länge und den verwendeten Zeichen)

besonders wichtig, da der Rechenaufwand bei einem Brute-Force-Angriff mit jedem weiteren Zeichen, das verwendet wird, stark ansteigt. Abbildung 13 zeigt exemplarisch die Rechenzeit, die ein aktuelles, durchschnittlich ausgestattetes Notebook benötigt, um ein Passwort durch einen Brute-Force-Angriff zu knacken. Die zweite Spalte zeigt die Rechenzeit, die ein durchschnittliches aktuelles Notebook benötigt, sofern keine Sonderzeichen verwendet werden, die dritte Spalte bezieht Sonderzeichen, also Kommata, Sternchen etc. mit ein. Großrechner oder spezielle Computer in einem kriminellen Verbund benötigen nur einen Bruchteil der angegebenen Zeiten.

Das zeichnet ein gutes Passwort aus

Ein sicheres Passwort sollte aus mindestens zehn Zeichen bestehen und sowohl Klein- als auch Großbuchstaben in Kombination mit Zahlen und Sonderzeichen verwenden – am besten in einer auf den ersten Blick sinnlosen Zusammensetzung, also zum Beispiel §BhKg%80!b. Doch ein solches Passwort zu bilden, das auch noch gut zu merken ist, stellt viele vor eine schier unlösbare Aufgabe. Aber so schwer ist es gar nicht. Mit ein paar Tricks lässt sich ein gutes Passwort sogar ziemlich einfach finden und merken.

Eine gute Hilfe sind dabei Dinge aus Ihrem Alltag beziehungsweise Dinge, die Sie besonders interessieren. Das kann Ihr Lieblingsbuch sein, die Vereine, die in der Fußballbundesliga spielen oder aber ein Kinderlied, wie das folgende Beispiel zeigt:

3KDmAR8KK!
3s **K**lappert **D**ie **m**ühle **A**m **R**auschenden **8**ach **K**lipp **K**lapp**!**

Um das Passwort zu «verbessern», wurde hier für ein «E» eine «3» verwendet und für ein «B» eine «8». Auch wurden die Wörter in ihrer Groß- und Kleinschreibung verändert und zu guter Letzt wurde ein «!» als Sonderzeichen angehängt.

Auf diese Weise ist es möglich, eine Vielzahl sehr sicherer – und trotzdem einprägsamer – Passwörter zu generieren (Softlink 311).

Der richtige Umgang mit Passwörtern

Und jetzt, da Sie endlich ein sicheres Passwort haben, das Sie sich zudem gut merken können, verwenden Sie es voller Enthusiasmus bei jedem Internetdienst, den Sie nutzen … Bitte nicht! Denn damit begehen Sie den nächsten großen Fehler und spielen einem potenziellen Angreifer in die Hände.

Angenommen, jemand schafft es tatsächlich, das Passwort für Ihr E-Mail-Konto zu knacken, dann wird er die gefundene Kombination von Benutzernamen (meist die E-Mail-Adresse oder der Name) und Passwort natürlich auch bei ebay, Amazon und bei anderen Diensten ausprobieren. Mit etwas Glück kann der Angreifer nun auf Ihren Namen im Internet einkaufen oder die Zugangsdaten für kriminelle Handlungen nutzen, die auf Sie zurückfallen. Daher ist es wichtig, für jeden Internetdienst, den Sie nutzen, ein eigenes Passwort zu verwenden. Für Foren, in denen Sie über Computer, Rezepte oder Fernsehserien diskutieren, ohne sicherheitskritische Daten zu hinterlegen, können Sie auch mal ein Passwort mehrfach benutzen. Bei Inhalten mit sicherheitskritischen Daten jedoch niemals!

TIPP: Grundsätzliches zu Passwörtern

- Wählen Sie ein mindestens zehnstelliges Passwort.
- Verwenden Sie Klein- und Großbuchstaben in Kombination mit Sonderzeichen und Zahlen möglichst in einer auf den ersten Blick sinnlosen Zusammensetzung.
- Nutzen Sie Gegebenheiten aus dem Alltag, um ein Passwort zu ersinnen (siehe Seite 53). Tauschen Sie dabei Buchstaben gegen ähnlich aussehende Zahlen aus, beispielsweise das B gegen eine 8 oder das E gegen eine 3.
- Verwenden Sie jedes Passwort nur für einen einzigen Dienst.
- Der beste Schlüssel bietet keinen Schutz, wenn ihn jemand kurzfristig entwenden und eine Kopie davon anfertigen kann. Das gilt auch für das Internet. Deshalb sollten Sie Ihre Passwörter nur eingeben, wenn zwischen Ihrem Browser und dem Webserver eine sichere Verbindung besteht, welche die Daten verschlüsselt (siehe Seite 36ff.).

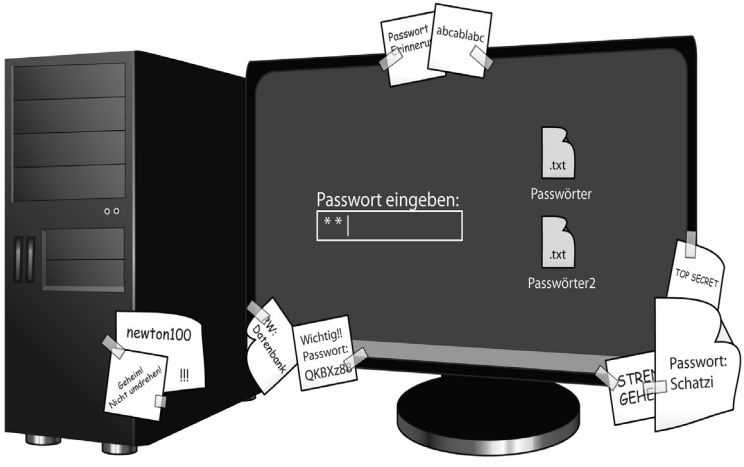


Abbildung 14: Negativ-Beispiele für die Aufbewahrung von Passwörtern

Werden sehr viele Dienste genutzt, für die Passwörter vergeben werden müssen, stoßen vielen Nutzer – was die Merkfähigkeit angeht – an ihre Grenzen, und es stellt sich die Frage: Was tun? Es gibt sehr kreative, aber leider wenig geeignete Lösungen für dieses Problem, die in der folgenden Abbildung angedeutet werden:

Denn natürlich sollten vertrauliche Daten nicht so öffentlich zur Schau gestellt werden. Eine sinnvolle Alternative sind sogenannte Passwortkarten, auf denen verschiedene Zeichenkombinationen abgebildet sind. Hier genügt es, sich lediglich bestimmte Anfangspunkte und Regeln zu merken, um ein Passwort zu hinterlegen. Beispielsweise bestimmt der Nutzer, dass ein bestimmtes Passwort bei «C/05» beginnt und ab dort zehn Stellen waagerecht verläuft, wobei jede Zeile für einen bestimmten Internetdienst steht. In Abbildung 15 wäre das Passwort «tAc8UpCpgw».

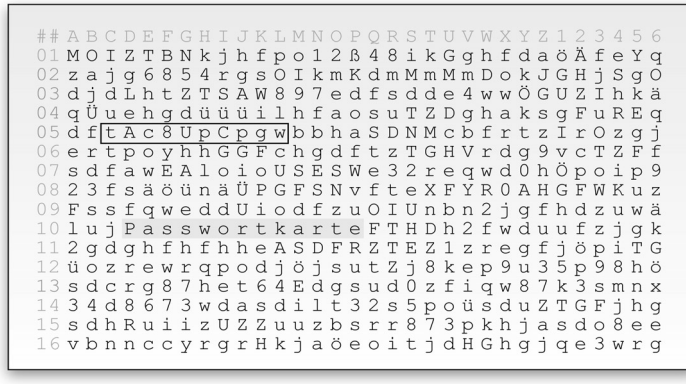


Abbildung 15: Die Passwortkarte ist eine gute Möglichkeit, um sich viele komplexe Passwörter zu merken.

Wer sehr viele Passwörter zu verwalten hat – die Autoren beispielsweise haben rund 100 Passwörter im Gebrauch –,

dem helfen Passwortspeicher. In diesen Speichern werden Passwörter verschlüsselt abgelegt, wodurch sie für niemand anderen zugänglich sind. Zusätzlich werden sie mit einem Master-Passwort geschützt. Beim Einsatz solcher Sicherheitsmechanismen muss das Master-Passwort, das den Zugang zu den gespeicherten Passwörtern schützt, den angesprochenen Sicherheitsvorgaben in besonderer Form genügen, das heißt, es sollte mindestens aus 13 Zeichen in einer kreativen, nicht nachvollziehbaren Zusammensetzung bestehen. Einige Experten empfehlen sogar ganze Sätze mit vielen Sonderzeichen. Die lassen sich meist gut merken und sind wirklich sicher.

Passwortspeicher gibt es in den unterschiedlichsten Ausführungen: als Software auf einem USB-Stick, als Programm auf dem Computer (Softlink 312) oder als Zusatzfunktion in Browsern. Letztere fragt nach einem abgeschlossenen Passwortdialog, also nachdem Sie sich mit Ihrem Benutzernamen und Passwort angemeldet haben, automatisch, ob das Passwort gespeichert werden soll (siehe Abbildung 16).



Abbildung 16: Automatische Funktion des Browsers zum Speichern von Zugangsdaten

Doch Vorsicht: Grundsätzlich kann die Passwortspeicherfunktion des Browsers nicht als ausreichend sicher betrachtet

werden. Für weniger sicherheitskritische Internetdienste, wie die Anmeldung in Foren, ist ein Einsatz möglich, beim Onlinebanking und ähnlich sensiblen Diensten sollten Sie dagegen auf diesen Service verzichten. Und vergeben Sie, falls Sie ihn verwenden, auf jeden Fall ein Master-Passwort für die Passwortspeicherung (siehe Abbildung 17). Diese Einstellung ist bei den aktuellen Browsern optional, aber absolut notwendig, um die Passwörter dem Zugriff Dritter, die denselben Computer verwenden, zu entziehen. Eingeschränkt kann ein Master-Passwort auch gegen Malware schützen, die sich auf dem Computer eingenistet hat und versucht, den Passwortspeicher auszulesen. Ist die Malware allerdings in der Lage, Tastenanschläge nachzuvollziehen oder den Hauptspeicher auszulesen, bietet auch das Master-Passwort keinen Schutz, da



Abbildung 17: Setzen Sie in den Browsereinstellungen unter dem Punkt «Sicherheit» den Haken vor «Master-Passwort verwenden», um diese Funktion zu aktivieren.

die Angreifer auf diese Weise auch an das Master-Passwort selbst gelangen.

Auch Passwortspeicher auf USB-Sticks oder die angesprochenen Programme haben unterschiedliche Sicherheitsniveaus. Am besten fragen Sie einen Fachmann oder recherchieren im Internet, ob die Lösung, die Sie nutzen wollen, für Ihre Bedürfnisse ausreichend ist. Natürlich gibt es auch in diesem Bereich frei verfügbare Tools wie beispielsweise Passwortsafe oder keepass (Workshop «keepass», siehe Softlink 312).

TIPP: Aufbewahrung von Passwörtern

- Notieren Sie Ihre Passwörter nie auf Papier, Sie machen diese sonst öffentlich zugänglich.
- Wenn Sie sich Ihre Passwörter nicht merken können, nutzen Sie kleine Helfer wie Passwortkarten oder Passwortverschlüsselungsprogramme!
- Nutzen Sie den Passwortspeicherungsservice des Browsers nur für unkritische Passwörter und nur auf Ihrem eigenen Computer. Verwenden Sie diesen aus Gewohnheit in einem Internetcafé, hat jeder Anwender, der nach Ihnen den Computer benutzt, Zugriff auf Ihre Passwörter! Verzichten Sie am besten ganz darauf.
- Besonders wichtig: Ändern Sie Ihre Passwörter regelmäßig alle drei bis sechs Monate! Tauschen Sie dabei nicht nur eine Zahl oder einen Buchstaben aus, sondern verändern Sie das Passwort stets an mehreren Stellen.

Passwort vergessen – was nun?

Es kommt natürlich vor, dass Nutzer ihr Passwort vergessen und nicht mehr auf den Internetdienst zugreifen können. Im

Normalfall gibt es für diese Situation das Helpdesk des Anbieters. Bei einem Anruf dort kann der Kundendienst im Normalfall weiterhelfen. Um diesen Vorgang zu vereinfachen und vor allem um Kosten für den Anbieter zu sparen, gibt es beim Einrichten eines personalisierten Internetdienstes häufig auch eine Möglichkeit zur Selbsthilfe für den Fall von akuter Vergesslichkeit. Wenn ein Nutzer zum Beispiel eine E-Mail-Adresse einrichtet, wird er aufgefordert, neben seinem Passwort auch Antworten auf verschiedene Fragen zu geben:

- Wie heißt Ihr Hund?
- Wie heißt Ihre beste Freundin?
- Wie lautet der Mädchenname Ihrer Mutter?

Im Verlustfall wird der Anwender dann auf eine Webseite geleitet, auf der ihm eine oder mehrere dieser Fragen gestellt werden. Beantwortet der Nutzer die Fragen richtig, wird das Passwort zurückgesetzt, und er kann ein neues wählen.

Der Grundgedanke dieser Selbsthilfemaßnahme ist nicht schlecht, aber unter Sicherheitsgesichtspunkten bedenklich. Denn bei einem Angriff dürfte es einfacher sein, diese Funktion auszuhebeln und das Passwort zurückzusetzen, als das Passwort selbst zu finden. Der Mädchenname der Mutter oder ähnliche Informationen sind meist leicht herauszufinden, besonders im Falle eines gezielten Angriffs. Die Anbieter müssen deshalb in diesem sensiblen Bereich nachbessern. Als Internetnutzer sollten Sie diese Funktion entweder meiden oder sich sicherheitstechnisch intelligente Antworten auf die Fragen überlegen. Beispielsweise könnten Sie die Namen nach einem bestimmten Schema verschlüsseln, indem Sie zwischen jeden Buchstaben eine Zahl oder ein Sonderzeichen setzen. Die Antwort auf die Frage nach dem Namen Ihres Hundes könn-

te dann zum Beispiel so aussehen: F!r1i!d1o!l1i!n1!. Stehen mehrere Fragen zur Auswahl, ist es klug, nur eine zu nutzen, denn je mehr mögliche Fragen und Antworten es gibt, desto mehr Angriffsfläche bieten Sie dem Angreifer.

Ausblick: der elektronische Personalausweis

Der Siegeszug des Passwortes scheint ungebrochen, aber der Druck, einen höheren Sicherheitslevel bei der Authentikation zu erreichen, ist enorm. Deshalb hat die Bundesrepublik mit dem neuen elektronischen Personalausweis eine Infrastruktur zur Verfügung gestellt, um den Identitätsnachweis im Internet für die Bundesbürger sicherer zu machen. Der Staat hat mit seiner Personalausweis-Infrastruktur natürlich auch optimale Voraussetzungen, dies umsetzen zu können.

Standes- und Melde- beziehungsweise Bürgerämter sichern die eindeutige und überprüfbare Identität von Personen: Das Standesamt sorgt dafür, dass wir über unseren Vor- und Nachnamen, den Geburtsort und das Geburtsdatum eindeutig identifizierbar sind. Das Melde- beziehungsweise Bürgeramt gibt die Personalausweise heraus, die es ermöglichen, diese eindeutige Identität zweifelsfrei nachzuweisen.

Ab November 2010 wird der elektronische Personalausweis im Scheckkartenformat, der mit einem kontaktlosen Sicherheits-Chip ausgestattet ist, den bisherigen Personalausweis ablösen. Der neue elektronische Personalausweis wird wie der alte Personalausweis für hoheitliche Kontrollen an Grenzen und im Inland verwendet.

Zusätzlich ist der elektronische Personalausweis aber mit der Funktion des elektronischen Identitätsnachweises (Authentikationsfunktion) ausgerüstet. Damit ist er auch ein Ausweis,

mit dem sich sein Besitzer im Internet sicher identifizieren und authentisieren lassen kann. Dazu muss der genutzte Computer mit einem Kartenleser und der zugehörigen Software (Bürgerclient) ausgerüstet sein. Das Besondere am Sicherheitskonzept des elektronischen Personalausweises ist, dass nur berechtigte Anbieter von Dienstleistungen in der Lage sind, die Daten des Ausweises abzufragen. Um diese Berechtigung zu erlangen, muss der jeweilige Anbieter ein entsprechendes Zertifikat beim Bundesverwaltungsamt beantragen, in dem genau definiert ist, was er kryptographisch (verschlüsselt und integritätsgesichert) auslesen darf – insbesondere im Hinblick auf den Daten- und Verbraucherschutz. Zudem behalten Sie als Ausweisinhaber stets die volle Kontrolle darüber, welche Ihrer persönlichen Daten an den Anbieter übermittelt werden. Wenn dieser mit dem Berechtigungszertifikat auf den Ausweis zugreift, werden Sie darüber informiert, was der berechtigte Anbieter auslesen darf, und können den Vorgang teilweise oder ganz untersagen.

Generell kann der elektronische Personalausweis nur ausgelesen werden, wenn der Nutzer diesen über die Eingabe einer PIN aktiviert. Diese PIN wird aber lediglich für die Aktivierung des Sicherheits-Chips auf dem Ausweis verwendet. Die eigentliche Verifikation erfolgt über sehr sichere Kryptographie-Protokolle zwischen dem Sicherheits-Chip auf dem elektronischen Personalausweis und einem Sicherheitsmodul der verifizierenden Stelle. Das Plus an Sicherheit liegt darin begründet, dass der Identifikationsnachweis nur mit dem Besitz des elektronischen Personalausweises *und* der PIN möglich ist, also mit der Kombination aus Besitz (elektronischer Personalausweis) und Wissen (Passwort). Darüber hinaus bietet der neue elektronische Personalausweis die

Möglichkeit, ein Zertifikat für die qualifizierte elektronische Signatur auf den Personalausweis zu laden. Damit sind die Besitzer dann auch in der Lage, online zu unterschreiben, zum Beispiel Verträge (Softlink 313).

TIPP: Elektronischer Personalausweis

- Geben Sie den elektronischen Personalausweis mit der passenden PIN nie weiter – auch nicht an Verwandte und Freunde!
- Legen Sie den elektronischen Personalausweis nur auf den Leser, wenn Sie sich im Internet damit anmelden wollen.
- Sorgen Sie dafür, dass der Basisschutz (siehe Seite 10ff.) stets gewährleistet ist.

E-Mail – von digitalen Postkarten und falschen Absendern

Die E-Mail ist das meistverwendete Kommunikationsmittel unserer modernen Gesellschaft. Es werden natürlich immer noch Briefe und Postkarten geschrieben, aber die meisten Informationen werden inzwischen per E-Mail versandt. Die Vorteile der E-Mail liegen auf der Hand: Sie ist meist innerhalb weniger Sekunden beim Adressaten und kann sofort bearbeitet werden.

Zusätzlich können Dateien an die E-Mail gehängt und sehr einfach und schnell ausgetauscht werden – ganz ohne Medienbruch. Auch sind E-Mails deutlich kostengünstiger als Briefe und Postkarten, was für viele, neben der Geschwindigkeit, sicher das wichtigste Argument ist. Doch wie steht es mit der Vertraulichkeit? Jeder weiß, dass man Vertrauliches nicht

auf eine Postkarte schreiben sollte, da jeder den Inhalt lesen kann. Bei einem Brief ist das anders, auch wenn es da ein paar kriminelle Tricks gibt, bei denen Wasserdampf eine Rolle spielt. Und wie sieht es bei der E-Mail aus? Um diese Frage beantworten zu können, ist es hilfreich zu verstehen, wie der E-Mail-Austausch vonstattengeht.

So funktioniert der E-Mail-Austausch im Internet

Damit eine E-Mail ihren Bestimmungsort erreicht, muss sie in einen digitalen Briefkasten geworfen werden. Diesen stellt der E-Mail-Anbieter, auch Provider genannt, zur Verfügung. Der E-Mail-Anbieter des Senders versendet die E-Mail an den Empfänger beziehungsweise an dessen E-Mail-Anbieter, was mit dem Transport von Briefen zwischen den verschiedenen Verteilerzentren vergleichbar ist. Der E-Mail-Anbieter des Empfängers liefert die E-Mail dann – genau wie ein Postbote – an das entsprechende Postfach des Empfängers. Daher heißt es E-Mail-Postfach.

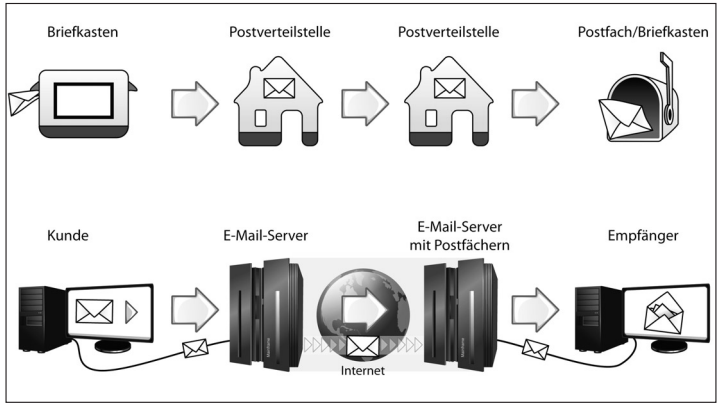


Abbildung 18: Der Postweg – real und virtuell

Die E-Mail-Adresse

Alle für die Zustellung nötigen Angaben beinhaltet die E-Mail-Adresse: Der erste Teil (vor dem @-Zeichen) gibt den konkreten Empfänger an – die E-Mail-Adresse norbert.pohlmann@sicher-im-internet.de kann beim E-Mail-Anbieter sicher-im-internet.de nur einmal vorhanden sein. Der zweite Teil (nach dem @-Zeichen) gibt die entsprechende Domain und damit meistens den Namen des E-Mail-Anbieters oder einer Firma an, also zum Beispiel gmx.de, t-online.de, yahoo.de oder siemens.de, otto.de, allianz.de. Sie ist mit der Adressangabe auf einem Brief vergleichbar.

Viele Anbieter wie GMX, WEB.DE, freenet und Google stellen Ihnen kostenlos eine E-Mail-Adresse mit Postfach zur Verfügung, wobei es eventuell überlegenswert ist, diese aufzuwerten. Meist erhalten Sie schon für ein geringes Entgelt deutlich mehr Speicherplatz für Ihr Postfach sowie zusätzliche Sicherheits- und Komfortfunktionen.

Verwalten können Sie Ihre E-Mails beziehungsweise Ihr E-Mail-Postfach auf zwei Arten: online im Internet per sogenanntem Webmailer mithilfe des Browsers oder lokal auf dem Computer über ein Programm, den sogenannten E-Mail-Client. Beispiele für E-Mail-Clients sind Mozilla Thunderbird, Microsoft Outlook oder The Bat. Natürlich können Sie auch beide Varianten parallel nutzen. Den Webmailer-Zugang stellt in der Regel der E-Mail-Anbieter zur Verfügung. Er hat den Vorteil, dass Sie von überall auf Ihr Postfach zugreifen können (über die Webseite des E-Mail-Anbieters). Allerdings müssen Sie zur Bearbeitung Ihrer E-Mails permanent online sein. Mit einem E-Mail-Client ist es dagegen möglich, auch offline zu arbeiten und nur für den Versand beziehungsweise den Empfang von E-Mails online zu gehen. Die E-Mail-

Clients bieten außerdem mehr Komfortfunktionen und ermöglichen die gleichzeitige Verwaltung mehrerer E-Mail-Adressen.

Wie Sie Ihre E-Mails verwalten, ist letztlich eine Frage des persönlichen Geschmacks. Bei permanenter Nutzung und mehreren Konten ist der E-Mail-Client aber mit Sicherheit die komfortablere Variante (Einstellungen, siehe Softlink 327).

TIPP: E-Mail-Verwaltung

Fragen Sie Ihre E-Mails nur selten oder von ständig wechselnden Computern aus ab, ist ein Webmailer-Zugang für Sie die praktischere Variante.

Wollen Sie mehrere E-Mail-Adressen komfortabel verwalten, sollten Sie sich – zusätzlich zum Webmailer-Zugang – für einen E-Mail-Client entscheiden.

Der richtige Umgang mit E-Mail-Adressen

In Telefonbüchern kann jeder seine Telefonnummern mitsamt der Anschrift angeben lassen. Seit einigen Jahren achten die Kunden jedoch immer mehr darauf, dass nur die Telefonnummer in den Telefonbüchern auftaucht, um einen Missbrauch der Daten durch Dritte zu erschweren. Inzwischen gehen viele sogar dazu über, den Telefonbucheintrag komplett zu streichen – in Zeiten von ständig zunehmender und immer aggressiver betriebener Telefonwerbung durchaus verständlich. Genau aus dem gleichen Grund sollten Sie auch Ihre E-Mail-Adresse – ebenso wie Ihre anderen persönlichen Daten – nicht leichtfertig preisgeben. Es ist sogar sinnvoll, sich mehrere E-Mail-Adressen zuzulegen und diese je nach Aktivität einzusetzen. Ihre «seriöse» Hauptadresse verwenden Sie

für Ihre Bankgeschäfte, das Buchen von Tickets, den Onlineeinkauf und die Kommunikation mit der Familie und guten Freunden. Im Geschäftsleben wählen Sie die Firmenadresse, also zum Beispiel Linnemann@internet-sicherheit.de. Und schließlich benötigen Sie eine möglichst anonyme E-Mail-Adresse wie ML04@googlemail.com Die kommt dann bei all den Gelegenheiten zum Einsatz, bei denen Sie nicht abschätzen können, wie die jeweiligen Dienste mit Ihren Daten umgehen, also in Foren, Blogs, bei Umfragen etc. Es kann nämlich leicht sein, dass Sie in der Folge mit Spam (siehe Seite 78 ff.) geradezu überschüttet werden – und es ist nicht ganz so ärgerlich, wenn das bei einem Postfach passiert, das ohnehin nicht für den regulären E-Mail-Verkehr gedacht war.

Ein weiteres Übel sind die sogenannten Harvester, die das Internet nach E-Mail-Adressen absuchen («crawlen») und diese sammeln, um anschließend Spam an sie zu versenden. Deshalb sollten Sie Ihre E-Mail-Adressen entsprechend schützen, wenn Sie sie auf privaten oder beruflichen Webseiten nennen. Das gilt auch für Dokumente, die auf einer Webseite abrufbar sind, egal ob es sich dabei um Office-Dokumente, PDFs oder PowerPoint-Präsentationen handelt. Denn gerade in solchen Dokumenten befinden sich in der Regel personenorientierte E-Mail-Adressen.

Eine einfache Gegenmaßnahme ist das «Verschleiern» der E-Mail-Adresse (Softlink 321), zum Beispiel nach folgendem Muster:

Originaladresse:
Linnemann@internet-sicherheit.de

Verschleierte Darstellung mit Leerzeichen und Umschreibungen:
Linnemann [at] internet – sicherheit [dot] de

Doch nicht nur die eigene E-Mail-Adresse muss geschützt werden, sondern auch fremde. Ein besonderer Fall ist der Versand von E-Mails an mehrere Empfänger. Hier sollten die E-Mail-Adressen der Empfänger in das Adressfeld «Bcc» eingetragen werden (siehe Seite 70). Als Empfänger in «An» wird dann meist die Absenderadresse eingetragen. So bekommen alle die E-Mail, sehen aber nur den Absender und nicht die weiteren Adressaten, welche die E-Mail ebenfalls bekommen haben.

Allerdings kann es manchmal auch gewünscht sein, dass alle sehen, wer sonst noch im Verteiler steht, zum Beispiel bei einer Geburtstagsüberraschungsparty.

Übrigens: Wenn eine E-Mail an sehr viele Adressaten (weit über 100) im An- oder Cc-Feld verschickt wird, können entsprechende Kontrollinstanzen im Internet das erkennen und den Absender als Spammer einstufen. Das hat zur Folge, dass dessen E-Mails nicht mehr zugestellt werden.

TIPP: Umgang mit E-Mail-Adressen

- Gehen Sie grundsätzlich vorsichtig mit Ihren privaten Daten wie E-Mail-Adresse, Name, Alter und Anschrift um. Viele Firmen verkaufen Datensätze, die dann für Werbezwecke verwendet werden.
- Geben Sie Ihre E-Mail-Adresse nur an Personen, die Sie kennen und/oder denen Sie vertrauen!
- Nutzen Sie je nach Aktivität verschiedene E-Mail-Adressen.
- Verschleiern Sie Ihre E-Mail-Adresse auf Dokumenten und Webseiten im Internet, um E-Mail-Harvestern zu entgehen.
- Nutzen Sie das Bcc-Feld, wenn Sie E-Mails an eine große Gruppe von Adressaten versenden, um nicht sämtliche E-Mail-Adressen für alle sichtbar zu machen.

Die wichtigsten Verhaltensregeln beim E-Mail-Austausch

Die Kommunikation via E-Mail ist im privaten und beruflichen Leben für viele bereits selbstverständlich geworden. Die Vorteile des schnellen und kostengünstigen Austauschs von Informationen und Dateien sind enorm, und man möchte sie nicht mehr missen.

Der richtige Umgang mit der E-Mail-Anwendung ist jedoch noch nicht optimal etabliert. Aus diesem Grund werden einige Verhaltensregeln beschrieben, die für alle Beteiligten bei der richtigen Umsetzung hilfreich sind. Diese Regeln helfen auch, die Vertrauenswürdigkeit von E-Mails besser einschätzen zu können.

Inhalt und Form

Jeder, der eine E-Mail schreibt, sollte sich genau überlegen, was er dem oder den anderen eigentlich mitteilen möchte. Die Tatsache, dass eine E-Mail schnell verfasst ist und kein Porto kostet, ist kein Grund, andere mit Belanglosigkeiten zu bombardieren. Auch ist die Unkompliziertheit des Mediums kein Freibrief für formale Nachlässigkeit. Ein freundlicher Umgangston, korrekte Rechtschreibung, Anrede und Schlussformel sowie eine übersichtliche Struktur sollten in einer E-Mail ebenso selbstverständlich sein wie in einem «normalen» Brief. Dazu gehört auch, dass die Betreffzeile immer einen aussagekräftigen Hinweis auf den Inhalt der E-Mail enthält.

Der oder die Empfänger

In einer E-Mail können verschiedene Kategorien von Empfängern definiert werden:

- Das Feld «An» (To) gibt die E-Mail-Adresse von primären Empfängern an. Hier sollten Sie nur Empfänger eintragen, von denen Sie eine Reaktion erwarten.
- Das Feld «Cc» (Carbon Copy = Durchschlag) gibt die E-Mail-Adressen der sekundären Empfänger an, die den Inhalt der E-Mail lediglich zur Kenntnis nehmen sollen. Bei der Zustellung wird zwischen primären und sekundären Empfängern nicht unterschieden.
- Das Feld «Bcc» (Blind Carbon Copy) hat die gleiche Bedeutung wie das Feld «Cc» – mit dem Unterschied, dass die Zeile «Bcc» in den Kopien, die an die verschiedenen Empfänger gesendet werden, nicht sichtbar ist. Das ermöglicht Ihnen, eine E-Mail an eine Gruppe von Empfängern zu schicken, ohne dass jeder die E-Mail-Adressen der anderen sieht (siehe Seite 68).

Die Antwort

Die E-Mail wird sehr schnell an den Empfänger ausgeliefert, der sich bemühen sollte, diese auch zügig zu beantworten. Im Geschäftsleben erwartet der Absender heute eine Antwort innerhalb eines Werktages. Wenn Sie also wissen, dass Sie nicht so schnell reagieren können, sollten Sie eine automatische Abwesenheitsnotiz versenden, die den Sender darüber informiert, dass Sie nicht da sind und ab wann er Sie wieder erreichen kann. Die entsprechende Autoresponder-Funktion bietet inzwischen fast jeder E-Mail-Anbieter an (Softlink 322).

Nutzen Sie zudem die Antworten-Funktion, damit der ursprüngliche Text wieder mit zurückgeschickt wird. So weiß der Empfänger auf einen Blick, worauf Sie sich beziehen. Dabei sollte der alte Text immer unten stehen und Ihre Antwort oben. Geht eine E-Mail mehrfach hin und her, sollten Sie sie

zwischendurch neu anlegen, damit sie nicht unendlich lang wird.

Die Signatur

Die Signatur ist ein Text, der an das Ende einer E-Mail angehängt wird und Informationen über den Absender enthält. Sie erleichtert die Kontaktaufnahme, zum Beispiel im Falle einer telefonischen Rückfrage, zeigt die rechtliche Stellung des Absenders (bei Unternehmen gesetzlich vorgeschrieben) und hilft bei der Einschätzung der Vertrauenswürdigkeit des Absenders. Die Signatur kann automatisch durch den E-Mail-Client oder Webmailer eingefügt werden.

TIPP: Vertrauenswürdigkeit einer E-Mail

Bei der Einschätzung, ob eine E-Mail vertrauenswürdig ist oder nicht, können neben der Signatur auch folgende Aspekte hilfreich sein:

- Sind Aufbau und Inhalt der E-Mail für Sie klar nachvollziehbar?
- Ist Ihnen der Absender oder die Organisation, von der die E-Mail kommt, persönlich bekannt oder haben Sie zumindest eine Vorstellung, warum Sie diese E-Mail bekommen?
- Wird Ihnen in der E-Mail ein Angebot gemacht, das unrealistisch ist (Geschenke)?
- Haben Sie die E-Mail erwartet?

E-Mails – Angriffe und Gefahren

Folgendes Szenario kann so oder so ähnlich überall passieren: Eine Angestellte versendet von ihrem Arbeitsplatz eine E-Mail an ihre Freundin im Büro nebenan, mit vielen intimen Einzelheiten zu ihrer heimlichen Beziehung mit dem Chef. Kurz

darauf erhalten alle Mitarbeiter des Unternehmens diese E-Mail von einem unbekannten Absender. Die E-Mail wurde «abgefangen» und veröffentlicht. Eine höchst unangenehme Situation für die Angestellte und natürlich auch für den Chef. Was ist passiert?

Eine E-Mail zu verschicken ist nichts anderes als eine Postkarte zu versenden, sprich: Jeder, der die E-Mail «in die Finger bekommt», kann sie auch lesen. Das ist den meisten Nutzern nur nicht bewusst. So kann zum Beispiel der E-Mail-Anbieter sämtliche E-Mails lesen, die über ihn verschickt werden (ob er es darf, ist eine andere Frage), aber auch jeder, der Zugriff auf das Netzwerk hat, in dem Sie sich befinden – sowohl am Arbeitsplatz als auch im Internetcafé. Deshalb sollten Sie sensible Daten niemals per E-Mail versenden, ohne entsprechende Vorsichtsmaßnahmen zu treffen (siehe Seite 82 f.). Und es lauern noch weitere Gefahren …

Vermeintlich vertrauenswürdige E-Mails

In Ihrem E-Mail-Postfach befindet sich eine E-Mail mit dem Absender eines guten Freundes. Laut Betreff bietet er Ihnen darin günstig Viagra-Tabletten an, oder er verweist per Link auf eine tolle Seite im Internet. Da Ihnen das seltsam vorkommt, fragen Sie nach. Das Ergebnis: Er versichert Ihnen glaubhaft, dass diese E-Mail nicht von ihm stammt. Wie aber kann das sein?

Der Absender kann bei E-Mails frei benannt werden – genau wie bei einer Postkarte. Dort können Sie als Absender auch den Namen des Bürgermeisters verwenden (wobei wir hierbei davon ausgehen, dass Sie nicht der Bürgermeister sind). Der Absender ist also kein Indiz für die Vertrauenswürdigkeit der E-Mail.

Das ist aus Betrügersicht natürlich eine hervorragende Grundlage für einen Angriff, nämlich mit E-Mails, die von einem vermeintlich vertrauenswürdigen Absender stammen und einen auf den ersten Blick interessanten Link beinhalten. Klicken Sie deshalb niemals auf Links, wenn Sie nicht genau wissen, worum es sich dabei handelt. Der Link könnte beispielsweise auf eine infizierte Webseite leiten, wodurch Malware auf den Computer geladen wird, die Ihre Daten ausspioniert und/oder die Kontrolle über Ihren Computer übernimmt. Auch der Link ist letztlich nur ein Text, der frei eingegeben werden kann. Ohne eine Kontrolle können Sie sich deshalb nie sicher sein, ob er Sie tatsächlich zu der angekündigten Webseite führt.

Bedeutet das jetzt, dass Sie nie wieder einen Link anklicken dürfen? Grundsätzlich natürlich nicht. Es gibt verschiedene Anhaltspunkte, anhand derer Sie drohende Gefahren erkennen können und die sich sehr schnell überprüfen lassen. Das Wichtigste ist wiederum, dass Sie bei der Bearbeitung Ihrer E-Mails gesunden Menschenverstand walten lassen. Warum sollten Sie einer E-Mail Beachtung schenken, die eine seltsame Information enthält oder in einer Sprache geschrieben ist, die der Absender normalerweise nicht verwendet? Bei Unsicherheit hilft es, den Freund oder Geschäftspartner einfach anzurufen, der die E-Mail geschickt hat, und nachzufragen, was es damit auf sich hat. Die meisten Angriffsversuche lassen sich so bereits abwehren. Zudem ist es immer ratsam, das Ziel eines Links durch Darüberfahren mit der Maus zu überprüfen (siehe Abbildung 19 sowie Seite 29 f.).

Grundsätzlich gibt es zwei Möglichkeiten, um auf eine solche E-Mail, wie sie Abbildung 19 zeigt, nicht hereinzufallen. Bei dieser E-Mail handelt es sich um eine HTML-Mail.

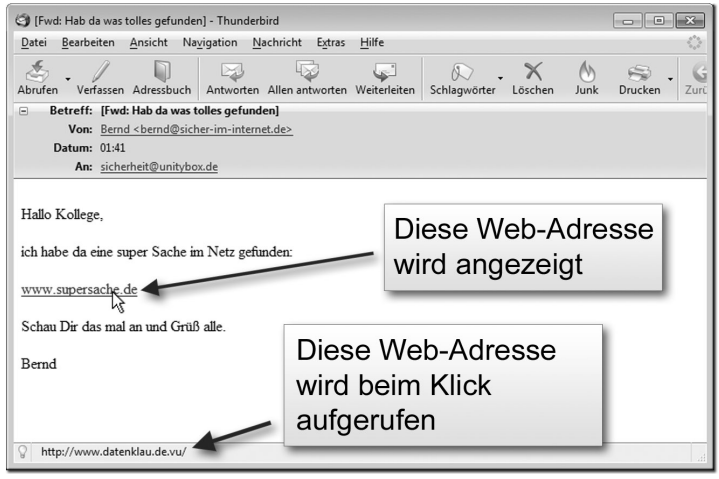


Abbildung 19: Gefälschte HTML-Mail im E-Mail-Client

Das bedeutet, dass sie wie eine Webseite aufgebaut ist und im Hintergrund mehr steht, als vordergründig zu sehen ist. Jedes

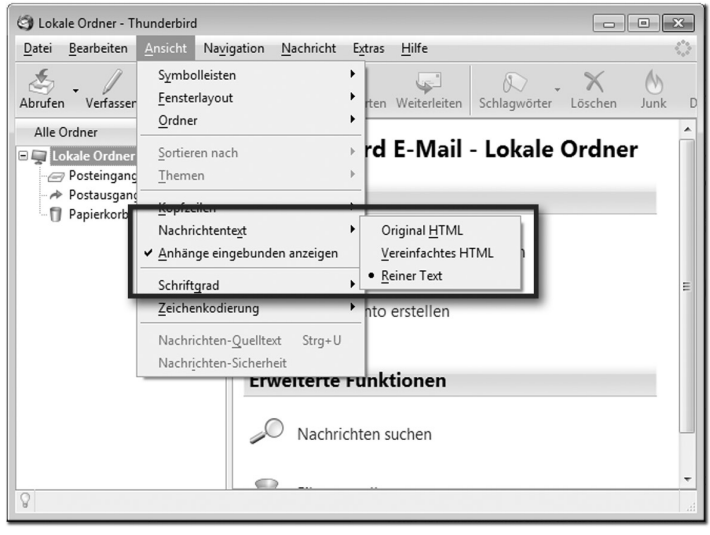


Abbildung 20: Umstellen der E-Mail-Ansicht von HTML zu reinem Text

E-Mail-Programm bietet aber die Möglichkeit, E-Mails in reiner Textform anzuzeigen (siehe Abbildung 20). Dann ist auf den ersten Blick zu erkennen, wohin ein Link führt, und es werden keine versteckten Befehle ausgeführt (siehe Abbildung 22).

Selbstverständlich können HTML-Mails nach der Überprüfung im «Nur-Text-Modus» wieder auf HTML umgestellt werden. Auch dabei ist allerdings Vorsicht geboten, da in HTML-Mails aktive Inhalte (siehe Seite 31 ff.) eingebettet sein können.

Dieselbe Problematik besteht beim Webmailer (siehe Abbildung 21), wobei manche E-Mail-Anbieter heute bereits darauf hinweisen, wenn die E-Mail HTML-Inhalte enthält. Dementsprechend gilt es auch hier, erst den Link zu kontrollieren, bevor ein Klick ausgeführt wird. Zwar sind inzwischen sowohl die Onlineangebote über Webmailer als auch die E-Mail-Clients auf den Computern mit Vorkehrungen verse-

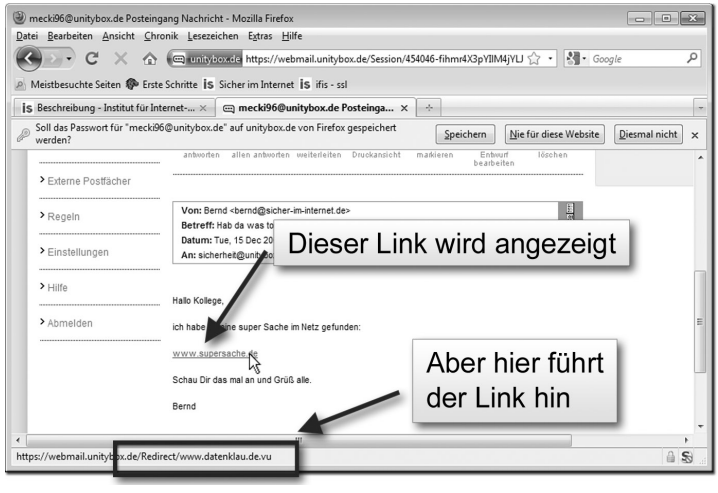


Abbildung 21: Gefälschte HTML-Mail bei einem Webmailer

hen, welche die gängigsten «bösen» Links erkennen, aber allein darauf sollten Sie sich nicht verlassen. Sie wissen ja: Vorsicht ist besser als Nachsicht.

Die zweite Möglichkeit, den Betrug zu durchschauen, ist die Kontrolle der sogenannten Headerdaten. Sowohl der E-Mail-Client als auch der Webmailer enthüllt in einer entsprechenden Einstellung «konkretere» Daten zum Absender, sodass Sie diese mit der im Feld «Von» angezeigten Adresse abgleichen können (siehe Abbildung 22). Die dazu notwendigen Kopf- oder Headerdaten rufen Sie auf, indem Sie im E-Mail-Client über den Menüpunkt «Ansicht» auf den Punkt «Kopfzeilen anzeigen» klicken. Je nach Webmailer können die einzelnen Benennungen ein wenig variieren. Suchen Sie in diesem Fall nach einer ähnlichen Webmailer-Einstellung. Die Daten, die im Header einer Mail angezeigt werden, sind für den Laien allerdings schwer zu lesen. Manchmal offenbart sich hier direkt die echte Absenderadresse, aber das muss nicht so sein (siehe Abbildung 22).

Mit geübtem Auge kann man in Abbildung 22 sehen, von welchem Mail-Server die E-Mail gekommen ist, was durchaus aufschlussreich sein kann. Zugegeben, hier sind einige Fachkenntnisse vonnöten, aber es zeigt, dass betrügerische E-Mails sehr wohl entlarvt werden können. Allerdings ist auch diese Methode kein 100-prozentiger Schutz, da Absender-E-Mail-Adressen so gefälscht werden können, dass es selbst im Header nicht zu erkennen ist. Es ist sogar möglich, E-Mails von sich selbst zu erhalten, die man nie losgeschickt hat.

Übrigens: In der reinen Textansicht wäre der Link, der sich in der HTML-Mail hinter «www.superSache.de» verbirgt, ebenfalls sichtbar – nämlich «www.datenklau.de». Generell sollten Sie Links in E-Mails niemals anklicken, wenn die

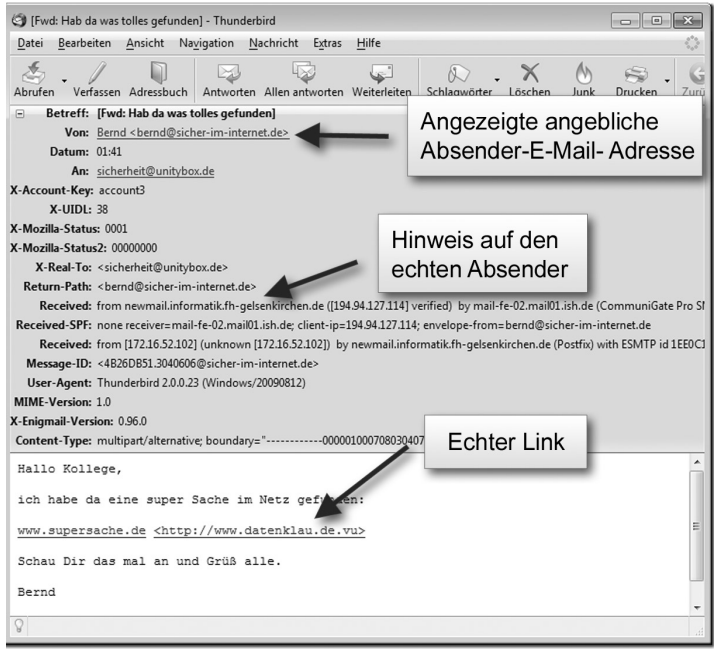


Abbildung 22: Hier wird die E-Mail als reiner Text mit vollständigem Header (Quelltext des E-Mail-Headers) angezeigt.

E-Mail nicht vertrauenswürdig ist. Suchen Sie ein in der E-Mail angegebenes Thema lieber «per Hand» im Internet oder geben Sie bei bekannten Links das Ziel auch per Hand in den Browser ein.

TIPP: Abwehr von E-Mail-Angriffen

- Versenden Sie sensible Daten niemals per E-Mail, ohne entsprechende Vorsichtsmaßnahmen zu treffen (siehe Seite 82 f.).
- E-Mails, die Ihnen seltsam vorkommen, sollten Sie umgehend löschen. Sind Sie sich nicht sicher, kontaktieren Sie den Absender, um nachzufragen – aber natürlich nicht über die Antwort-Funktion!

- Fahren Sie mit der Maus über jeden Link und überprüfen Sie in der Statusleiste dessen Zieladresse, bevor Sie ihn anklicken. Ist die E-Mail nicht absolut vertrauenswürdig, verzichten Sie darauf. Suchen Sie das in der E-Mail angegebene Thema dann lieber «per Hand». Auch Ihnen bereits bekannte Adressen sollten Sie besser manuell in den Browser eingeben, anstatt sie per Link anzusteuern.
- Empfangen Sie E-Mails möglichst in reiner Textform und bearbeiten Sie sie nicht als HTML-Mail.
- Kontrollieren Sie – sofern Sie bereits über einige Computerkenntnisse verfügen – beim geringsten Verdacht den Quelltext des E-Mail-Headers und vertrauen Sie nicht blind auf die Absenderadresse.

Spam

SPAM war ursprünglich ein Markenname für Dosenfleisch. Die Übernahme des Begriffs als Bezeichnung für unerwünschte Nachrichten lässt sich unter anderem auf einen Sketch aus der englischen Comedyshow «Monty Python's Flying Circus» zurückführen. Doch leider ist das Thema Spam im Internet weniger amüsant. Spam-E-Mails, in einigen E-Mail-Programmen auch als Junk bezeichnet, sind unerwünschte, wert-, nutz- und sinnlose Nachrichten. Sie stellen derzeit vermutlich das größte Problem im Internet dar, denn rund 95 Prozent des gesamten E-Mail-Verkehrs sind Spam, also E-Mails, die keiner haben möchte.

Die Gefahren, die von ihnen ausgehen, sind vielschichtig. Die reine Werbemail möchte Sie meist nur dazu verleiten, ein bestimmtes Produkt zu kaufen. Es kann sich dahinter aber auch ein Angriff auf Ihre persönlichen Daten verbergen. Entsprechende Links können Sie, wie bereits auf Seite 31 ff.

beschrieben, auf Seiten führen, die direkt Trojanische Pferde auf Ihren Computer laden. Die Folge ist der Kontrollverlust über den Computer und die Dateien. Phishing-Mails haben es auf Ihre Bankdaten abgesehen und werden im Abschnitt «Onlinebanking» genauer erläutert (siehe Seite 98 ff.). Darüber hinaus gibt es eine bestimmte Sorte von Spam-Mails, Jamaika-E-Mails genannt, in denen Ihnen eine Provision versprochen wird, wenn Sie eine bestimmte Summe Geld entgegennehmen und weiterüberweisen. Auf dieses Angebot sollten Sie keinesfalls eingehen und die E-Mail sofort löschen, denn hier wird Geldwäsche betrieben oder aber ein Versuch gestartet, Ihnen Geld aus der Tasche zu ziehen. Leider fallen immer wieder Menschen auf diesen Trick herein und verlieren dadurch viel Geld.

Denken Sie daran: Auch im Internet wird kein Geld verschenkt!

Oftmals enthalten Spam-Mails auch Viren, Würmer und andere Malware, die Sie jedoch mit einem entsprechenden Sicherheitsprogramm entschärfen können (siehe Seite 11 ff.). Die meisten Security Suiten enthalten zudem einen Spam-Filter, der Ihnen hilft, das Problem Spam in den Griff zu bekommen (Softlink 323).

TIPP: Schutz vor Spam-Mails

- Nutzen Sie Spam-Filter, um Ihr Postfach möglichst Spam-frei zu halten. Diese werden auch von vielen E-Mail-Providern angeboten.
- Ignorieren Sie E-Mails, mit denen Sie nichts anfangen können, einfach und löschen Sie sie ungeöffnet.
- Öffnen Sie keine E-Mails, die Ihnen seltsam vorkommen. Wenn jemand, den Sie nicht kennen, wirklich etwas von Ihnen

möchte, wird er sich – wenn es wichtig ist – auch telefonisch melden oder eine E-Mail so verfassen, dass Sie sie von Spam unterscheiden können.
- Folgen Sie niemals irgendwelchen dubiosen Aufforderungen wie Geldüberweisungen für Erbschaften oder Ähnlichem.
- Kaufen Sie keine Ware oder Dienstleistung, die mittels Spam-Mail beworben wird. Wenn niemand mehr auf diese Angebote eingeht, wird Spam als Marketinginstrument uninteressant.

Hoax – falsche E-Mails

Hoax-E-Mails warnen klassischerweise vor angeblichen Viren oder anderen Gefährdungen: «Ein sehr gefährlicher Virus verbreitet sich aktuell sehr schnell. Sie erkennen ihn an dem Betreff , …'. Löschen Sie E-Mails mit diesem Betreff sofort und leiten Sie diese Warnung auch an andere weiter, damit der Virus sich nicht weiter verbreitet.»

Die Botschaft klingt im ersten Moment sehr hilfsbereit, ist aber nur eine Täuschung. Diese, als Hoax bezeichneten Nachrichten, sind nämlich völlig haltlos. Sie spielen mit der Angst des Anwenders, beinhalten selbst einen Virus oder dienen dem Sammeln von E-Mail-Adressen für Spam-Zwecke. Sie können sie also getrost löschen, selbst wenn Sie mittlerweile sogar mit dem Tod bedroht werden, falls Sie sie nicht weitersenden. Häufig enthalten diese E-Mails auch Verweise auf bekannte Organisationen wie Microsoft und verfügen über einen Absender, der auf den ersten Blick über jeden Zweifel erhaben ist (Polizei, Krankenhaus usw.). Doch lassen Sie sich davon nicht täuschen! Eine Liste bekannter Hoax-Mails finden Sie unter Softlink 324.

E-Mail-Anhänge

Auf zwei Arten können E-Mails direkt, also ohne erst auf einen Link zu klicken, für den Computer gefährlich werden. Erstens, indem sie HTML-Code beziehungsweise JavaScript enthalten. Das können Sie mithilfe entsprechender Einstellungen ausschließen (siehe Seite 74ff.). Die zweite Möglichkeit ist, dass sich die Schadsoftware im Anhang befindet. Das ist zugleich die einfachste Form eines Angriffs. Ein solcher Virus, Wurm oder ein solches Trojanisches Pferd wird aber nur gefährlich, wenn Sie den Anhang auch öffnen.

Besonders problematisch sind selbstausführende Dateien – vermeintlich schnell erkennbar an der Endung «.exe» –, deren Ausführung die direkte Installation einer Schadsoftware auf Ihrem Computer zur Folge haben kann. Aber die Angreifer sind schlauer geworden und verbergen die Exe-Dateien in anderen Dateiformaten (zum Beispiel pdf, doc oder avi) oder nutzen Sicherheitslücken in Office- und Multimediaprogrammen. Doch solange Sie eine einfache Regel beherzigen, ist auch diese Gefahr relativ leicht zu bannen: Öffnen Sie E-Mail-Anhänge nur, wenn Sie diese für vertrauenswürdig halten. Haben Sie Zweifel, kann eine kurze Nachfrage beim Absender der E-Mail Klarheit schaffen.

TIPP: E-Mail-Anhänge

- Öffnen Sie keine E-Mail-Anhänge, die Ihnen nicht vertrauenswürdig erscheinen – und erst recht keine Exe-Dateien.
- Bedenken Sie, dass Angreifer ihre Malware in so ziemlich allen Formaten (insbesondere auch pdf oder doc) verstecken können.
- Nehmen Sie im Zweifelsfall Rücksprache mit dem Absender, bevor Sie etwas öffnen.

Verschlüsselung – von der Postkarte zum Brief

Dass eine E-Mail von Dritten genauso leicht gelesen werden kann wie eine Postkarte, wurde bereits erwähnt. Aber auch das lässt sich mit ein wenig Mehraufwand ändern, indem Sie Ihre E-Mails verschlüsseln und sie so für alle außer einem spezifischen Empfänger unleserlich machen. Dazu benötigen sowohl Sie als auch der Empfänger einen Schlüssel, mit dessen Hilfe Sie die Daten ver- beziehungsweise entschlüsseln können. Die drei am häufigsten genutzten Technologien zur Verschlüsselung von E-Mails sind:

- PGP (Pretty Good Privacy)
- S/MIME (Secure/Multipurpose Internet E-Mail Extensions)
- passwortverschlüsselte Anhänge

Der Vollständigkeit halber sei erwähnt, dass S/MIME auch zusammen mit PGP verwendet werden kann.

Die Verfahren unterscheiden sich vor allem durch die Art des Schlüssels. PGP benötigt einen entsprechenden PGP-Schlüssel, während S/MIME typischerweise ein sogenanntes X.509v3-Zertifikat zur Verschlüsselung erfordert. S/MIME wird von den meisten E-Mail-Clients standardmäßig unterstützt, für PGP ist dagegen häufig eine Erweiterung notwendig. Beide sind auch kostenlos einsetzbar, wobei es für S/MIME nur sehr wenige kostenlose und sinnvoll nutzbare Zertifikate gibt. Einen PGP-Schlüssel können Sie mithilfe verschiedener Programme erzeugen, die den OpenPGP-Standard umsetzen. Das kann zum Beispiel über das freie PGP-Programm des Projekts GnuPG geschehen oder auch über kommerzielle Angebote (Workshop «PGP», siehe Softlink 325).

Durch den Einsatz dieser Technologien können E-Mails nicht nur verschlüsselt und somit für Fremde unleserlich gemacht werden, sondern auch digital signiert, also unterschrieben werden. Damit kann der Empfänger sicher sein, dass der Absender tatsächlich der ist, für den er sich ausgibt. So wird gleichzeitig das Problem des gefälschten Absenders gelöst.

Für den privaten Gebrauch ist es am einfachsten, PGP einzusetzen. Dabei ist wichtig zu wissen, dass der Kommunikationspartner natürlich über die gleiche Verschlüsselungsmethode verfügen muss. Bei PGP benötigen die Partner jeweils die öffentlichen Schlüssel voneinander. Ist die Verschlüsselung jedoch erst einmal eingerichtet, genügt ein Mausklick, um eine E-Mail zu verschlüsseln. Wie Sie eine solche PGP-Verschlüsselung installieren und verwenden, zeigt der Onlineworkshop (Softlink 325). Wollen Sie mehr zum Thema Verschlüsselung wissen, sei Ihnen der Onlineartikel «Kryptographie» empfohlen, den Sie unter Softlink 326 finden.

TIPP: E-Mail-Verschlüsselung

- Wenn Sie sicherheitskritische Daten per E-Mail versenden, sollten Sie die Daten unbedingt verschlüsseln.
- Wenn Sie eine Verschlüsselung verwenden, können Sie auch signieren. So können Sie den Absender eindeutig identifizieren und sicher sein, dass die E-Mail nicht manipuliert worden ist.

Ausblick: DE-Mail

Unter dem Namen DE-Mail wird von der Bundesrepublik und einigen privatwirtschaftlichen Unternehmen ein E-Mail-Dienst ins Leben gerufen, der den sicheren Austausch rechts-

gültiger Mails (Dokumente) zwischen Bürgern, Behörden und Unternehmen über das Internet möglich machen soll.

Um eine flächendeckende und sichere E-Mail-Kommunikation zu ermöglichen, sollen bei dem neuen DE-Mail-Dienst die Anbieter im Rahmen eines staatlich definierten Akkreditierungsverfahrens nachweisen, dass sie die geforderten Funktionalitäten erfüllen, die IT-Sicherheit gewährleisten und den Datenschutz einhalten. Dieser Zustand wird dann regelmäßig überprüft, und die Sicherheitsanforderungen werden der aktuellen Entwicklung angepasst. Anbieter des DE-Mail-Dienstes sollen die heutigen Webmail-Anbieter sein, die sich für den Dienst akkreditieren lassen. Als besondere Sicherheitsmechanismen werden die folgenden Maßnahmen umgesetzt:

- Sichere Anmeldeverfahren werden verwendet, zum Beispiel mithilfe des neuen elektronischen Personalausweises.
- Die Kommunikationsverbindung vom Computer des Nutzers zum DE-Mail-Anbieter erfolgt unter der Nutzung einer SSL/TLS-Verschlüsselung (siehe Seite 36 ff.).
- Die E-Mails werden zwischen den DE-Mail-Anbietern nur in verschlüsselter und integritätsgesicherter Form übertragen und gespeichert.
- Der Absender kann zusätzlich eine qualifizierte signierte (Kryptographie, siehe Softlink 326) Bestätigung anfordern, wann er die E-Mail verschickt hat und wann die E-Mail in das Postfach des Empfängers eingestellt wurde (DE-Mail-Einschreiben), die der heutigen Zustellung eines Einschreibens durch den Briefträger entspricht.

Dadurch, dass nur eindeutig identifizierbare Teilnehmer den DE-Mail-Dienst nutzen, wird sich auch die Spam-Rate voraussichtlich auf einem sehr niedrigen Niveau bewegen.

Die E-Mail-Adressen sollen folgendermaßen aufgebaut sein: ‹Vorname›.‹Nachnahme›@‹DE-Mail-Anbieter›.de-mail.de.

DE-Mail stellt mit den beschriebenen Verfahren aber keine durchgehende Verschlüsselung der E-Mails sicher, sondern nur des Transports. Dementsprechend wird bei sensiblen Daten auch weiterhin eine zusätzliche Verschlüsselung (PGP, S/MIME) notwendig sein.

Web 2.0 – das Mitmach-Web

Stellen Sie sich vor, Sie sitzen mit ein paar Freunden zusammen und reden über die wirklich wichtigen Dinge des Lebens: Welche aktuellen Musikalben gibt es? Wo kann man gut essen gehen? Wie war die Premiere des neuen Theaterstücks? Was macht der Nachbar wieder Verrücktes? Dieser Austausch von Informationen und Meinungen hilft uns, auf dem neusten Stand zu bleiben. Allerdings ist das informationstechnische Potenzial eines solchen «Kaffeekränzchens» doch sehr beschränkt, weil nur eine begrenzte Anzahl von Personen daran teilnehmen kann. Wäre es da nicht genial, wenn Sie sich aussuchen könnten, wer alles zum Kaffeeklatsch kommt und zudem das Thema selbst bestimmen? Herzlich willkommen im Web 2.0!

Der Begriff Web 2.0 ist durchaus umstritten, hat sich aber für die aktuelle Entwicklung im Internet etabliert und steht mittlerweile für die interaktive Zusammenarbeit vieler Nutzer, die gleichzeitig Anbieter und Konsumenten von Informationen sind. War das World Wide Web ursprünglich eine riesige Sammlung von verknüpften Dokumenten, die mithilfe

eines Browsers gefunden werden können, stellt ein Anbieter heute lediglich eine Web-2.0-Anwendung zur Verfügung, und die Nutzer sorgen für die Inhalte selbst.

Social Networking – ein Trend erobert das Web

Eine immer beliebter werdende Form von öffentlichen Web-2.0-Anwendungen ist das sogenannte Social Networking. Beispiele dafür sind Webseiten wie Facebook, StudiVZ, SchuelerVZ, MySpace, YouTube, XING, LinkedIn, Twitter & Co, wo sich Nutzer aus verschiedenen Gesellschaftsgruppen

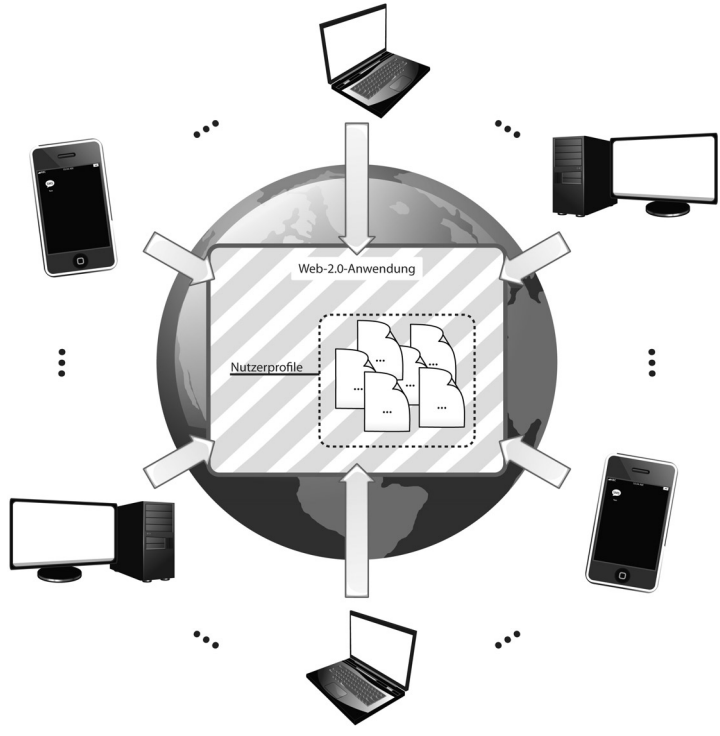


Abbildung 23: Social Networking als Web-2.0-Anwendung

auf verschiedene Arten kennenlernen und miteinander vernetzen können. Es gibt aber auch viele Web-2.0-Anwendungen, die speziell für bestimmte Städte und Regionen, bestimmte Berufsgruppen wie Lehrer und Anwälte oder einzelne Interessensgruppen wie SAP-Anwender aufgebaut wurden.

Neben den Social-Networking-Portalen, in denen die Nutzer Profilseiten mit persönlichen Informationen wie Werdegang, Freunde und Hobbys anlegen können, zählen auch Blogs, Wikis und Tauschseiten für Bilder oder Videos zu den Web-2.0-Anwendungen. Ebenfalls spannend sind Angebote wie Radio-Webseiten, bei denen anhand des Musikverhaltens der Nutzer aus Hunderten von Radiosendern ein entsprechendes Musik-Programm zusammengestellt wird.

Bei einem Blog oder Weblog handelt es sich um ein öffentlich einsehbares Tagebuch oder Journal. Autoren schreiben über bestimmte Aspekte des eigenen Lebens sowie ihre Meinungen zu spezifischen Themen – und die Leser kommentieren das Ganze. Ein Wiki ist eine Artikelsammlung im Internet, die nicht nur von jedem gelesen, sondern auch von jedem verändert werden kann. Das bekannteste Wiki ist Wikipedia, eine Wissens-Enzyklopädie, bei der die Idee der kollektiven Intelligenz umgesetzt wird, indem jeder Nutzer an den Inhalten aktiv mitarbeiten kann. Dadurch entsteht ein selbstregulierender Mechanismus, denn im Prinzip kann jeder Nutzer den Inhalt auf Korrektheit überprüfen und die vorhandenen Artikel korrigieren.

All diese neuen Anwendungen sind nur möglich, weil das Internet inzwischen eine breite Akzeptanz gefunden hat. Die Hemmschwelle, neue Anwendungen im Internet auszuprobieren, ist gesunken, sodass viele Nutzer den neuen Web-2.0-

Angeboten offen gegenüberstehen. Diese positive Entwicklung hat aber natürlich auch ihre Kehrseite. Gerade junge Menschen erzählen arglos über ihr Privatleben, ihre Arbeit, ihre Hobbys und ihre Interessen. Scheinbar hat diese Generation ein hohes Maß an Grundvertrauen, was den Umgang mit ihren persönlichen Daten angeht. Sie fühlen sich aufgrund der Anonymität in der Masse sicher und geben sehr viel von sich preis. Und diese Informationen sind im Prinzip für jeden einsehbar. Nicht nur Freunde oder Bekannte, sondern beispielsweise auch Personalchefs können sie lesen. Internetnutzer müssen deshalb – als Individuum und als Gesellschaft – lernen, mit den neuen Herausforderungen des digitalen Lebens umzugehen. Dazu gehört in erster Linie ein waches Bewusstsein dafür, was mit den eingestellten Informationen geschehen kann.

Ein weiterer interessanter Aspekt ist die rechtliche Situation hinsichtlich der von den Nutzern generierten und veröffentlichten Inhalte. Wem gehören die Kommentare in Blogs, die hochgeladenen Videos oder zur Schau gestellten Bilder? Wie verdienen die Anbieter von Web-2.0-Anwendungen das Geld, das nötig ist, um diese zu betreiben? Denn das kann je nach Größe schnell 100.000 bis mehrere Millionen Euro pro Jahr kosten.

Wikipedia zum Beispiel finanziert sich durch freiwillige Spenden, während bei einigen beruflich genutzten Web-2.0-Anwendungen die Nutzer monatliche Beiträge bezahlen müssen. Und manche finanzieren sich eben durch den Verkauf von Informationen, welche die Nutzer in die Web-2.0-Anwendung einstellen, oder durch generelle sowie individualisierte Werbung, die aus den vorhandenen Nutzerinformationen (Alter, Geschlecht, Hobbys, Beruf usw.) erstellt wird.

Social Networking mit Blick auf Datenschutz und Datensicherheit

Durch die Selbstbeschreibung in Social-Network-Anwendungen können Nutzer leicht alte Freunde wiederfinden, neue Freundschaften knüpfen oder virtuell Gruppen beitreten, welche die gleichen Interessen teilen. All das geschieht freiwillig und in einem ziemlich großen Umfang. Denn je mehr jeder Einzelne von sich preisgibt, und je aktiver er sich in der digitalen Szene bewegt, desto stärker wird er wahrgenommen.

Doch gerade dieser Aspekt des Social Networking wirft die Frage auf, wie es bei diesen Anwendungen um die informationelle Selbstbestimmung bestellt ist. Werden persönliche Daten analysiert oder gar an Dritte weitergegeben? Nicht selten basiert das Geschäftsmodell eines Web-2.0-Anbieters auf der Weitergabe von anonymisierten oder auch nicht anonymisierten Informationen, die Profile oder Statistiken über die Nutzung von spezifischen Seiten enthalten. Die jeweilige Handhabung des Datenschutzes wird explizit in den jeweiligen Allgemeinen Geschäftsbedingungen (AGB) erläutert. Es gibt zum Beispiel Anbieter, die penibel darauf achten, dass die Datenschutzgesetze eingehalten und personenbezogene Daten geschützt werden. Und es gibt natürlich Web-2.0-Anbieter, welche die Weitergabe von Informationen ausdrücklich erwähnen, um dadurch die gesetzlichen Bestimmungen zu erfüllen, die Nutzungsbedingungen durchzusetzen und ihre Interessen zu schützen, damit sie mit den Informationen der Nutzer Geld verdienen können.

Neben den scheinbar anonymen Bewegungsprofilen besteht auch die Gefahr, dass aus einer Kombination der per-

sönlichen Nutzerinformationen und den Verlinkungen innerhalb eines Netzwerks regelrechte Soziogramme erstellt werden. Die Web-2.0-Anbieter können diese für eine individualisierte Werbung nutzen. Ebenso ist die Möglichkeit, indirekt und relativ anonym neue Kontakte zu knüpfen, ein weiterer Gefahren-Aspekt des Social Networking. Zum Beispiel können Sexualstraftäter die Netzwerke nutzen, um Minderjährige anzusprechen. Vorfälle dieser Art nehmen Behörden immer öfter zum Anlass, die Profildatenbanken der betroffenen Web-2.0-Anbieter mit Informationen zu Sexual- oder anderen Straftätern abzugleichen. Dieses eigentlich positive Vorgehen wirft einmal mehr die Frage auf, ob und inwieweit der Datenschutz beim Social Networking tatsächlich gegeben ist und ob die Anwender nicht zu gläsernen Menschen werden, wenn eigentlich voneinander unabhängige Datenbestände miteinander verknüpft werden.

Weiß ein Internetnutzer nicht, mit wem er Kontakt hat, besteht noch eine weitere Gefahr. Große Web-2.0-Anwendungen sind genau wie Internetauktionshäuser und ähnliche Anwendungen attraktive Ziele für das Ausspähen von Nutzerdaten, etwa durch Phishing-Attacken (siehe auch Seite 100 ff.). Die so erlangten Zugangsdaten werden beispielsweise benutzt, um das Profil des Betroffenen zu manipulieren. Das hat meist einen großen sozialen Schaden für die betreffende Person zur Folge, zum Beispiel durch falsche Informationen über politische oder sonstige Einstellungen des Nutzers (Stichwort Cyber-Bullying, also virtuelles Mobbing). Auch ist die Wahrscheinlichkeit leider groß, dass der Geschädigte das gleiche Passwort für weitere Internetdienste benutzt, was zu Folgeschäden führen kann – zum sogenannten «Identitätskollaps».

Um sich dagegen zu schützen, bieten die meisten Web-2.0-Anwendungen Ihnen die Möglichkeit festzulegen, welche Informationen von wem gelesen werden dürfen. Sie können sich also überlegen, ob Sie Ihr Profil – oder Teile davon – auch außerhalb der eigentlichen Anwendung, also zum Beispiel für Suchmaschinen, freigeben möchten oder nicht. Genauso ist es in der Regel möglich, innerhalb der Web-2.0-Anwendungen zu entscheiden, ob alle Nutzer oder nur eine definierte Auswahl (Freunde, Nachbarn, Sportkameraden, Geschäftspartner …) auf Ihr Profil zugreifen dürfen. So können Sie unter anderem verhindern, dass unerwünschte Personen, wie der bereits angesprochene Personalchef, diese Inhalte zu sehen bekommen.

Soziale Beziehungen sind eine elementare Voraussetzung für ein erfülltes Leben. Wir lernen schon sehr früh, soziale Beziehungen einzugehen und integrieren uns – zumindest tun das die meisten von uns – in Gemeinschaften, denen wir uns zugehörig fühlen, zum Beispiel in die Familie, den Freundes- oder den Kollegenkreis. Innerhalb dieser Gemeinschaften positionieren wir uns entsprechend unserer Rolle. So hat beispielsweise jeder eine klare Vorstellung davon, wie er sich in seinem Freundeskreis verhalten soll, beziehungsweise was dort von ihm erwartet wird. Diese genauen Vorstellungen sollten wir auch in Bezug auf das digitale Leben entwickeln und uns überlegen, wie unsere Darstellung im Web 2.0 aussehen soll. Das heißt, jeder sollte bewusst entscheiden, welche Fotos er seinen Verwandten, seinen Freunden, seinen Kollegen oder seinen Sportkameraden präsentieren will. Und schon allein bei diesem Aspekt wird deutlich, dass wir uns in den verschiedenen Web-2.0-Angeboten wahrscheinlich auch unterschiedlich präsentieren wollen. Ebenfalls wichtig ist, zu entscheiden, wie groß die Gruppe sein soll und wer Mitglied

werden darf, beziehungsweise wer nicht hinein soll. Wenn jeder von uns diese Möglichkeiten aktiv gestaltet, dann können Social Networks eine echte Bereicherung für unser digitales Leben sein.

TIPP: Social Networks

- Gehen Sie stets sparsam mit Ihren persönlichen Daten um und geben Sie in Ihren Profilen nur die notwendigsten Informationen an.
- Wenn Sie sich bei einem Angebot nicht sicher sind, nutzen Sie ein Pseudonym statt Ihres echten Namens und ein eigenständiges Passwort.
- Verwenden Sie ein sicheres Passwort (siehe Seite 53 f.), damit niemand Ihre persönlichen Daten unbefugt ändern kann (Stichwort «Identitätsdiebstahl»).
- Geben Sie Ihr Passwort nicht leichtsinnig weiter.
- Definieren Sie für sich, welche Informationen Sie in welchem Social Network angeben wollen, um sich im Web 2.0 darzustellen.
- Legen Sie nach dem Beitritt zu einem Social Network sofort fest, wer auf Ihr Profil zugreifen darf (von außen und von innen), und nutzen Sie die Profileinstellungen zum Datenschutz.
- Sie sollten nur Informationen preisgeben (Fotos, Hobbys etc.), die Ihnen auch später einmal nicht peinlich sind oder schaden können.
- Zum Schutz Ihrer personenbezogenen Daten sollten Sie die AGBs des Web-2.0-Anbieters vor dem Erstellen eines Profils genau prüfen. Beachten Sie dabei, ob Informationen an Dritte weitergegeben werden und besonders in welchem Ausmaß.
- Seien Sie gegenüber anderen Teilnehmern im Web 2.0 zunächst einmal grundsätzlich misstrauisch. Das schützt Sie unter

Umständen vor fatalen Fehlentscheidungen. Bedingt durch die Anonymität des Internets ist nämlich nicht jeder der, für den er sich ausgibt.

User generated Content – die rechtliche Situation

Im Web 2.0, dem Mitmach-Web, ist jeder angehalten, eigene Texte zu veröffentlichen oder fremde zu kommentieren sowie Informationen zu sammeln und zu tauschen. Diese vom Nutzer eingestellten Inhalte werden auch User generated Content genannt. Da es dabei im Prinzip keine konkrete Unterscheidung zwischen dem Nutzer und dem Autor gibt, stellt sich die Frage, wem die Inhalte gehören. Hierzu gibt es einige Regelungen, wie zum Beispiel die Creative-Commons-Lizenzen (Softlink 331), deren Abstufungsgrade vom fast vollständigen Vorbehalt der Rechte bis hin zum völligen Verzicht auf Urheberrechte (Gemeinfreiheit) reichen. Wichtig sind in diesem Zusammenhang drei Punkte: Soll die Nennung des Urhebers vorgeschrieben sein? Ist die kommerzielle Nutzung der Inhalte erlaubt? Sind Veränderungen erlaubt? Mit diesen Lizenzen können Sie beispielsweise für Ihr Internettagebuch (Blog) festlegen, was genau mit den veröffentlichten Inhalten passieren darf.

Eine nicht so ohne Weiteres zu beantwortende Frage ist die, wem die zahlreichen Kommentare in den Blogs gehören. Aber auch hier können die Creative-Commons-Lizenzen Klarheit schaffen, indem man mit ihrer Hilfe in den AGBs festlegt, dass sämtliche Inhalte des Blogs, also alle Blogeinträge sowie die Kommentare der Besucher, nicht kommerziell verwendet oder verändert werden dürfen – wohl aber mit Nennung des Urhebers zitiert oder anderweitig publiziert werden

können. Ist ein Kommentator mit dieser Regelung nicht einverstanden, muss er sich entscheiden, ob er seinen Kommentar trotzdem an dieser Stelle abgibt oder in einem anderen Blog (mit passender rechtlicher Grundlage) und dann darauf verweist.

Ein anderer Bereich, in dem die rechtliche Situation bezüglich der Inhalte von großer Bedeutung ist, sind Dokumente, die der Allgemeinheit über Wikis zugänglich gemacht werden. Das im Internet sehr bekannte Beispiel Wikipedia zeigt, dass eine Gruppe interessierter Menschen sogar eine ganze Enzyklopädie auf die Beine stellen kann. Hierbei kommt für die Texte eine GNU-Lizenz zum Tragen, nämlich die GNU-Lizenz für freie Dokumentation – GNU-FDL (Softlink 332) –, zusammen mit der Creative-Commons-Attribution-ShareAlike-Lizenz 3.0 (CC-BY-SA). Dies sind Lizenzen für «freie Inhalte», die besagen, dass der Autor, also der Urheber der Information, keine Vergütung erhält und die Verbreitung ausdrücklich wünscht. Der Autor stellt den Inhalt damit jedem im Internet kostenlos zur Verfügung, macht ihn also gemeinfrei. Das gilt allerdings nur dann, wenn ein Dritter mit der Benutzung, Vervielfältigung, Verbreitung oder Veränderung des Inhalts auf gleiche Weise verfährt.

TIPP: Eigene Inhalte im Internet

- Überlegen Sie sich – bevor Sie den Inhalt einstellen – genau, was damit im Internet möglich sein soll und was nicht.
- Überprüfen Sie, ob die von der Web-2.0-Anwendung festgelegten Lizenzen und Rechte mit Ihren Vorstellungen übereinstimmen.
- Beachten Sie die entsprechenden gesetzlichen Bestimmungen (siehe Seite 162 ff.).

Inhaltsspeicherung und -austausch

Das Speichern und Tauschen von Bildern und Videos ist ein weiterer großer Bereich, in dem es viele Web-2.0-Anwendungen gibt. Die Nutzer können ihre Dokumente auf den Web-2.0-Server des Anbieters laden und so jederzeit und von jedem Ort darauf zugreifen. Außerdem sehen einige Nutzer diesen Dienst auch als eine Art Back-up ihrer lokalen Daten. Und natürlich wird auch hier über Inhalte, die der Allgemeinheit zugänglich gemacht wurden, diskutiert und sich ausgetauscht. Besonders Videoplattformen wie YouTube oder sogenannte Video-Podcasts erfreuen sich derzeit großer Beliebtheit. Mittels Videobotschaften bieten Autoren individuelle Videos, beispielsweise ihr Tagebuch, allen Interessierten im Internet zum Download an.

Spannend ist hierbei die Betrachtung der vom Anbieter beanspruchten Rechte und Lizenzen, wobei zwischen der Inhaltsspeicherung und dem Inhaltsaustausch unterschieden werden muss. Es gibt Anbieter, die sich komplett vom übertragenen Inhalt distanzieren und keinerlei Haftung übernehmen, während andere weitgehende Rechte und Lizenzen für Veränderung, Verkauf, Vervielfältigung oder Verbreitung der Inhalte für sich beanspruchen. Beide haben zwei Dinge gemeinsam: Sie setzen voraus, dass der Nutzer des Dienstes die Rechte für den eingestellten Inhalt besitzt und dass dieser nicht gegen geltendes Recht verstößt.

Nutzt nun jemand ein solches Angebot als Onlinefestplatte oder als Back-up-Möglichkeit, hat er keine Garantie dafür, dass die Daten unverändert und vor allem verfügbar bleiben. In den Nutzungsbedingungen und AGBs wird meist nur vage auf diese Punkte eingegangen. Schwammige Formulierungen

wie: «Wir fahren öfter Back-ups, als Sie die Dateien ändern können», geben dem Nutzer keine Sicherheit, da auf die Punkte Integrität und Verfügbarkeit nur indirekt eingegangen wird. Auch andere harte Fakten wie Verschlüsselung und Übertragungssicherheit werden weder konkret angesprochen noch garantiert.

Wie Sie bereits an diesen kurzen Ausführungen sehen, sind die Möglichkeiten des Web 2.0 sowie die entsprechende Rechtslage noch ziemlich undurchsichtig. Gehen Sie deshalb stets mit der gebotenen Vorsicht zu Werke. Sie sollten bei Ihren Ausflügen in die digitale Welt zudem im Hinterkopf behalten, dass das Internet nichts vergisst. Das bedeutet, dass alle Informationen sehr lange im Internet gespeichert werden und im Regelfall für alle Interessierten jederzeit verfügbar sind. Ein Beispiel dafür ist das gemeinnützige Projekt www.archive.org. Ein Internetarchiv, das 1996 gegründet wurde und sich die Langzeitarchivierung digitaler Daten in frei zugänglicher Form zur Aufgabe gemacht hat. Es speichert Momentaufnahmen von allen Webseiten sowie weitere Informationen.

TIPP: Inhaltsspeicherung und -austausch

Überprüfen Sie, ob die von der Web-2.0-Anwendung festgelegten Lizenzen und Rechte mit Ihren Vorstellungen übereinstimmen. Auch sind Plattformen wie YouTube oder Flickr keine adäquate Back-up-Möglichkeit.

Vertrauliche Unternehmensdaten im Web 2.0

Das Web 2.0 ist auch für Unternehmen interessant. Deren Mitarbeiter können sich über Web-2.0-Anwendungen sehr schnell neues Wissen aneignen und Informationen beschaffen,

was die Innovationsgeschwindigkeit im Unternehmen steigern kann. Dazu tragen natürlich auch Diskussionen unter den Mitarbeitern über neue Ideen bei. Doch wer sich an Diskussionen in den Web-2.0-Anwendungen beteiligt, sollte immer bedenken, dass er der Konkurrenz damit unter Umständen wertvolle Informationen in die Hände spielt. Daher gilt: Vertrauliche Unternehmensinformationen sollten generell nicht im Internet besprochen werden.

Exkurs: das Phänomen Twitter

Barack Obama tut es, Britney Spears tut es und Paulo Coelho ebenfalls: twittern. Mithilfe des Internetdienstes Twitter lassen immer mehr Menschen – ob prominent oder nicht – die Welt daran teilhaben, was sie gerade tun, denken oder planen. Dabei handelt es sich um ein öffentlich einsehbares Tagebuch (Mikroblog), in dem sich der Nutzer mittels kurzer Nachrichten (maximal 140 Zeichen) entsprechend darstellen kann. Die Nachrichten sind in der Regel aus der Ich-Perspektive verfasst und stellen für den Verfasser und die Leser ein einfach zu handhabendes Echtzeit-Kommunikationsmedium dar, wobei die Leser bei Twitter als Follower bezeichnet werden. Der Verfasser kann entscheiden, ob er seine Nachrichten allen Interessierten oder nur einer definierten Gruppe zugänglich machen will.

Ein Problem bei Twitter ist, dass viele Nutzer ein Passwort auswählen, das sich leicht knacken lässt (siehe Seite 51 ff.). Die Folge: Fremde können unter einer falschen Identität Nachrichten versenden. Das Problem dabei ist, dass die Unbekannten den Betroffenen so Dinge in den Mund legen können, die nicht der Wahrheit entsprechen und diese in ein schlechtes Licht rücken.

Ein weiteres Problem ist, dass Nutzer sich unter einem falschen Namen anmelden können. Eine Überprüfung des sich registrierenden Nutzers wird nicht zwingend durchgeführt. Das vermutlich beste Beispiel für einen solchen Fall ist Rob Vegas, der einige Monate lang als Harald Schmidt «zwitscherte». Zwar hat Twitter hier einen ersten Schritt unternommen, um Abhilfe zu schaffen, und sogenannte Verified Accounts eingeführt (bei denen eine Verifikation des Nutzers vorgenommen wird), die an einem blauen Siegel zu erkennen sind. Doch aufgrund des hohen manuellen Aufwands erhalten dieses Siegel derzeit nur sehr wenige Accounts.

Und schließlich gilt auch bei der Twitter-Nutzung, dass sich der «Twitternde» genau überlegen sollte, was er der Öffentlichkeit preisgibt. Die Information über den momentanen Aufenthaltsort zum Beispiel kann auch für Einbrecher durchaus interessant sein …

TIPP: Vorsichtsmaßnahmen beim Twittern

- Wollen Sie über Twitter Nachrichten verbreiten, überlegen Sie sich im Vorfeld genau, wer die Nachrichten lesen soll und welche Art von Information darin enthalten sein soll.
- Nutzen Sie Twitter als Follower, sollten Sie aufpassen, dass die Nachrichten auch wirklich von demjenigen stammen, den Sie hinter dem Profil vermuten.

Onlinebanking – Sicher, wenn's ums Geld geht

«Das Geld hat noch keinen reich gemacht», sagte schon der römische Philosoph und Dichter Lucius Annaeus Seneca (4 v. Chr. – 65 n. Chr.). Trotzdem ist jeder aus verständlichen

Gründen bemüht, es zu bekommen und nicht leichtfertig zu verlieren. Die digitale Technik hält dabei immer stärker Einzug in das private Finanzwesen. Bezahlt wird häufig mit der ec-Karte, die einen kleinen Computerchip sowie einen Magnetstreifen besitzt, und das Bankkonto wird online verwaltet. Und genau wie im realen Leben gibt es auch in der digitalen Welt Betrüger, die es auf Ihr Geld abgesehen haben. Deshalb sollten Sie bei der Abwicklung Ihrer Finanzgeschäfte im Internet unbedingt einige Punkte beachten. Sie lernen in diesem Kapitel die häufigsten digitalen Angriffe kennen und erfahren, wie Sie sich davor schützen können. Zudem erhalten Sie einen Überblick über die aktuell üblichen Onlinebanking-Verfahren und werden grundsätzlich für den Umgang mit kritischen Finanzdaten im Internet sensibilisiert.

Risiken beim Onlinebanking – Angiffsszenarien

Die Angriffsfläche beim Onlinebanking ist deutlich größer als beim Besuch bei einer Bank, da der digitale Angreifer keinen überschaubaren und überprüfbaren physischen Zugriff benötigt, sondern von überall auf der Welt – oft von Strafverfolgung verschont – agieren kann. Doch sind die Angriffe auf Bankdaten nur selten gegen eine bestimmte Person gerichtet. Die organisierte Kriminalität hat sich darauf spezialisiert, mithilfe globaler Attacken möglichst viele Zugangs- und Transaktionsdaten zu stehlen, um die entsprechenden Bankkonten übernehmen und ausrauben zu können. Die Angriffe richten sich dabei meist gegen Privatpersonen, da der Schutzlevel hier in der Regel am niedrigsten ist (Unternehmen beschäftigen nicht selten ganze Abteilungen, die sich um die Sicherheit kümmern).

Onlinebanking-Attacken haben Tradition. Sie werden permanent weiterentwickelt und sind so effektiv und präsent, dass sie nach wie vor eine große Gefahr darstellen. Hersteller von Banking-Software und Browsern sowie auch die Banken selbst versuchen zwar, immer neue Abwehrmechanismen zu finden, diese können jedoch nur zusammen mit dem korrekten und vorausschauenden Verhalten des Nutzers zum gewünschten Ergebnis führen.

Erschwerend kommt hinzu, dass jeder mit ein bisschen krimineller Energie und ohne Angst vor dem Gesetz diese Angriffe mehr oder weniger gut durchführen kann, weil die Software, die er dazu benötigt, mehr oder weniger offen zum Kauf angeboten wird. Die kriminellen Verkäufer stellen sogar einen Support für die Angriffssoftware zur Verfügung. Doch Sie können sich schützen.

Der Phishing-Angriff

Der bekannteste Angriff, der speziell beim Onlinebanking seit Jahren Hochkonjunktur feiert, ist der Phishing-Angriff. Der Begriff setzt sich aus den Wörtern «Password» und «Fishing» zusammen und tauchte Anfang 1996 erstmals im Zusammenhang mit dem Diebstahl von Internetzugangsdaten (IDs und Passwörter) von AOL-Kunden auf. Inzwischen hat er sich jedoch als allgemeiner Ausdruck für den Identitäts- und Passwortdiebstahl im Internet etabliert.

Phishing ist ein Problem, das zahlreiche Branchen betrifft, eine jedoch ganz besonders: Laut einer Statistik der Anti-Phishing Working Group sind über 80 Prozent aller Phishing-Angriffe gegen den Finanzdienstleistungssektor gerichtet. Die ersten Attacken gegen deutsche Bankkunden wurden im Juli 2004 verzeichnet, und sie nehmen seitdem massiv zu. Wurden

im Jahr 2004 noch 200.000 Phishing-E-Mails pro Monat registriert, steigerte sich die Zahl 2005 auf 100.000 Phishing-E-Mails pro Tag. Im Frühjahr 2008 war durchschnittlich eine Phishing-Mail pro 150 E-Mails zu beobachten.

Basis des Phishing-Angriffs ist im Finanzsektor häufig eine präparierte E-Mail, die optisch einer E-Mail der Bank nachempfunden ist.

In dieser E-Mail werden die Internetnutzer gebeten, auf einen bestimmten Link zu klicken, der zu einer gefälschten Onlinebanking-Webseite führt, die der echten Bank-Webseite oft haargenau gleicht. Auf der falschen Webseite geben die Nutzer dann wie gewohnt ihre Zugangsdaten ein und spielen sie so dem Angreifer direkt in die Hände. Das ermöglicht ihm zwar einen Überblick über das «gestohlene Bankkonto», aber noch keine Überweisung, denn dazu benötigt er mindestens eine Transaktionsnummer (TAN). Also

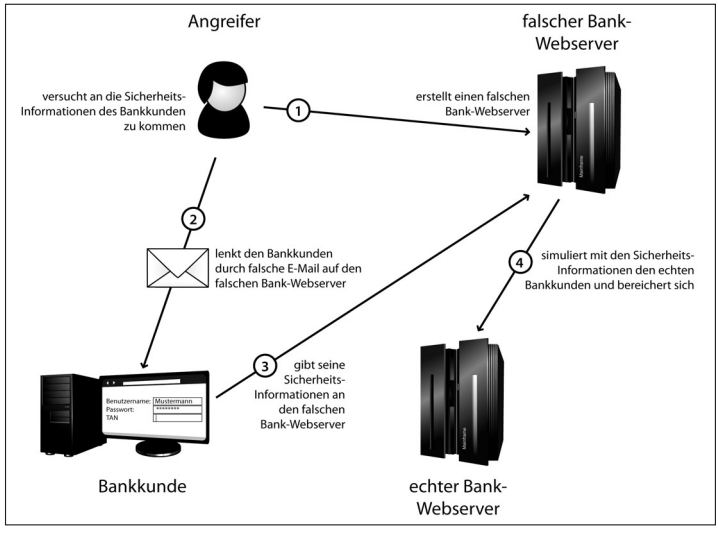


Abbildung 24: Der Ablauf einer Phishing-Attacke

werden die Nutzer bei diesem Verfahren zusätzlich aufgefordert, eine oder mehrere TANs einzugeben. Diese nutzt der Angreifer dann umgehend, um Geld vom Bankkonto zu stehlen, indem er einen bestimmten Betrag auf ein Angreifer-Bankkonto überweist (siehe Abbildung 24).

In der Regel ist das ein Konto, das von einer Bank geführt wird, die ihren Sitz in einem Land hat, in dem eine Strafverfolgung nicht möglich ist – oder die Gelder werden mithilfe leichtgläubiger Bürger «gewaschen» (siehe Seite 79).

Allerdings muss eine Phishing-Attacke nicht zwangsläufig durch eine E-Mail ausgelöst werden. Grundsätzlich können Internetnutzer über jede Art von gefälschten Links auf die Phishing-Webseiten gelangen. Eine Möglichkeit, Webseiten dahingehend zu manipulieren, ist das sogenannte Cross Site Scripting (siehe Seite 32f.). So kann beispielsweise auf der Webseite eines Onlinekaufhauses eine Information stehen, die auf Probleme mit Onlinekonten hinweist und einen Link anbietet, der den Nutzer vermeintlich direkt zu seiner Bank weiterleitet.

TIPP: So schützen Sie sich vor Phishing-Angriffen

- Klicken Sie nie auf Links in E-Mails, die angeblich zu Ihrer Bank führen. Banken schreiben keine E-Mails, wenn es um sicherheitskritische Vorgänge geht.
- Verwenden Sie generell keine Links, um auf die Webseite Ihrer Bank zu gelangen. Tippen Sie die Webadresse immer per Hand in die Adresszeile Ihres Browsers ein.
- Geben Sie auf einer Webseite niemals mehr als eine TAN-Nummer ein, auch wenn Sie dazu aufgefordert werden – und diese eine auch nur zum Ausführen einer regulären Banktransaktion.

Der Pharming-Angriff

Das sogenannte Pharming könnte als die Weiterentwicklung von Phishing angesehen werden, da der Pharming-Angriff wesentlich komplexer und die Täuschung für den Onlinebanking-Nutzer – besonders für den technisch eher unversierten – schwerer zu durchschauen ist.

Wie bereits beschrieben, werden Webseiten üblicherweise über ihre Webadresse (URL) aufgerufen, zum Beispiel in der Form www.name.de. Diese namentlichen Webadressen «zeigen» auf eine bestimmte IP-Adresse und werden vom sogenannten Domain Name Server (DNS) entsprechend umgewandelt (siehe Seite 42f.). Beim Pharming-Angriff wird nun der Name einer Webadresse durch Manipulation auf eine andere IP-Adresse gelenkt, sodass der Nutzer auf eine gefälschte Webseite gelangt. Das kann auf zwei Arten geschehen. Entweder werden die Domain Name Server manipuliert, was einen hohen Aufwand bedeutet und daher nur sehr selten passiert. Oder es wird – was meist der Fall ist – mithilfe von Malware eine bestimmte Datei, die sogenannte Hosts-Datei, auf dem Computer des Nutzers verändert. Diese Datei löst ebenfalls die Webadresse in eine IP-Adresse auf, noch bevor ein DNS befragt wird. Sie kann jedoch nur manipuliert werden, wenn die dazu nötigen Schreibrechte vorhanden sind. Das ist ein weiterer Punkt, warum Sie nicht als Administrator im Internet surfen sollten (siehe Seite 23f.).

Sie können diese Datei auch selbst überprüfen, wenn Sie das Gefühl haben, Opfer eines Pharming-Angriffs geworden zu sein (siehe Screenvideo, Softlink 341). Die Hosts-Datei ist am einfachsten zu finden, indem Sie eine Suche auf der Systempartition (meistens C:) nach «hosts» durchführen. Bei Windows XP befindet sich die Hosts-Datei zum Beispiel

unter C:\WINDOWS\system32\drivers\etc\hosts. Steht in der Datei – sie kann mit einem Editor oder einem Textverarbeitungsprogramm geöffnet werden – der Name einer Bank oder einer anderen Webseite, die mit sicherheitskritischen Vorgängen wie Bezahldiensten zu tun hat, kann das ein Indiz für einen Pharming-Angriff sein. Abbildung 25 zeigt den typischen Aufbau einer Hosts-Datei. Relevant sind nur die Einträge ohne «#». Im Normalfall ist dort nur der «Localhost-Eintrag» zu finden, und dieser ist völlig unbedenklich.

```
# Copyright © 1993-1999 Microsoft Corp.
#
# Dies ist eine HOSTS-Beispieldatei, die von Microsoft TCP/IP
# für Windows 2000 verwendet wird.
#
# Diese Datei enthält die Zuordnungen der IP-Adressen zu den
jeweiligen Hostnamen.
# Jeder Eintrag muss in einer eigenen Zeile stehen.
# Die IP-Adresse sollte in der ersten Spalte gefolgt vom
# zugehörigen Hostnamen stehen.
# Die IP-Adresse und der Hostname müssen durch mindestens
ein
# Leerzeichen getrennt sein.
#
# Zusätzliche Kommentare (so wie in dieser Datei) können in
# einzelnen Zeilen oder hinter dem Computernamen eingefügt
werden,
# müssen aber mit dem Zeichen '#' eingegeben werden.
#
# Zum Beispiel:
#
#   102.54.94.97    rhino.acme.com      # Quellserver
#    38.25.63.10    x.acme.com          # x-Clienthost

127.0.0.1    localhost
```

Abbildung 25: Aufbau einer nicht manipulierten Hosts-Datei

TIPP: So schützen Sie sich vor Pharming

- Stellen Sie sicher, dass der Basisschutz (siehe Seite 10 ff.) eingehalten ist, um sich keine Schadsoftware auf Ihrem Computer «einzufangen».
- Zusätzlich sollten Sie darauf achten, dass die Webseite ein gültiges Zertifikat Ihres Onlinebanking-Anbieters beinhaltet und dieses gegebenenfalls überprüfen (siehe Seite 36 ff. sowie Workshop «SSL/TLS», Softlink 223). Besondere Vorsicht ist geboten, wenn eine Warnmeldung («Ungültiges Zertifikat») erscheint, sobald Sie auf Ihre Bankseite gehen. Stoppen Sie sofort das Onlinebanking und fragen Sie Ihre Bank, wenn Sie sich nicht sicher sind, wie Sie die Seite überprüfen können.
- Wenn Sie vermuten, einer Pharming-Attacke zum Opfer gefallen zu sein, oder auch etwas zur Prävention tun möchten, überprüfen Sie die Hosts-Datei Ihres Computers. Finden Sie dort Einträge von Bank- oder Bezahldienstseiten, holen Sie sich Rat beim Experten und stoppen Sie alle sicherheitskritischen Vorgänge am Computer.

Angriffe über Schadsoftware

Grundsätzlich ist ein Betriebssystem wie Windows, Linux oder Mac OS angreifbar. Gelingt es einem Angreifer, beispielsweise ein Trojanisches Pferd auf dem Computer zu installieren, erlangt er die vollständige Kontrolle und ist unter anderem in der Lage, alle Tastaturanschläge mitzulesen (sogenanntes Key-Logging). Die auf diese Weise ausgespähten Informationen senden die Key-Logger – für den Nutzer unsichtbar – direkt oder indirekt zu den Angreifern. Und diese sind natürlich in erster Linie an Passwörtern und anderen sensiblen Daten interessiert, weshalb das Key-Logging – neben Phishing und Pharming – ebenfalls eine Gefahr für Sie als

Onlinebanking-Nutzer darstellt. Eine wirksame Abwehrmaßnahme ist auch hier der Basisschutz.

Onlinebanking-Verfahren – Welches ist wie sicher?

Zur Durchführung und zum Schutz der Transaktionen gibt es verschiedene Verfahren, die auch ein unterschiedlich hohes Maß an Sicherheit bieten. Die meisten Onlinebanking-Verfahren, mit Ausnahme des FinTS/HBCI-Verfahrens, basieren auf der Kombination aus PIN und TAN. Diese werden im Folgenden kurz erläutert und im Hinblick auf die Sicherheit bewertet. Dabei ist zu beachten, dass alte und unsichere Verfahren mit der Einführung neuer Verfahren abgeschaltet werden müssen, um mögliche Hintertüren zu schließen. Bei einem kürzlich aufgetretenen Betrugsfall war zwar ein neues iTAN-Verfahren eingeführt worden, aber das alte TAN-Verfahren wurde nicht deaktiviert. Somit konnten durch Phishing gewonnene iTANs auch weiterhin uneingeschränkt als TANs genutzt werden. Zuständig dafür ist die Bank. Fragen Sie dort explizit nach und probieren Sie Ihr altes Verfahren nach der «offiziellen» Umstellung noch einmal aus, um sicherzugehen, dass es deaktiviert ist.

TAN

Das einfache TAN-Verfahren basiert auf einer Liste von einmalig zu verwendenden TANs. TANs sind numerische Einmalpasswörter, die meist eine Länge von sechs Stellen haben und dem Nutzer in Form einer Liste von seiner Bank ausgehändigt werden. Dieser wiederum verwendet sie, um seine Transaktionen, zum Beispiel eine Überweisung, zu bestätigen, nachdem er sich per PIN in sein Bankkonto eingeloggt

hat. Erst durch die Eingabe einer korrekten TAN, die der Bank ebenfalls bekannt ist, wird die gewünschte Transaktion tatsächlich ausgeführt. Dabei kann jede TAN auf der Liste nur einmal verwendet werden, die Reihenfolge ist egal. Die TAN-Nummern sind also nicht an bestimmte Transaktionen gebunden. Die TAN wird, bildlich gesprochen, nach ihrer Verwendung aufseiten der Bank und beim Nutzer von der Liste gestrichen.

Dieses Verfahren wird heute als unsicher eingestuft, da bei einem Phishing-Angriff mehrere TANs ausgespäht werden können, die der Angreifer dann flexibel für seine Zwecke verwenden kann.

iTAN

Bei der iTAN (der indizierten TAN) muss eine ganz bestimmte TAN benutzt werden, um eine Transaktion zu legitimieren. Die TANs sind zu diesem Zweck auf der TAN-Liste entsprechend nummeriert. Das erschwert dem Angreifer seine Arbeit, da er bei seinem Phishing-Angriff genau die richtige TAN «erbeuten» muss. Er ist somit gezwungen, entweder in Echtzeit zu arbeiten oder eine ganze TAN-Liste zu ergaunern, wodurch sich der Sicherheitslevel beim iTan-Verfahren ein wenig erhöht. Das Verfahren kann aber auch nicht mehr empfohlen werden.

mTAN

mTAN (mobile TAN, auch SMSTAN genannt) verbessert die Sicherheit bereits erheblich, da neben der Bindung an eine bestimmte TAN auch noch ein Medienbruch erfolgt. Das bedeutet, dass die TAN bei der Initiierung einer Transaktion per SMS von der Bank an ein bestimmtes Handy des Onlineban-

king-Nutzers gesendet wird. In der SMS befinden sich neben der TAN auch Informationen zu der gewünschten Transaktion, zum Beispiel der Betrag und die Zielkontonummer, um auszuschließen, dass ein Angreifer die Transaktion manipuliert hat (Filme zu TAN-Verfahren siehe Softlink 342). Aktuell ist mTAN eines der sichersten Onlinebanking-Verfahren, da es für einen Angreifer sehr schwer ist, die Computerkommunikation und parallel die Handykommunikation zu überwachen. Allerdings fallen dabei meist zusätzliche Kosten für die SMS an (teilweise werden diese jedoch auch von den Banken übernommen). Aber es ist eine lohnende Investition, die einen angemessenen Sicherheitsstandard garantiert.

Sm@rtTAN, Sm@rtTAN Plus und ChipTAN

Das Sm@rtTAN-Verfahren stellt eine weitere Alternative zur TAN-Liste dar. Die Basis von Sm@rtTAN ist ein kleines zusätzliches Gerät mit Display, auch Token genannt, in das der Nutzer seine ec-Karte einführen kann. Der Token errechnet dann auf Knopfdruck die TAN, die für die gewünschte Transaktion verwendet werden soll. Dieses Verfahren ähnelt sicherheitstechnisch dem iTAN-Verfahren, da der Vorgang keine Man-in-the-middle-Angriffe verhindern kann, also Angriffe, bei denen sich der Angreifer in die Kommunikation zwischen Absender und Empfänger einklinkt und die Kommunikation zu seinen Gunsten verändert. Das bedeutet, dass der Nutzer nicht nachvollziehen kann, ob beim Transaktionsvorgang direkt mit der Bank kommuniziert wird oder ob sich ein Angreifer dazwischengeschaltet hat.

Daher wurde das Sm@rtTAN-Plus-Verfahren eingeführt, je nach Kreditinstitut auch ChipTAN genannt. Der hierfür benötigte Token besitzt zusätzlich eine eigene Tastatur. Startet

der Nutzer eine Transaktion, erhält er von der Bank zwei Nummern als Antwort angezeigt. Eine beinhaltet Teile der Kontonummer des Empfängers, die zweite ist ein Bankcode. Die Kontonummernteile werden mit der Transaktion verglichen. Dann gibt der Nutzer beide Nummern in den Token ein, der daraus – zusammen mit den Informationen von der eingesteckten ec-Karte – eine TAN errechnet (Filme zum TAN-Verfahren siehe Softlink 334).

Das Sm@rtTAN- beziehungsweise ChipTAN-Verfahren gibt es ganz aktuell auch in einer optischen Lösung. Dazu erhalten die TAN-Generatoren (Token) eine optische Schnittstelle. Nach Eingabe der Transaktionsdaten erscheint eine Animation. Der TAN-Generator wird dann vor den Monitor gehalten und liest den Code aus. Aus dem optischen Code, den Transaktionsdaten und den Daten der Karte werden die TANs generiert und auf der Anzeige des Tokens angezeigt. Dieses Onlinebanking-Verfahren ist vom Sicherheitslevel her ebenfalls gut geeignet. Achten Sie darauf, dass Sie alle Eingaben genau überprüfen. Allerdings fallen auch hier eventuell zusätzliche Kosten für den Token an.

HBCI/FinTS

Mit HBCI (Homebanking Computer Interface) wurde schon vor vielen Jahren ein solider offener Homebanking-Standard in Deutschland eingeführt, der in einer neuen Version inzwischen als FinTS (Financial Transaction Services) bekannt ist. Er sieht die Verwendung einer SmartCard vor, die mit einer elektronischen Signatur ausgestattet ist. Der sogenannte Klasse-3-Kartenleser zeigt in diesem Fall die Überweisungsdaten auf seinem Display an, und der Nutzer bestätigt die Transaktion mit seiner PIN, die direkt in den

Kartenleser eingegeben wird und nicht auf dem Computer. Das bedeutet, dass Computer und PIN völlig unabhängig voneinander sind, wodurch einer Malware auf dem Computer die Angriffsfläche entzogen wird. Der Einsatz von Kartenlesern der Klasse 2 und 1 wird nicht empfohlen, denn die Integrität und die Verbindlichkeit beim Transaktionsvorgang sind nur mit dem Klasse-3-Kartenleser gegeben. Dieser Kartenleser garantiert, dass die Tastatur und das Display des Kartenlesers während einer PIN-Eingabe nur unter der Kontrolle des Kartenlesers stehen und nicht vom Computer beeinflusst werden können.

Das HBCI/FinTS-Verfahren ist in Bezug auf das Sicherheitsniveau mit dem mTAN-Verfahren vergleichbar. Leider ist es jedoch kaum verbreitet, da sowohl die Kartenleser als auch die entsprechende Onlinebanking-Software deutlich teurer sind als andere, unsichere Verfahren.

TIPP: Onlinebanking-Verfahren

- Nutzen Sie für das Onlinebanking möglichst eines der folgenden Verfahren: mTAN, Sm@rtTAN Plus oder FinTS.
- Nutzen Sie neue Verfahren, wenn diese ein höheres Sicherheitsniveau bieten – auch wenn sie möglicherweise mit Zusatzkosten verbunden sind. Die Investition lohnt sich in jedem Fall!
- All diese Verfahren bieten nur dann optimalen Schutz, wenn Sie sie richtig anwenden. Achten Sie also beispielsweise darauf, dass Sie Ihr Handy, in dem Ihre Zugangsdaten gespeichert sind, nicht aus der Hand geben, wenn Sie mTan verwenden.

Onlinebanking mit Banking-Software

Alternativ zum browserbasierten Onlinebanking können Sie auch eine Banking-Software verwenden. Diese Anwendun-

gen sind zwar im Allgemeinen kostenpflichtig, bieten aber in den aktuellen Versionen sehr guten Schutz und zusätzlichen Komfort. Phishing-Angriffe sind hier – genau wie alle anderen browserrelevanten Angriffe – im Grunde ausgeschlossen. Sämtliche aktuellen Onlinebanking-Programme unterstützen darüber hinaus die empfohlenen Verfahren mTAN, FinTS und Sm@rtTAN Plus. Trotzdem sind auch sie angreifbar, vor allem mithilfe von Trojanischen Pferden. Sorgen Sie also stets für einen optimalen Basisschutz (siehe Seite 10 ff.)!

Besonders empfehlenswert ist die Banking-Software, wenn Sie technisch nicht so versiert sind und/oder mehrere Konten verwalten wollen. Bedenken Sie jedoch, dass Sie dann an den Computer gebunden sind, auf dem die Software installiert ist.

TIPP: Die wichtigsten Verhaltensregeln zum Onlinebanking

- Rufen Sie die Webseite Ihrer Bank beim browserbasierten Onlinebanking immer durch die manuelle Eingabe der Bankadresse auf. Nutzen Sie keine Links aus E-Mails oder von unbekannten Webseiten.
- Überprüfen Sie nach Eingabe der Bankadresse die Verschlüsselung der Verbindung, indem Sie darauf achten, dass die Webadresse in der Adresszeile mit «https» beginnt, der Name der Bank – je nach Browser – entsprechend markiert ist und ein Schloss-Symbol angezeigt wird.
- Gehen Sie sorgfältig mit Ihren Zugangsdaten um: Geben Sie diese nicht weiter, speichern Sie sie nicht in Klartext auf Ihrem Computer und schreiben Sie sie nicht auf.
- Verwenden Sie ein sicheres Passwort (siehe Seite 53 f.) beziehungsweise eine zusammenhangslose PIN (nicht das Geburts-

datum!) und ändern Sie diese sicherheitsrelevanten Daten regelmäßig – möglichst alle drei Monate.

- Onlinebanking sollte nie an einem fremden Computer, zum Beispiel im Internetcafé, durchgeführt werden. Nutzen Sie nur Ihren eigenen, gut geschützten Computer.
- Nutzen Sie das Onlinebanking-Angebot nicht in öffentlichen Netzen wie Hotspots im Bahnhof oder in Cafés. Das gilt auch für fremde WLANs und kabelgebundene Netze, denen Sie nicht vertrauen können. Hier sind Ihre Daten in Gefahr.
- Stellen Sie sicher, dass Ihr Computer gemäß den Sicherheitsgrundregeln geschützt ist (siehe Seite 10ff.), bevor Sie online gehen, um Ihre Bankgeschäfte zu erledigen.
- Überprüfen Sie regelmäßig Ihre Bankkontobewegungen auf Ungereimtheiten und fragen Sie in einem solchen Fall sofort bei Ihrer Bank nach.
- Vereinbaren Sie mit Ihrer Bank ein Limit für tägliche Geldbewegungen beim Onlinebanking.
- Achten Sie bei der Nutzung einer Banking-Software immer auf die Aktualität des Programms.
- Um bei Ungereimtheiten auf Nummer sicher zu gehen, können Sie das Zertifikat überprüfen und den Fingerprint des Zertifikats mit der Bank abgleichen. Dieses Verfahren ist jedoch sehr aufwändig und stellt sozusagen das letzte Mittel dar (siehe Seite 36ff.).

Exkurs: die wichtigsten Verhaltensweisen offline

Die meisten Bankgeschäfte lassen sich mittlerweile bequem vom heimischen Computer aus erledigen. Aber auch wenn Sie den Geldkartenchip Ihrer ec-Karte bereits im Internet aufladen können, Bargeld müssen Sie sich nach wie vor am

Bankschalter oder an Geldautomaten holen. Und auch Letztere sind Teil der digitalen Welt. Deshalb finden Sie hier, um das Thema Onlinebanking abzurunden, zudem die wichtigsten Grundregeln zur Nutzung von Geldautomaten. Denn auch diese werden vielfach manipuliert – man nennt das Skimming –, um an die Zugangsdaten von Ihrem Konto zu gelangen.

TIPP: Die Nutzung von Geldautomaten

- Kontrollieren Sie den Geldautomaten vor der Nutzung auf Manipulationsspuren an Tastatur und Karteneinschub.
- Während der Interaktion mit dem Automaten sollten Sie sich in keinem Fall ablenken lassen, sondern stets den Vorgang beobachten.
- Schützen Sie Ihre Eingaben und Aktionen vor Blicken und Kameras von potenziellen Angreifern.

E-Commerce – Shoppen «hoch n»

Das Internet ist wohl das größte Einkaufszentrum, das man sich vorstellen kann, und es gibt fast nichts, was man dort nicht bekommt. Ganz im Gegenteil: Gegenüber dem realen Leben kommen sogar noch neue Angebote hinzu. So ist es im Internet kein Problem, bestimmte Artikel aus Zeitschriften einzeln zu erwerben. Auch kostenpflichtige Software kann problemlos online gekauft werden, indem Sie eine entsprechende Lizenz erwerben und das gewünschte Programm einfach herunterladen. Alles geht sehr schnell und kann bequem von zu Hause aus erledigt werden. Weitere Vorteile des Onlineshopping sind: keine Parkplatzprobleme, keine Warte-

schlangen, kein Ladenschluss, der berücksichtigt werden muss, und keine «Zensur» durch die Nachbarn an der Kasse. Einer der größten Vorteile des Interneteinkaufs ist aber wohl die Möglichkeit, ohne großen Aufwand Preise zu vergleichen und so das günstigste Angebot herauszufiltern – wobei Sie immer auch die Kosten für den Versand berücksichtigen sollten.

Doch diese schöne neue Warenwelt wirft auch Fragen auf: Wie vertrauenswürdig ist der von mir besuchte Onlineshop? Was geschieht mit den sensiblen Daten, die der Anbieter für Lieferung und Bezahlung von mir erhält? Wie sicher ist der Onlinekauf? Und wie funktionieren die verschiedenen Bezahlverfahren im Internet?

Ein vertrauenswürdiger Onlineshop

Jeder Mensch hat seine Lieblingsgeschäfte, egal ob er Lebensmittel, Kleidung, Möbel, Musik oder Autos kauft. Die Verkäufer sind sympathisch, die Lage praktisch und das Ambiente angenehm – Vertrauen hat sich über die Zeit entwickelt. Und genau das ist im Internet schwierig, weil alles virtuell ist und es keinen persönlichen Verkäufer gibt, zu dem ein Vertrauensverhältnis aufgebaut werden kann. Wie aber können Sie dann feststellen, ob der Anbieter, bei dem Sie online ein Schnäppchen ergattern möchten, tatsächlich seriös ist?

Ein Aspekt, auf den Sie achten sollten, ist eine professionelle, aufgeräumte Webseite. Das allein reicht jedoch als Entscheidungsgrundlage noch nicht aus. Der Onlineshop sollte zudem auf jeden Fall schon länger existieren. Auch der Blick ins Impressum kann einen Hinweis auf dessen Vertrauenswürdigkeit geben (siehe Tipp). Zusätzlich können Sie prüfen, ob sich per Suchmaschine Referenzen zu dem fraglichen

Onlineshop finden lassen, denn die lassen sich in ihrer Gesamtheit nur schwer fälschen. Fragen Sie darüber hinaus Freunde und Bekannte, ob sie bereits Erfahrungen mit diesem Onlineshop gemacht haben. All diese Informationen zusammen bilden dann die Basis für einen vertrauenswürdigen Einkauf (Softlink 344).

Eine weitere Entscheidungshilfe können Browser-Add-ons sein (zum Beispiel für den Firefox), die bei Betreten bestimmter Onlineshops eine entsprechende Empfehlung anzeigen. Ein Beispiel dafür ist das Add-on WoT (Softlink 351), das auf den Bewertungen zahlreicher Nutzer im Hinblick auf Vertrauenswürdigkeit, Händlerzuverlässigkeit, Datenschutz oder auch Jugendschutz basiert. Ist WoT installiert, signalisiert es per Ampelfarben, ob die Webseite bedenkenlos genutzt werden kann oder eher mit Vorsicht zu genießen ist. WoT steht übrigens für «Web of Trust» und zeigt ein sehr positives Phänomen des Internets: Immer wieder finden sich viele Freiwillige zu großen Projekten zusammen, um das Internet für seine Nutzer sicherer zu machen.

TIPP: So erkennen Sie vertrauenswürdige Onlineshops

- Schauen Sie im Impressum eines Onlineshops auf die rechtlichen Merkmale (Organisationsform, verantwortliche Person, Anschrift, Gründungsdatum usw.) und überprüfen Sie diese gegebenenfalls.
- Kaufen Sie nur bei Onlineshops, die schon länger bestehen und sich im Internet etabliert haben. Bleiben Sie aber auch hier wachsam, da Onlineshops genau wie «reale» Geschäfte den Besitzer wechseln können.
- Geben Sie den Namen des Onlineshops in eine Suchmaschine ein und überprüfen Sie die Ergebnisse.

- Nutzen Sie zudem entsprechende Bewertungsseiten (zum Beispiel idealo.de, preissuchmaschine.de und günstiger.de) oder auch Add-ons wie WoT (Softlink 351).
- Kaufen Sie bevorzugt bei Onlineshops, die Ihnen von Personen Ihres Vertrauens empfohlen werden, oder fragen Sie Bekannte und Freunde, ob Sie mit dem Onlineshop, den Sie nutzen möchten, bereits positive Erfahrungen gemacht haben.

Das richtige Verhalten beim Onlineeinkauf

Wer sich bei vielen Onlineshops registriert, verteilt natürlich auch seine persönlichen Daten (personenbezogene Daten und Finanzdaten) im Internet. Daher sollten Sie eine Auswahl treffen. Beziehen Sie bei dieser Überlegung auch die Frage ein, welche Daten Sie preisgeben wollen/müssen und ob bestimmte Dienste des Onlineshops für Sie überhaupt sinnvoll sind. Bei Amazon können Nutzer zum Beispiel Wunschlisten – für den Hochzeitstisch oder den Geburtstag – und Ähnliches erstellen, die, verknüpft mit dem Namen des Nutzers, teilweise über Google zu finden sind. Das stimmt natürlich nicht mit dem Grundsatz der Datensparsamkeit des Datenschutzes überein. Eine gute Möglichkeit zu testen, ob ein Onlineshop vertrauliche Daten offen zugänglich macht, ist die Eingabe des eigenen Namens in eine Personensuchmaschine wie www.123people.de oder www.yasni.de. Diese finden nämlich auch Wunschlisten etc.

Wenn Sie jedoch Ihre Auswahl sorgfältig treffen und alle wichtigen Hinweise beachten, steht einem ungetrübten Shopping-Vergnügen im Internet nichts im Wege – auch wenn es manchmal schöner ist, durch eine Einkaufsstraße zu schlendern.

TIPP: Die wichtigsten Verhaltensregeln beim Onlineeinkauf

- Melden Sie sich nicht bei jedem x-beliebigen Onlineshop an. Machen Sie es ähnlich wie im realen Leben und entscheiden Sie sich für bestimmte Anlaufpunkte für die verschiedenen Produktgruppen.
- Nutzen Sie nicht jeden Dienst in einem Onlineshop, wie zum Beispiel Wunschlisten. Diese Daten sind oft unter Ihrem Namen frei im Internet verfügbar.

Sicher anmelden und registrieren

Haben Sie sich für einen Onlineshop entschieden, sollten Sie darauf achten, dass dieser eine verschlüsselte SSL/TLS-Übertragung der Registrierungsdaten zwischen dem Computer und dem Webserver gewährleistet (siehe Seite 36 ff.). Die Verschlüsselung ist allerdings erst erforderlich, wenn Sie Ihre persönlichen Daten eingeben, und nicht schon beim Stöbern im Warenangebot.

Damit Sie Ihre Daten nicht jedes Mal von Neuem eingeben müssen, speichern die meisten Onlineshops die Angaben, die bei der Registrierung gemacht werden, und verlangen zusätzlich einen Benutzernamen und ein Passwort. Das sollte gemäß den Regeln für ein sicheres Passwort gewählt werden (siehe Seite 53 f.). Beim nächsten Bestellvorgang reicht dann die Kombination aus Benutzername und Passwort.

Allerdings muss hier noch eine Unart mancher Anbieter angesprochen werden: Manchmal geben Nutzer ihre persönlichen Daten verschlüsselt auf einer Webseite ein und bekommen danach eine Bestätigung per E-Mail. Das ist grundsätzlich auch in Ordnung, solange Passwort und Benutzername

darin nicht in Klartext genannt werden. Denn E-Mails sind primär nicht verschlüsselt (siehe Seite 82 f.). In diesem Fall sollten Sie dem Onlineshop seinen Fehler mitteilen und das Passwort sofort ändern. Wird Ihnen auch dieses wieder übermittelt, sollten Sie die Registrierung löschen oder sperren, damit kein Schaden entstehen kann. Das gilt auch für Benutzerkonten, die Sie nicht mehr benutzen.

TIPP: Anmelden bei einem Onlineshop

- Geben Sie persönliche Daten nur ein, wenn Sie von der Vertrauenswürdigkeit des Onlineshops überzeugt sind.
- Nutzen Sie bei jedem Onlineshop ein anderes, sicheres Passwort (siehe Seite 53 f.).
- Erhalten Sie nach der Anmeldung eine unverschlüsselte E-Mail mit Ihren Zugangsdaten, also Benutzername und Passwort, machen Sie den Onlineshop auf den Missstand aufmerksam und ändern Sie Ihre Daten telefonisch oder online.
- Onlineshops und Dienste, die Sie nicht mehr nutzen, sollten Sie kündigen; lassen Sie Ihre Bank- und Kundendaten dann vollständig löschen. Weisen Sie den Onlineshop explizit auf die vollständige Löschung aller persönlichen Daten hin.

Sicher bezahlen im Internet

Ist das Produkt gefunden und ausgewählt, stellt sich die Frage nach der Bezahlung. Die Onlineshops bieten dazu eine Vielzahl von Möglichkeiten, die von der Kreditkarte über die normale Banküberweisung und den Bankeinzug bis hin zu Internetbezahldiensten wie PayPal und ClickandBuy reichen. Einige dieser Bezahldienste übermitteln dem Anbieter direkt eine Bezahlbestätigung, sodass dieser den Versand der Ware

unmittelbar einleiten kann. All diese Zahlungsarten haben Vor- und Nachteile, die in der folgenden Abbildung aufgelistet sind. Eine generelle Empfehlung, für welche Methode Sie sich entscheiden sollten, gibt es nicht. Wählen Sie die Methode immer entsprechend dem Einkauf. Die Vorabüberweisung beispielsweise birgt immer die Gefahr, dass Sie etwas bezahlen, was später nicht geliefert wird; sie ist also nur bei kleinen Beträgen und vertrauenswürdigen Händlern sinnvoll. Das Wichtigste ist, sich immer mit unterschiedlichen, sehr guten Passwörtern – oder zukünftig mit dem elektronischen Personalausweis (siehe Seite 61 ff.) – abzusichern. Teilweise bieten die Bezahldienste zusätzliche Sicherheitsmechanismen wie eine Treuhandfunktion an, die Sie auch verwenden sollten.

Die sicherste Art zu zahlen ist, sich die Ware auf Rechnung schicken zu lassen und den Betrag im Nachhinein zu überweisen. So geht der Käufer nicht in Vorleistung und kann die Ware prüfen. Leider wird diese Möglichkeit nur selten angeboten, da sie ein größeres Risiko für den Onlineshop darstellt, nicht oder nur mit Verzögerung an sein Geld zu kommen.

TIPP: Sicher bezahlen

- Versuchen Sie, die Bezahlart dem Onlineshop anzupassen. Beim ersten Kauf ist der Lastschrifteinzug nicht die beste Wahl.
- Denken Sie daran, dass Ihnen als privater Käufer ein gesetzliches Umtauschrecht innerhalb von zwei Wochen zusteht.
- Kaufen Sie möglichst bei Onlineshops aus dem Inland, um rechtliche Schwierigkeiten im Ausland zu vermeiden.
- Überprüfen Sie Ihre Kontoauszüge auf Richtigkeit, wenn Sie etwas im Internet bezahlt haben.
- Bewahren Sie Bestellbestätigungen und Rechnungen in gedruckter oder digitaler Form auf!

Bezahlart	Vorteile	Nachteile
Kredit-karte	• Schnell • Weltweit anerkannt • Geldrückbuchung bei Missbrauch möglich	• Oft erneute Dateneingabe notwendig – Gefahr der Ausspähung • Verteilen von Finanzinformationen im Internet
Vorkasse	• Bekanntes Verfahren (einfach) • Es werden keine Finanzdaten des Käufers über das Internet ausgetauscht	• Langsam, da die Ware erst nach Geldeingang versendet wird • Basiert auf dem Vertrauen, dass der Onlineshop die Ware tatsächlich schickt • Einmal überwiesenes Geld lässt sich nicht zurückholen
Rechnung	• Kein finanzielles Risiko • Schnell • Es werden keine kritischen Finanz-daten über das Inter-net ausgetauscht	• Wird meist nur für Firmen oder Stammkunden angeboten
Nach-nahme	• Schnell • Es werden keine Finanzdaten über das Internet ausgetauscht	• Das Paket muss persönlich entgegen-genommen werden • Bei fehlerhafter Ware kann es zu Schwierig-keiten bei der Rücknahme kommen • Hohe Gebühren
Last-schrift-verfahren	• Geld kann in einer bestimmten Frist «zurückgeholt» werden	• Es werden Finanz-daten über das Internet ausgetauscht

	• Schnell	• Kontodeckung muss muss gewährleistet sein, sonst fallen teure Gebühren an
PayPal	• Sehr schneller Geldtransfer (wenige Minuten) • Käuferschutz bei ebay, teilweise Kostenvorteile beim Versand • Daten werden nur bei PayPal gespeichert, nicht bei mehreren Shops • Giropay, Kreditkarte, Lastschrift und Überweisung nutzbar	• Ein zentraler Account; ein Angreifer sollte Ihren PayPal-Account keinesfalls knacken können, deshalb unbedingt ein absolut sicheres Passwort wählen • Nicht bei jedem Onlineshop verfügbar
Online-Überweisung Giropay	• Vorteile wie bei «Rechnung» • Konzept der Banken • Daten nur der Bank bekannt (PIN und TAN) • Händler bekommt sofort Bezahlbestätigung	• Nicht bei jedem Onlineshop verfügbar • Nicht mit jeder Bank möglich
Clickand Buy (Firstgate)	• Vorteile wie bei «PayPal» (bis auf Käuferschutz bei ebay)	• Siehe PayPal

Abbildung 26: Vor- und Nachteile verschiedener Zahlungsarten im Internet

Auktionshäuser im Internet – 3, 2, 1 … Falle

Zum Ersten, zum Zweiten und zum Dritten. Etwas Nervenkitzel ist immer dabei, wenn eine Auktion läuft, und er macht den Kauf oftmals zu einem richtigen Erlebnis. Auch online ist das Ersteigern von Waren ganz groß in Mode und soll sogar süchtig machen. Stolze 8,541 Milliarden Euro betrug der Umsatz von ebay im Jahr 2008 und belegt damit eindrucksvoll die Beliebtheit von Onlineauktionen. Das bekannteste und weltweit größte Internetauktionshaus ist eine Instanz im Internet und soll hier als Beispiel dafür dienen, wie sicher oder unsicher Onlineauktionen sind. Auch die Frage, wie man sich dabei optimalerweise verhält, wird natürlich beantwortet.

Diese Fallen lauern bei Internetauktionen

Was das Bezahlen und die Registrierung angeht, gelten für Internetauktionen genau dieselben Regeln wie für den Onlineeinkauf (siehe Seite 113 ff.). Allerdings lauern auf Auktionswebseiten zusätzliche Gefahren. Denn im Gegensatz zu Einzelhändlern, bei denen es einen Verkäufer und viele Kunden gibt, kann bei ebay jeder die Rolle des Käufers und des Verkäufers übernehmen. Die geschäftlichen Verbindungen sind also extrem vielfältig und verwoben. Beliebt bei den Angreifern ist es daher, einen fremden ebay-Account zu «übernehmen». Die Zugangsdaten eines ebay-Mitglieds werden ausspioniert, und der ebay-Account eignet sich dann hervorragend, um fiktive Waren zu verkaufen. Die Folgen muss der Besitzer des ebay-Accounts ausbaden, der in den meisten Fällen überhaupt nichts davon mitbekommen hat. Es sei denn, er schaut während der falschen Auktionen in seinen ebay-Account, was jedoch

nur möglich ist, wenn die Angreifer sein Passwort und seine Daten in der Zwischenzeit nicht bereits geändert haben. Und genau das werden sie, damit der Nutzer nicht mehr an seinen ebay-Account herankommt. Die Übernahme Ihres ebay-Accounts können Sie vermeiden, indem Sie sichere Passwörter (siehe Seite 53f.) verwenden und die Zugangsdaten nicht weitergeben. Wenn sich alle daran halten, wird es für Angreifer sehr schwer, hier Missbrauch zu betreiben.

Aber warum sollte jemand auf die Idee kommen, die Zugangsdaten seines ebay-Accounts weiterzugeben? Diese Frage wird oft gestellt, und die wenigsten denken dabei an elektronische Fallen, die im Internet aufgestellt werden. Hier kommt das klassische Phishing zum Einsatz (siehe Seite 100ff.), bei dem der Nutzer aufgefordert wird, auf einen Link zu einer manipulierten Webseite zu klicken. Als Grund wird in diesen Fällen oftmals eine Neuerung am ebay-Account angegeben. Auch ist es möglich, über Cross-Site-Scripting-Angriffe Webseiten entsprechend zu verändern (siehe Seite 32f.). Daher sollten Sie niemals kleine, ominöse Anzeigen anklicken, die beispielsweise Gewinne offerieren oder angeblich zu ebay beziehungsweise einer anderen bekannten Webseite führen. Gewöhnen Sie sich zudem an, sich das Ziel eines Links in der Statusleiste des Browsers anzeigen zu lassen, bevor Sie tatsächlich draufklicken (siehe Seite 29f.).

TIPP: Onlineauktionen

- Verwenden Sie bei Auktionswebseiten nur sichere Passwörter und geben Sie Ihre Zugangsdaten nicht an Dritte weiter.
- Klicken Sie weder in E-Mails noch auf Webseiten auf seltsam erscheinende Angebote, die angeblich zu einem Auktionshaus führen.

- Beachten Sie zudem die Tipps aus den Abschnitten «Internetbrowser» (siehe Seite 26ff.) und «Bezahlen im Internet» (siehe Seite 118ff.).

So bieten Sie sicher mit

Auktionshäuser sind aber keinesfalls ein reiner Sündenpfuhl. Manchmal findet sich durchaus das ein oder andere Schnäppchen, und die Freude ist groß, wenn der Kauf günstig und erfolgreich war. Damit es hinterher jedoch keine bösen Überraschungen gibt, sollten Sie das Angebot und den Anbieter im Vorfeld genau unter die Lupe nehmen. Lesen Sie die Artikelbeschreibungen sorgfältig, damit Ihnen völlig klar wird, was genau zum Verkauf steht. Wenn ein Foto dabei ist, zeigt es eventuell mehr, als letztendlich zu ersteigern ist. So ist nicht selten ein Auto abgebildet, obwohl nur die Reifen angeboten werden.

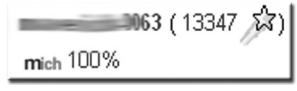


Abbildung 27: Benutzername mit Bewertung bei ebay

Ist ein Anbieter schon lange dabei und hat viele positive Bewertungen erhalten, ist das ein wichtiger Hinweis auf seine Vertrauenswürdigkeit. Deshalb sollten Sie nach jeder Auktion – egal ob Sie Käufer oder Verkäufer sind – eine Bewertung abgeben. Die Anzahl der Bewertungen zeigt sich hinter dem jeweiligen Nutzernamen.

So hat der Verkäufer in Abbildung 27 beispielsweise bereits an 13.347 Auktionen mitgewirkt und im Schnitt eine positive Bewertungsrate von 100 Prozent erhalten. Diesem Verkäufer

sollten potenzielle Bieter eher vertrauen als einem Verkäufer mit 74 oder 30 Prozent. Wollen Sie es genauer wissen, führt Sie ein Klick auf die Zahl hinter dem Verkäufernamen direkt zu den einzelnen Bewertungen.

Die Anbieter bei ebay können sowohl Privatpersonen als auch gewerbliche Händler sein, deren Zahl stark zugenommen hat. Diese unterliegen dann natürlich auch den gesetzlichen Pflichten. Das ist insofern gut zu wissen, da Sie die Ware bei einem offiziellen Händler innerhalb von zwei Wochen zurückgeben können. Wenn sich trotz Bewertung und genauen Studiums des Angebotstextes kein rechtes Vertrauen einstellen will, hilft es oftmals, den Verkäufer per E-Mail anzuschreiben und unklare Punkte noch einmal abzuklären. Die Geschwindigkeit und Art der Antwort gibt ebenfalls Aufschluss über die Vertrauenswürdigkeit des Anbieters.

Hat es dann schließlich mit dem Kauf geklappt, gilt es noch die passende Zahlungsart auszuwählen (siehe Seite 118 ff.), denn gerade bei wertvolleren Produkten ist es nicht unbedingt empfehlenswert, gegen Vorkasse zu bezahlen. Handelt es sich um kleinere Beträge, ist PayPal eine gute Alternative, da es einen Käuferschutz für ebay-Auktionen anbietet und in Fällen von falscher oder nicht gelieferter Ware das Geld erstattet. Bei größeren Summen bietet sich ein Treuhandservice an, der das Geld verwahrt, bis der Artikel ordnungsgemäß an seinem Bestimmungsort angekommen ist (Softlink 361).

TIPP: Sicheres Mitbieten bei Onlineauktionen

- Lesen Sie das Angebot genau, damit Sie exakt wissen, worum es sich bei dem Verkaufsgegenstand handelt.
- Fragen Sie bei Unklarheiten per E-Mail beim Händler nach, bevor Sie mitbieten.

- Überprüfen Sie die Bewertungen des Anbieters und wie lange er schon bei ebay aktiv ist.
- Beachten Sie, ob ein Händler oder eine Privatperson anbietet.
- Überprüfen Sie die angebotenen Zahlungsmöglichkeiten und nutzen Sie bei höheren Summen eine Bezahlart mit Käuferschutz oder sogar einen Treuhandservice.

Internettelefonie & Chatten – Kommunikation total

«Ich ruf dich aus Amerika an, sobald ich eine Telefonzelle gefunden habe, denn Handytelefonate und SMS aus dem Ausland sind ganz schön teuer. Allerdings fürchte ich, dass wir dann nicht oft voneinander hören werden …» Kennen Sie Sätze wie diese noch? In Zeiten des Internets gehören sie endgültig der Vergangenheit an, denn das Internet ist ein Kommunikationswunder – global und nicht standortgebunden. Urlauber können E-Mails anstelle von teuren und langsamen Briefen schreiben oder, wenn sie sich gleichzeitig mit ihrem Gesprächspartner im Internet befinden, einander Nachrichten schicken und direkt darauf antworten. Selbst um die Stimme eines anderen zu hören wird das herkömmliche Telefon nicht mehr unbedingt benötigt. Nutzer können heute mithilfe des Internets über alle Grenzen hinweg telefonieren und kommunizieren. Aber um ganz ehrlich zu sein: Eine E-Mail ist einfach nicht das Gleiche wie eine von Hand geschriebene Postkarte, die um den halben Erdball gereist ist. Nichtsdestotrotz soll in diesem Kapitel dargestellt werden, wie Sie das Internet für Telefonie und zum Chatten nutzen können und an welchen Stellen die Sicherheit eine Rolle spielt.

Internettelefonie – Wie funktioniert das?

Grundsätzlich bedeutet Internettelefonie nur, dass die Sprachdaten nicht mehr über das herkömmliche Telefonnetz übermittelt werden, sondern als Datenpakete über die Internetinfrastruktur. Daher wird die Internettelefonie als Voice over IP, kurz VoIP, bezeichnet, wobei IP (Internetprotokoll) einfach ausgedrückt das Protokoll ist, mit dem die Daten im Internet übertragen werden.

Einige Telefonanbieter nutzen VoIP bereits seit Jahren im Hintergrund, um die Sprachdaten an ihr Ziel zu befördern. Aber auch viele Nutzer telefonieren heute – manche sogar, ohne es zu wissen – mit VoIP. Denn zahlreiche DSL-Anbieter stellen den Telefondienst über das Internet zur Verfügung. In diesem Fall ist bei der ausgelieferten Hardware ein Modem dabei, an das die Telefonanlage oder das herkömmliche Telefon angeschlossen wird. Darüber hinaus gibt es natürlich auch «echte» VoIP-Telefone, die direkt an den Internetanschluss (beziehungsweise Netzwerkanschluss) angeschlossen werden. Dann müssen nur noch die Zugangsdaten des jeweiligen VoIP-Anbieters eingegeben werden, und schon kann der Nutzer telefonieren. Dabei handelt es sich entweder um reine VoIP-Anbieter, wie zum Beispiel sipgate, oder um den Provider des Internetanschlusses.

Für VoIP wird jedoch nicht zwingend ein Telefon benötigt. Die Telefonie kann genauso direkt über den Computer ablaufen. Dazu benötigt der Nutzer eine Mikrofon/-Lautsprecher-Kombination (Headset) sowie ein Softphone. Ein Softphone (siehe Abbildung 28) ist ein Computerprogramm, das ein Telefon simuliert. Sie können es kostenlos im Internet herunterladen (Softlink 371). Auch hier müssen nur

die Zugangsdaten des VoIP-Anbieters eingegeben werden, und schon kann telefoniert werden. Für Gespräche innerhalb des Internets fallen dabei normalerweise keine Kosten an.



Abbildung 28: Ein typisches Softphone

VoIP-Anbieter ermöglichen über entsprechende Gateways zudem Anrufe ins Fest- oder Mobilfunknetz. Hierfür werden zwar Gebühren berechnet, aber diese sind meist wesentlich geringer als die eines herkömmlichen Telefonanbieters.

VoIP ist technisch inzwischen sehr ausgereift und bietet in der Regel eine gute Sprachqualität sowie einige Komfortfunktionen, die beim herkömmlichen Telefonieren nicht möglich sind. Voraussetzung ist allerdings ein schneller DSL-Anschluss (mit Flatrate), der die zügige Übertragung großer Datenmengen zulässt, da beim Telefonieren die Leitung nicht

nur für den Austausch der Sprachdaten, sondern auch für die Übermittlung aller anderen Daten genutzt wird – schnelles UMTS (siehe Seite 160 f.) funktioniert natürlich ebenso. Das ist auch der Grund, warum die Sprachqualität bei einem sehr hohen Datenaufkommen leidet.

In der Standardanwendung ist VoIP nicht verschlüsselt. Das bedeutet, dass ohne zusätzliche Vorkehrungen alle Sprachdaten von Dritten, die auf irgendeine Weise an die Leitung angeschlossen sind, wie zum Beispiel andere Computer im Netzwerk, «mitgeschnitten» werden können. Es ist daher sinnvoll, einen Anbieter zu wählen, der eine Verschlüsselung zur Verfügung stellt. Geht das aus der Beschreibung nicht hervor, sollten Sie nachfragen, ob und wie der VoIP-Anbieter verschlüsselt und welche Einstellungen Sie dafür eventuell vornehmen müssen.

TIPP: Internettelefonie

- Die Qualität eines VoIP-Gesprächs hängt stark von der Leistungsfähigkeit (Bandbreite) des Internetanschlusses ab. Aktuelle DSL-Anschlüsse sind die Mindestanforderung.
- VoIP ist in der Standardanwendung nicht verschlüsselt. Informieren Sie sich deshalb bei Ihrem Anbieter, ob Ihre Telefonate verschlüsselt werden und welche Einstellungen Sie dafür gegebenenfalls vornehmen müssen.
- VoIP-Telefonie ist nur bei einer Flatrate sehr kostengünstig, da viele Daten übertragen werden.

Chatten – die moderne Echtzeitkommunikation

Chatten bedeutet so viel wie plaudern und bezeichnet die Kommunikation per Texteingabe in Echtzeit. Das ist die offi-

zielle Definition, aber es gibt mittlerweile sehr unterschiedliche Ausprägungen.

Webchat

Webchats, die in Webseiten eingebettet sind, sind die Chats der ersten Stunde. Der Nutzer meldet sich an und kann in einem Chatroom mit anderen Nutzern Textnachrichten austauschen. In den Webchats sind meist mehrere Personen gleichzeitig anwesend, aber es gibt auch die Möglichkeit, mit einzelnen Anwesenden ein «Privatgespräch» zu beginnen.

Der Erfolg der Chatrooms lässt sich auch darauf zurückführen, dass die Gesprächspartner anonym bleiben. Ein Chatter meldet sich mit einem fiktiven Namen an, und niemand weiß, wer sich dahinter verbirgt – ob Mann, ob Frau, ob jung, ob alt. Diese Anonymität hat sowohl positive als auch negative Auswirkungen.

Von Vorteil ist diese Art der Kommunikation zum Beispiel für Beratungsstellen. Die Hemmschwelle der Betroffenen, über ihre Probleme zu reden, ist dabei deutlich geringer. Auch für Serviceaufgaben lassen sich Chats gut verwenden, zum Beispiel für Supportanfragen zu Produkten oder bei Reklamationen. Auf der anderen Seite bringt die Möglichkeit, genau die Identität anzunehmen, die man gerade haben möchte, Gefahren mit sich, welche die Chats ziemlich in Verruf gebracht haben. Denn im realen Leben würde man sich intuitiv von zwielichtigen, nicht vertrauenswürdig wirkenden Menschen fernhalten und es gar nicht erst zu einer Kontaktaufnahme kommen lassen. Anonyme Chatrooms machen aber genau das nahezu unmöglich. So können auch Menschen mit kriminellen Absichten durch längere Gespräche Vertrauen bei ihrem Gegenüber aufbauen. Sollte es dann zu einem realen

Treffen kommen, kann es gefährlich werden. Deshalb ist es wichtig, dass jedem Chatter die Anonymität des Chats und ihre Folgen bewusst sind. Lassen Sie sich also nicht auf seltsame Gespräche oder spätere Treffen ein, wenn Ihr Gegenüber sich vorher nicht glaubwürdig zu erkennen gegeben hat. Außerdem sollten Sie in einem Chat nicht leichtfertig persönliche Daten preisgeben. Der gewählte Benutzername, auch Nickname genannt, den sich jeder Chatter geben muss, sollte keine Rückschlüsse auf Ihre reale Identität zulassen. Eventuell ist Ihr Gesprächspartner ein potenzieller Einbrecher und versucht über geschickte Fragen herauszufinden, wo Sie wohnen und wann Sie nicht zu Hause sind.

Eine ganz andere Gefahrenquelle stellen die Links dar, die in Chats verteilt werden. Für sie gilt dasselbe wie für Links in E-Mails und auf Webseiten (siehe Seite 73 ff.): Niemals unbedacht anklicken!

TIPP: Das sollten Sie im Webchat beachten

- Denken Sie immer daran, dass Sie in einem anonymen Chat nie sicher wissen können, wer sich hinter dem Namen des Gegenübers verbirgt.
- Geben Sie nicht leichtfertig Informationen über sich preis.
- Wählen Sie als Nickname immer einen Fantasienamen, der keine Rückschlüsse auf Sie zulässt.

Instant Messaging

Deutlich stärker verbreitet und auch in Firmen im Einsatz ist mittlerweile das Instant Messaging. Für diese Art des Chattens wird ein Programm auf dem Computer benötigt, das mit einem entsprechenden Dienst im Internet verbunden wird. Bekannte Anbieter von Messaging-Diensten sind ICQ, MSN

und GoogleTalk. Jeder dieser Anbieter stellt meist ein eigenes Programm (Messenger) für das Instant Messaging zur Verfügung. Es gibt jedoch auch freie – meist kostenlose – Messenger wie Pidgin oder Trillian, welche die Möglichkeit bieten, mehrere Konten von verschiedenen Anbietern gleichzeitig zu verwalten (siehe Abbildung 29).

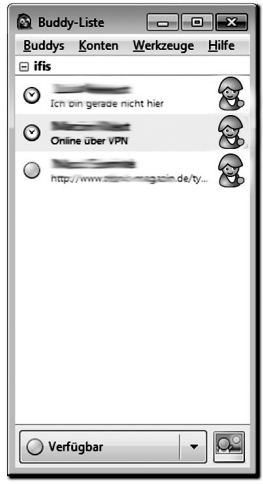


Abbildung 29: Typischer Messenger mit zwei aktiven Konten

Beim Instant Messaging führt der Nutzer eine Liste von Gesprächspartnern, mit denen er spontan Kontakt aufnehmen kann. Er kann sehen, wann die Teilnehmer online sind und in separaten Chatfenstern mit ihnen kommunizieren. Anonym ist der Gesprächspartner in diesem Fall normalerweise nicht.

Instant Messaging ist zu einer gängigen Art der Kommunikation geworden, um mit Freunden und Kollegen in Echtzeit kurze Informationen auszutauschen. Zusätzliche Komfortfunktionen, wie zum Beispiel die Übertragung von Dateien, sind bei den Messengern inzwischen Standard.

Allerdings bilden Messenger auch eine Spielwiese für Angreifer. Es gilt daher auch hier wieder das Gebot, keine unbekannten Links anzuklicken und möglichst wenige Informationen über sich preiszugeben. Schauen Sie sich dazu die angebotenen Einstellungen zur Privatsphäre genau an. Auch sollten Sie Anfragen von Fremden, die in Ihre persönliche Kontaktliste aufgenommen werden möchten, grundsätzlich ablehnen, da es sich dabei um Angriffe oder um Spam, also unerwünschte Werbeangebote, handeln kann.

Genau wie bei der Internettelefonie (siehe Seite 126 ff.) sind die Nachrichten beim Instant Messaging zunächst einmal nicht verschlüsselt. Dementsprechend sollten keine sicherheitskritischen Daten übermittelt werden. Für manche Messenger gibt es allerdings entsprechende Plug-ins, also Zusatzprogramme, die eine sogenannte Ende-zu-Ende-Verschlüsselung zwischen den Gesprächspartnern zulassen. Ein solches Plug-in ist OTR (Off-the-Record), was so viel wie «vertraulich» bedeutet. Neben der Verschlüsselung der Nachrichten kann bei OTR auch nicht mehr nachvollzogen werden, wer die Nachrichten geschrieben hat. Im Fachjargon spricht man bei dieser Funktion von Abstreitbarkeit. Das Einrichten von OTR ist einfach und basiert darauf, dass die beiden kommunizierenden Personen ein Geheimnis austauschen, beispielsweise ein Passwort (OTR-Workshop, siehe Softlink 372).

TIPP: Wichtig beim Instant Messaging

- Schauen Sie sich die Einstellungen des Messengers zur Privatsphäre an und geben Sie so wenig persönliche Informationen wie möglich preis.
- Nehmen Sie nur Ihnen bekannte Personen in Ihre Kontaktliste

auf und weisen Sie Anfragen von Unbekannten grundsätzlich zurück.
- Klicken Sie nicht unbedarft auf Links in Nachrichten, die Sie nicht zuordnen können.
- Geben Sie keine sicherheitsrelevanten Daten über einen Messenger weiter, außer Sie nutzen eine Verschlüsselung wie OTR.

Exkurs: Skype – ein prominenter Vertreter für VoIP und Messaging

Skype ist der wohl bekannteste Internettelefondienst und soll deshalb hier kurz aufgeführt werden. Er vereint Internettelefonie und Messaging, womit Skype allerdings nicht allein ist. Auch andere Dienste bieten bereits beides in Kombination an. Telefonate innerhalb des Skype-Netzes, also zwischen zwei Skype-Nutzern, sind kostenlos.

Der Nutzer hat aber darüber hinaus die Möglichkeit, Geld auf sein Skype-Konto zu laden und so auch ins Fest- oder Handynetz zu telefonieren, SMS zu schreiben oder Faxe zu verschicken. Skype-Telefonate sind verschlüsselt, allerdings gibt Skype nicht preis, auf welche Art. Im Fachjargon wird dies «Security by Obscurity» genannt, aber aktuell scheint die Verschlüsselung sicher zu sein. Hinzu kommen noch einige weitere Komfortfunktionen.

TIPP: Skype
- Skype-Telefonate sind von vornherein verschlüsselt.
- Bei der Benutzung von Skype sind alle Tipps zu beachten, die auch schon bei den Punkten «Internettelefonie» und «Messaging» genannt wurden.

Kindersicherung fürs Internet – keine Sorge um den Nachwuchs

Kinder sind «Digital Natives», das bedeutet, dass sie in eine Welt mit Computern, Internet und Handys geboren wurden. Die aktive Nutzung des Internets ist deshalb ein natürlicher Teil ihres Lebens. Es ist neben der Familie, dem Freundeskreis, der Schule und Freizeitgruppen auch erheblich an der Erziehung der Kinder beteiligt und prägt ihre Wertvorstellungen und Verhaltensweisen.

Daher muss es das Ziel sein, Kinder frühzeitig mit diesem Medium vertraut zu machen, damit sie den eigenverantwortlichen und kompetenten Umgang mit dem Computer und dem Internet lernen. Sie müssen wissen, welche Gefahren im Internet lauern, welche Regeln es einzuhalten gilt und wie man sich generell im Internet verhält. Das können Eltern, Lehrer und andere Erziehungsverantwortliche aber nur dann vermitteln, wenn sie selbst über die entsprechende Internetkompetenz verfügen!

TIPP: Entwicklung von Internetkompetenz

- Eignen Sie sich als Erziehungsverantwortlicher selbst die nötige Internetkompetenz an, damit Sie in der Lage sind, diese weiterzuvermitteln.
- Seien Sie Vorbild im Umgang mit dem Internet. Wenn Sie von Ihren Kindern erwarten, dass sie keine Musik illegal herunterladen, dann sollten Sie das ebenfalls nicht tun.
- Erkunden Sie gemeinsam mit Ihren Kindern die Nutzungsmöglichkeiten des Internets und seien Sie bereit, von Ihren Kindern zu lernen.

Welche Inhalte für Kinder geeignet sind und worauf Sie achten müssen

Kinder sind leichter zu beeinflussen, zu beeindrucken und auch zu verunsichern als Erwachsene. Deshalb sollten sie nicht auf Webseiten geraten können – absichtlich oder zufällig –, die schädlich für sie sind, wie zum Beispiel solche mit Gewalt verherrlichenden, pornographischen und rassistischen Inhalten. Aber auch soziale Netzwerke können für Kinder eine Gefahr darstellen: Pädophile versuchen, Kinder im Chat zu persönlichen Treffen zu überreden, Dealer nutzen die Internetplattform, um Drogen zu verkaufen, und Selbstmordforen gefährden Kinder, die sich in einer labilen Stimmungslage befinden.

Um Ihre Kinder davor zu schützen, sollten Sie mit ihnen regelmäßig über mögliche Gefahren reden und ihnen entsprechende Regeln und Handlungsempfehlungen an die Hand geben (siehe Tipp).

TIPP: Allgemeine Verhaltensregeln für Kinder

- Glaube nicht alles, was du im Internet liest.
- Gib niemals im Internet deinen Namen, deine Adresse und deine Telefonnummer bekannt.
- Pass auf, wenn du aus dem Internet Dateien herunterlädst.
- Sprich mit deinen Eltern oder anderen Vertrauenspersonen, bevor du dich mit Bekanntschaften aus dem Internet triffst.
- Das Internet ist kein rechtsfreier Raum.
- Das Umgehen von Schutzmaßnahmen ist verboten.
- Denke dir in Chaträumen einen Fantasienamen aus und erfinde eine Adresse (das ist keine Lüge, sondern ein Schutz).
- Vertraue deine Passwörter niemandem an.

Kinder unter zehn Jahren

Kinder unter zehn Jahren sollten bei der Nutzung des Internets sehr intensiv betreut werden und nicht unbeaufsichtigt im Internet «unterwegs» sein. Zwar reicht der Basisschutz aus, um schädliche Software abzuwehren, aber Kinder haben den gesunden Menschenverstand für das Surfen noch nicht entwickelt. Sie sind noch nicht in der Lage, sich gegen Gewaltdarstellungen, Pornographie usw. selbst zu schützen.

Für Kinder im Vorschul- und Grundschulalter gibt es im Internet ein breit gefächertes Angebot an speziellen Kinderwebseiten und Suchmaschinen, deren Inhalte dem Alter angemessen sind. Beispiele dafür sind:

- http://www.fragfinn.de
- http://www.blinde-kuh.de
- http://www.internauten.de
- http://www.internet-abc.de

Eine ausführlichere Auflistung von kindgerechten Webseiten finden Sie unter http://www.seitenstark.de. Da sich das Angebot jedoch ständig verändert, sollten Sie sich gemeinsam mit den Kindern ein Bild darüber machen, welche Webseiten tatsächlich für das jeweilige Alter angemessen sind.

Die Webseite http://schau-hin.info rät, bei der Suche nach guten Kinderwebseiten besonders auf folgende Kriterien zu achten:

- *Gut gemacht*: Die Themen der Webseite sind attraktiv, aktuell, spielerisch, kind- und altersgerecht sowie interaktiv aufbereitet. Kinder finden sich leicht auf der Webseite zurecht.
- *Sicherheit*: Damit Kinder sicher chatten können, gibt es bestimmte Mindeststandards. Dazu gehört, dass erwachsene

Moderatoren bei den Chats anwesend sind, Kinder über einen Notruf jederzeit mit der Redaktion sprechen können und Datenaustausch sowie Webcam-Übertragungen tabu sind.

- *Persönliche Daten*: Gute Kinderwebseiten sollten nur die nötigsten Angaben abfragen. Persönliche Daten wie Adresse, Telefonnummer und Hobbys bleiben geheim.
- *Keine Werbung*: Kinder können Werbung von redaktionellen Informationen nur schwer trennen. Deshalb enthalten geeignete Kinderwebseiten möglichst keine Werbung. Wenn doch, ist die Werbung klar als solche gekennzeichnet und stört nicht beim Surfen.
- *Klarer Absender*: Die Kinderwebseite beinhaltet eine kurze Selbstdarstellung. Darin wird beantwortet, worum es bei dem Onlineangebot geht, wer dahinter steckt und wie derjenige zu erreichen ist.

Kinder über zehn Jahren

Kinder, die älter als zehn Jahre sind, lassen sich in der Regel nicht mehr gern «über die Schulter» schauen. Und sie neigen dazu, alles am Computer und im Internet auszuprobieren. Die Vorteile dieses unbefangenen Umgangs mit dem Internet liegen auf der Hand: Die Kinder können mit Freunden chatten, neue Freundschaften knüpfen, spielen, Musik hören und vieles mehr.

Allerdings ist es notwendig, dass Sie als Eltern im kontinuierlichen Gespräch mit den Kindern bleiben und darüber informiert sind, was diese im Internet tun. Auch sollten Sie entsprechende Nutzungsvereinbarungen mit Ihren Kindern treffen (wie oft und wie lange).

TIPP: Vereinbarungen mit Kindern

- Stellen Sie für Ihre Kinder Regeln bezüglich der Nutzung des Internets auf (zeitlich und inhaltlich) und achten Sie auf deren Einhaltung.
- Verabreden Sie mit Ihren Kindern, dass sie Ihnen Dinge im Internet zeigen, die ihnen seltsam vorkommen oder Angst machen.

Kinderschutzprogramme

Es gibt auch Software, die dabei hilft, das Risiko für Kinder im Internet zu minimieren. Beispiele für kostenlose Jugendschutzprogramme sind www.parents-friend.de und www.jugendschutzprogramm.de.
Das Leistungsspektrum solcher Programme ist umfangreich. In der Regel bieten sie folgende Sicherheitsmaßnahmen:

- Sperrung bestimmter Webseiten
- Beschränkung der Zeiten, innerhalb derer das Internet oder der Computer durch die Kinder genutzt werden kann.
- Beschränkung der Laufzeiten bestimmter Programme, wie zum Beispiel von Computerspielen.
- Absicherung von Systemeinstellungen, die Kinder versehentlich oder bewusst verändern möchten.
- Einschränkungen von Verzeichnissen, Laufwerken und Programmen

Neben Jugend- und Kinderschutzprogrammen für den gesamten Computer gibt es auch entsprechende Add-ons für den Browser. Ein Beispiel hierfür ist das Add-On Glubble für den Firefox (Softlink 381), das wie auf Seite 45 beschrieben installiert wird. Damit lässt sich eine Familienseite anlegen,

und es können Rechte für die einzelnen Familienmitglieder vergeben werden. Wird der Browser in den Kindermodus geschaltet, bekommt er ein kindgerechtes Aussehen und zeigt nur noch bestimmte Seiten an. Möchte das Kind einen Inhalt sehen, der noch nicht freigeschaltet ist, kann es automatisiert eine Anfrage an die Eltern senden. Achtung: Ist ein zweiter Browser ohne Kinderschutz installiert, kann das Kind natürlich auch diesen nutzen und ungeschützt im Internet surfen. Das sollte entsprechend vermieden werden. Glubble sollte jedoch immer nur ein unterstützender technischer Zusatz sein und das gemeinsame Entdecken des Internets nicht ersetzen.

TIPP: Verbotene Inhalte

Wenn Sie oder Ihre Kinder fragwürdige oder verbotene Webseiten und Angebote im Internet entdecken, dann melden Sie dies dem Verband zur Freiwilligen Selbstkontrolle unter www.internet-beschwerdestelle.de. Diese Einrichtung kann gegebenenfalls geeignete Schritte gegen den Webseitenbetreiber einleiten. Weitere und aktualisierte Informationen zum Kinderschutz im Internet finden Sie unter Softlink 382.

Antennen ausfahren – Zugang zum Internet

«Es hat gefunkt» steht umgangssprachlich für den Anfang einer Verbindung zwischen zwei Menschen oder auch dafür, etwas begriffen zu haben. Um die Funktechnik zu erklären, wäre ein Ausflug in die Physik notwendig, der Ihnen hier aber erspart bleiben soll.

Funknetzwerke sind «die begonnene Zukunft». Kaum eine Technologie hat sich so rasant verbreitet wie Wireless LAN (WLAN), aber auch seine «Kollegen» GSM, UMTS, Bluetooth und Co. sind gewaltig auf dem Vormarsch. Denn sie bilden die Basis für das prognostizierte «Überall-Internet». Und die Möglichkeiten scheinen in der Tat grenzenlos: Während eines Stadtbummels durch eine historische Altstadt doziert das Handy im Vorbeigehen über ein Gebäude – die Daten dazu kommen direkt aus dem Internet. Im Café an der Ecke können Internetnutzer frühstücken und gleichzeitig mit dem Handy, dem Notebook oder einer WLAN-Uhr ihre E-Mails abfragen. Und auch zu Hause ist es vorbei mit dem Kabelchaos. Arbeiten mit dem Notebook auf der Couch wird zum entspannten Erlebnis.

Die Funktechnologie bietet eine Menge Vorteile – aber auch Gefahren, wenn sie nicht richtig eingesetzt wird. Denn sensible Daten, die über die Luft übertragen werden, können ganz einfach mitgelesen werden, wenn sie nicht ausreichend geschützt sind. Deshalb wird in diesem Kapitel der richtige

und vor allem sichere Umgang mit den unterschiedlichen Funktechnologien erläutert.

DSL und WLAN – sicher einrichten und sicher nutzen

Vor einigen Jahren stellte bereits ein Prominenter in einem Fernsehspot die Frage: «Bin ich schon drin?» Die damalige Werbung eines Internetanbieters sollte suggerieren, wie einfach es ist, mit seiner Zugangstechnologie ins Internet zu gelangen. Auch lag zu dieser Zeit noch jede Woche eine CD in deutschen Briefkästen, die 50 Stunden kostenloses Surfen versprach – ein Angebot, das heute, da die Flatrate die privaten Haushalte erobert hat, niemanden mehr hinter dem Ofen hervorlocken würde. Sie sehen, auch vor zehn Jahren versprach die Werbung schon den problemlosen Anschluss des Computers ans Internet. Aber damals wie heute gibt es immer wieder Probleme …

Dieses Kapitel soll Ihnen einen kurzen Überblick geben, wie ein Internetanschluss heutzutage eingerichtet wird. Ein besonderes Augenmerk liegt dabei auf dem DSL-Router mit WLAN-Funktion, der in der Regel vom Anschlussanbieter gleich mitgeliefert wird.

Was ist Wireless LAN (WLAN) genau?

Die Abkürzung WLAN steht für Wireless Local Area Network, die kabellose Datenübertragung in Verbindung mit Computern, Notebooks, Handys, Lautsprechern, Internetradios, Massenspeichern oder Inventurscannern in Kaufhäu-

sern. Es ist fraglos eine eindrucksvolle Technik, bei der die Daten in Funkwellen übertragen und wieder aufgefangen werden. Die Reichweite eines normalen WLAN-Routers beträgt 30 bis 100 Meter (mit einer entsprechenden Antenne bis 300 Meter), wobei der Empfang durch Hindernisse wie dicke Wände beeinträchtigt oder sogar komplett verhindert werden kann. Aber die Reichweite der Funksignale kann mit zusätzlichen Routern, die das Funksignal als Repeater auffangen und weiterleiten, verlängert werden. Direkte WLAN-Verbindungen zwischen zwei oder mehreren Endgeräten ohne feste Infrastruktur nennt man auch Ad-hoc-Modus.

DSL – die Varianten

Es gibt verschiedene Möglichkeiten, ins Internet zu gelangen. Für den privaten Haushalt sind vor allem zwei Varianten üblich. Die erste ist der traditionelle Zugang über die Telefonleitung. Digital Subscriber Line (DSL) bezeichnet dabei einen

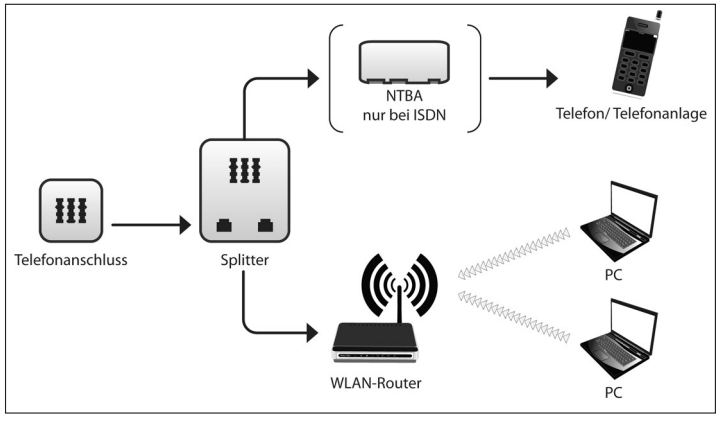


Abbildung 30: Verkabelung der notwendigen Geräte bei einem DSL-/Anschluss über die Telefonleitung (WLAN-Router mit integriertem Modem)

Übertragungsstandard, der Daten mit hohen Übertragungsraten über einfache Telefonleitungen zum Internet sendet und von dort empfängt.

Die zweite Variante ist der Zugang über das Netz eines Kabelbetreibers, also über die Steckdose, an die auch der Fernseher angeschlossen ist. Bei dieser Variante ist in der Regel ein «Telefonanschluss» mit integriert, wodurch die eigentliche Telefonleitung eventuell überflüssig wird. Allerdings muss hier teilweise noch mit Qualitätseinbußen gerechnet werden (siehe Seite 128f.).

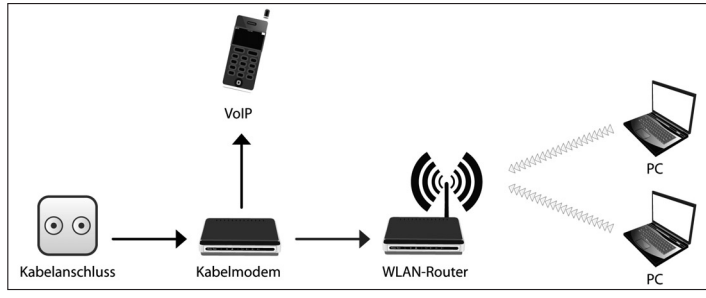


Abbildung 31: Verkabelung der notwendigen Geräte bei einem DSL-Anschluss über das Kabelnetz

Je nach Anschlussart erhält der Kunde ein DSL- oder Kabelmodem für den Telefonanschluss, das gemäß der beiliegenden Anleitung angeschlossen wird. Bei DSL über den Telefonanschluss wird außerdem ein Splitter verwendet, der das Telefon- und das Datensignal trennt. Bei Verwendung von ISDN kommt hinter dem Splitter in der Telefonleitung noch eine Box namens NTBA zum Einsatz. Zusätzlich erhält der Kunde im Allgemeinen einen WLAN-Router. Dieser wird mit dem jeweiligen Modem beziehungsweise über ein Kabel direkt mit dem Telefonanschluss verbunden (sofern das Mo-

dem bereits im Router integriert ist). Für Nutzer, die sich das Einrichten des Internetzugangs nicht selbst zutrauen, bieten die Internetanbieter mittlerweile die Einrichtung der Geräte zu einem Pauschalpreis an.

DSL-Router sicher konfigurieren

Ein Router ist ein Netzkoppelelement, das im Einsatzfeld Heimnetzwerk die Schaltstelle zwischen dem Hausanschluss in den eigenen vier Wänden und dem Internet bildet. Ein Router entscheidet, welche Daten aus dem Internet wohin ins Heimnetzwerk geschickt werden und umgekehrt. Er ist für die Internetverbindung jedoch nicht zwingend notwendig. Wird nur ein einziger Computer angeschlossen, kann dieser direkt mit dem Modem verbunden werden. Das ist heutzutage aber eher unüblich und im Hinblick auf die Erweiterbarkeit und Sicherheit auch nicht sinnvoll. Um sämtliche Sicherheits-, Mobilitäts- und Praktikabilitätsvorteile nutzen zu können, sind Router Standard, die auch WLAN anbieten, also WLAN-Router. An einen handelsüblichen WLAN-Router lassen sich im Normalfall vier Computer per Kabel anschließen und meist 253 Geräte per WLAN (zumindest theoretisch, mehr als fünf sind jedoch nicht empfehlenswert).

Die Konfiguration des Routers ist je nach Hersteller und Internetanbieter unterschiedlich, lässt sich aber im Normalfall über die mitgelieferte Software von einem angeschlossenen Computer aus durchführen. Dabei gilt es immer drei Dinge zu erledigen:

- Einstellen der Verbindung zum Internetanbieter mit Zugangsdaten (bei Internetverbindungen über das Kabelnetz fällt diese Einstellung meist weg)

- Einstellen der WLAN-Funktionen
- Überprüfen/Konfigurieren der Sicherheitseinstellungen

Um den Nutzer bei diesen Aufgaben zu unterstützen, denken sich die Hersteller immer neue Assistenzprogramme und Methoden aus. Deshalb können hier nicht alle Möglichkeiten der Routerkonfiguration beschrieben werden. Stattdessen wird ein Weg vorgestellt, der – unabhängig vom verwendeten Modell und Internetanbieter – eigentlich immer funktioniert.

Alle Router können über ihr sogenanntes Webinterface bedient werden. Verbinden Sie dazu zunächst den Router über ein Kabel mit dem Computer (das Modem muss entsprechend der Anleitung in die Telefon- oder Kabeldose eingesteckt sein). Dann öffnen Sie auf dem angeschlossenen Computer den Browser und geben in die Adresszeile die Adresse des Routers ein. Diese lautet in der Regel 192.168.1.1, 192.168.2.1 oder 192.168.1.0. Genauere Angaben finden Sie in der Anleitung Ihres Geräts. Haben Sie die richtige Adresse aufgerufen, geben Sie die Zugangsdaten, die ebenfalls in der Anleitung angegeben sind, in Form von Benutzername und Passwort in die entsprechende Eingabemaske ein. Im Anschluss daran zeigt der Router sein Webinterface, in dem Sie alle notwendigen Einstellungen vornehmen können. Nutzen Sie dazu den Einrichtungsassistenten, sofern einer vorhanden ist. Als Allererstes aber sollten Sie das Passwort des Routers ändern, da es sich im Auslieferungszustand um ein Standardpasswort handelt, damit nur Sie als Administrator des Routers Zugriff haben.

Die Abbildung 32 zeigt beispielhaft das Webinterface eines Routers. Je nach Hersteller wird es kleine Unterschiede geben, aber die Grundfunktionen sind immer dieselben.

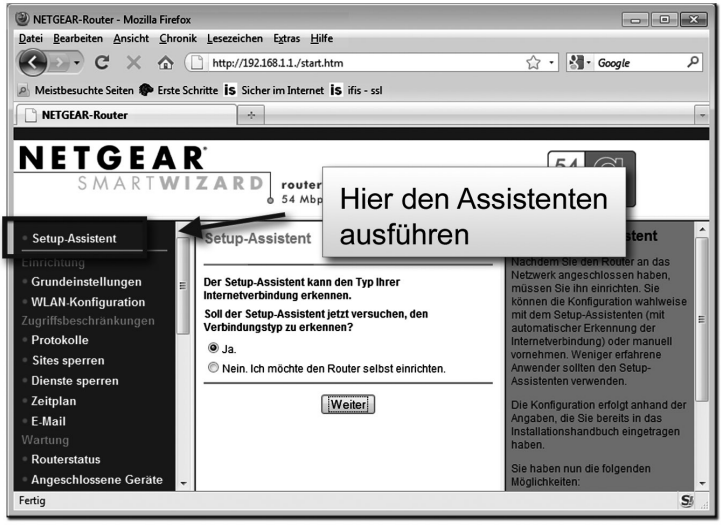


Abbildung 32: Webinterface eines Routers in der Übersicht

Ziehen Sie nun die Betriebsanleitung des jeweiligen Modells zurate, um alle notwendigen Einstellungen durchzuführen. Wichtig ist an dieser Stelle zu verstehen, zwischen welchen Geräten die jeweiligen Verbindungen aufgebaut werden. Das WLAN wird nur zwischen WLAN-Router und dem empfangenden Computer aufgebaut. Die Internetverbindung dagegen wird zwischen Router, Modem und Internetanbieter aufgebaut. Die häufigsten Fehler, die dabei passieren können, sind:

- Ein WLAN-Router kann erst eine Verbindung zum Internet aufbauen, wenn alle Geräte ordnungsgemäß verbunden sind und die Zugangsdaten des Internetanbieters korrekt in den Router beziehungsweise das Modem (bei Anschlüssen über Kabel) eingegeben wurden.
- WLAN funktioniert normalerweise nicht sofort, sondern muss erst konfiguriert werden. Dafür ist beim Einrichten

meist eine Kabelverbindung zwischen WLAN-Router und Computer notwendig. Es gibt allerdings auch WLAN-Router, die eine Funkverbindung mit einem dazugehörigen Empfänger (zum Beispiel USB-WLAN-Stick) per Knopfdruck einrichten können.

Ein grundsätzliches Vorgehen beim Router lautet – auch in Bezug auf die Sicherheit: Alles was nicht gebraucht wird, gehört ausgeschaltet. Deaktivieren Sie dementsprechend die WLAN-Funktion im Webinterface, wenn Sie diese nicht verwenden. Keine Sorge, sie lässt sich jederzeit wieder aktivieren. Auch der WLAN-Router selbst sollte ausgeschaltet werden, wenn er über längere Zeit nicht gebraucht wird. Das spart Strom, vermeidet Fehler und vermindert potenzielle Angriffsflächen.

Übrigens: Fast alle WLAN-Router verfügen über eine zusätzliche Sicherheitsfunktion, die immer angeschaltet sein sollte – eine Firewall.

Diese Firewall überprüft den Netzwerkverkehr zwischen dem Internet und dem Heimnetzwerk und achtet darauf, dass keine Ungereimtheiten auftreten, die auf einen Angriff schließen lassen. Standardangriffe von außen wehrt die Firewall im Router direkt ab. Sie ist damit eine prima Ergänzung zur Personal Firewall auf den Computern (siehe Seite 14 ff.), kann diese aber nicht ersetzen.

Im Regelfall wird Ihr Router noch weitere (Profi-)Einstellungen bieten, die aber für den Hausgebrauch im Allgemeinen bereits vorkonfiguriert sind. Diese Funktionen und Einstellungen sollten Sie nur verwenden beziehungsweise verändern, wenn Ihnen die Auswirkungen genau bekannt sind (Router konfigurieren, siehe Softlink 411).

TIPP: Routerkonfiguration

- Wenn Sie sich mit der Technik gar nicht auskennen, lassen Sie sich den Internetzugang vom Internetanbieter einrichten. Das kostet oft nur eine kleine Pauschale oder ist sogar im Angebot enthalten.
- Schalten Sie den WLAN-Router ab, wenn Sie ihn länger nicht benutzen. Das spart Strom und entzieht eventuellen Angreifern die Angriffsfläche.
- Deaktivieren Sie die WLAN-Funktion, wenn Sie sie nicht verwenden.
- Aktivieren Sie die Firewall des Routers (normalerweise ist das per Voreinstellung gegeben).
- Ändern Sie bei der Inbetriebnahme eines Routers das Zugangspasswort und bewahren Sie es sicher auf, am besten im Gedächtnis.

Die richtige WLAN-Verschlüsselung

Grundsätzlich lässt sich jede Funkverbindung für den normalen Gebrauch bedenkenlos einsetzen, wenn im Vorfeld die entsprechenden Sicherheitsvorkehrungen getroffen wurden. Das Wichtigste ist die Verschlüsselung der Daten, denn über das WLAN übertragene, unverschlüsselte Daten können von jedem, der sich in Reichweite des WLANs befindet, abgefangen werden – auch ohne große technische Kenntnisse. Heikel wird das vor allem dann, wenn es sich dabei um persönliche und sicherheitskritische Daten handelt. Für ein Firmennetzwerk gilt das natürlich erst recht.

Aktuell gibt es drei grundsätzliche Verschlüsselungsmethoden zur Absicherung des WLAN-Funkverkehrs: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) und

WPA2. Die WEP-Verschlüsselungsmethode ist bereits vor Jahren geknackt worden und nicht mehr sicher genug, da sie innerhalb von nur zwei Minuten mit einfachsten Mitteln entschlüsselt werden kann. Die darauf aufbauende WPA-Verschlüsselungsmethode ist noch nutzbar, aber nicht mehr zukunftsorientiert. Der Nachfolger WPA2 ist aktuell die sicherste Verschlüsselungsart und sollte Ihre erste Wahl bei der Verschlüsselung der WLAN-Verbindung sein.

TIPP: Die richtige WLAN-Verschlüsselungsmethode auswählen

- Sie müssen Ihr WLAN immer verschlüsseln.
- Verwenden Sie, wenn möglich, immer eine WPA2-Verschlüsselung.
- Nur wenn Sie Geräte betreiben, die WPA2 noch nicht unterstützen, sollten Sie WPA nutzen.
- Beobachten Sie die Nachrichten in den Medien oder die aktuellen Informationen im Internet, um zeitnah reagieren zu können, sollte die WPA-Methode geknackt werden.

Die WLAN-Verschlüsselung einstellen

Haben Sie sich für eine Verschlüsselungsmethode entschieden, müssen Sie die WLAN-Verschlüsselung entsprechend konfigurieren. Zuerst benötigt das WLAN einen Namen. Dieser wird SSID genannt. Die SSID (Service Set Identifier), auch Netzwerkname genannt, bezeichnet die Kennung eines Funknetzwerks. Diese sollte keine Rückschlüsse auf den Betreiber zulassen, wenn es sich um ein privates WLAN handelt, damit ein potenzieller Angreifer nicht schon anhand des Namens sein Ziel erkennen kann. Die SSID kann durch eine Einstellung im WLAN-Router auch verborgen werden, was

die Sicherheit zusätzlich erhöht. Doch zurück zur Verschlüsselung: Jeder, der eine verschlüsselte WLAN-Verbindung nutzen möchte, benötigt einen Schlüssel, um seine Nutzungsberechtigung nachzuweisen. Schließlich sollen ja nur bestimmte Personen, zum Beispiel Familienangehörige oder Freunde, die einen besuchen, das WLAN verwenden können.

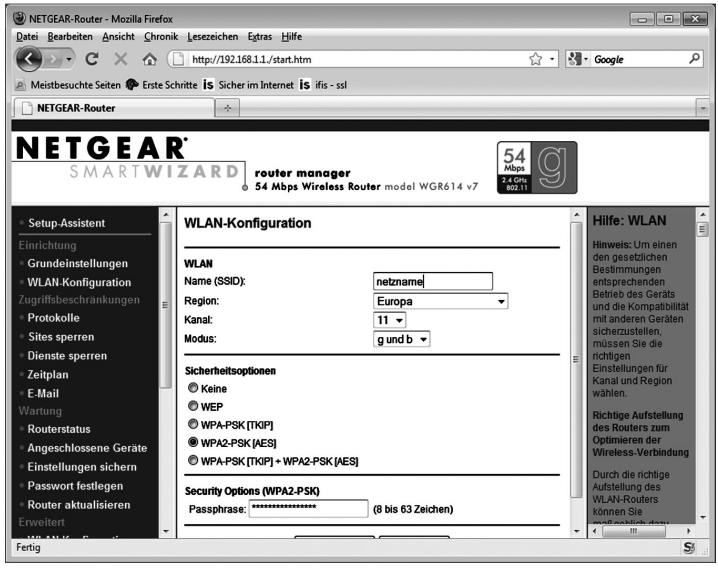


Abbildung 33: WLAN-Konfiguration des Routers – Sicherheitseinstellungen

Dazu stehen grundsätzlich zwei Verfahren zur Auswahl: PSK oder Radius. Radius ist ein Protokoll, das nur in Unternehmen genutzt wird, weshalb für Sie als Privatanwender nur der PSK infrage kommt. PSK steht für Pre-Shared Key. Dieser Schlüssel wird von demjenigen, der das WLAN konfiguriert, mithilfe einer sogenannten Passphrase erzeugt und an die Teilnehmer, die «Zutritt» zum WLAN erhalten sollen, weitergegeben. Die Passphrase besteht aus Buchstaben, Zahlen und

Sonderzeichen, die in das dafür vorgesehene Feld eingegeben werden (siehe Abbildung 33).

Soll nun ein Computer mit dem WLAN verbunden werden, fragt dieser nach der Passphrase. Zusätzlich kann bei der Konfiguration zwischen den Verschlüsselungsprotokollen TKIP (Temporal Key Integrity Protocol) und AES (Advanced Encryption Standard) gewählt werden. Das sind die Verschlüsselungsprotokolle, die in der jeweiligen Spezifikation festgelegt sind. Für WPA wird normalerweise das Protokoll TKIP und für WPA2 das Protokoll AES verwendet. In seltenen Fällen ist es auch möglich, WPA mit AES zu wählen.

Eine WLAN-Verschlüsselung einzurichten, ist mit den heutigen handelsüblichen Routern sehr einfach. Die Verschlüsselung findet zwischen einem sogenannten Access Point im Router und dem Computer statt. Bei neueren Computern, aber auch bei immer mehr Handys, ist WLAN bereits integriert. Ist dies bei Ihrem Computer nicht der Fall, benötigen Sie entweder eine WLAN-Karte oder even-

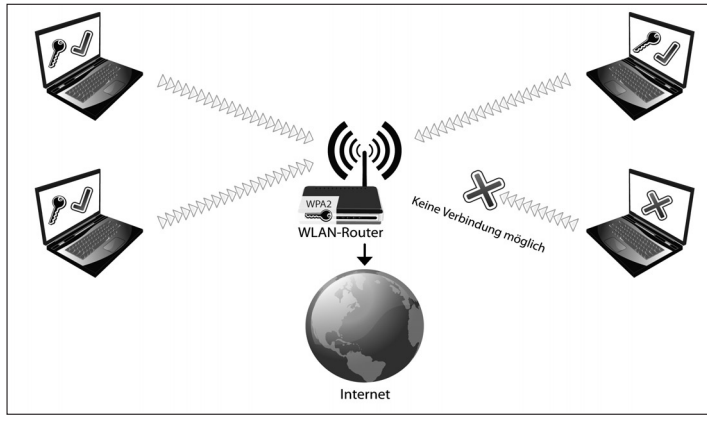


Abbildung 34: Aufbau eines WLANs mit Anbindung an das Internet über einen WLAN-Router

tuell einen WLAN-USB-Stick, um WLAN-Empfang zu erhalten.

Teilweise kann die Verschlüsselung auch ganz einfach per Knopfdruck vorgenommen werden. Der Schlüssel wird dann automatisch generiert. Grundsätzlich gilt: Wer die Passphrase (Schlüssel beziehungsweise Key) kennt, kann sich bei dem WLAN-Router anmelden. Daher muss die Passphrase wie ein Passwort aus großen und kleinen Buchstaben, Zahlen und Sonderzeichen bestehen und sollte mindestens 13 Stellen lang sein. Der Einsatz einer WPA2-Verschlüsselung mit der Passphrase «Sonne» bringt keinen Schutz, da die Passphrase sehr schnell durch automatisiertes Ausprobieren gefunden werden kann.

TIPP: Einstellen der WLAN-Verschlüsselung

- Nutzen Sie für WPA2 beziehungsweise WPA einen mehr als 13-stelligen Schlüssel mit Groß- und Kleinschreibung, Sonderzeichen und Zahlen.
- Verwahren Sie Ihren Schlüssel gut und geben Sie ihn nur an vertrauenswürdige Personen weiter, die Ihr Heimnetzwerk verwenden dürfen.

Verschlüsselung ist notwendig

«Aber wozu der ganze Aufwand?», werden Sie sich jetzt vielleicht fragen, schließlich haben Sie ja nichts zu verheimlichen. Doch auch, wenn es nichts zu verheimlichen gibt, bleibt die Tatsache bestehen, dass jeder x-beliebige Außenstehende ein unverschlüsseltes WLAN verwenden und im schlimmsten Fall für kriminelle Handlungen missbrauchen kann. Werden über das WLAN dann kinderpornographische Inhalte heruntergeladen oder Anleitungen zum Bombenbau ins Internet gestellt,

richtet sich die Fahndung zuerst gegen den Inhaber des WLANs. Der unbedarfte WLAN-Nutzer gerät so ins Fadenkreuz der Polizei. Auf die spannende rechtliche Seite der unterlassenen WLAN-Verschlüsselung geht das Kapitel «Ihre Rechte und Pflichten als Internetnutzer» (siehe Seite 162ff.) genauer ein.

TIPP: Unerlässlich: die Verschlüsselung
Auch wer nichts zu verheimlichen hat, muss seinen WLAN-Zugang schützen, um sicherzustellen, dass darüber keine kriminellen Handlungen erfolgen (siehe Seite 170ff.).

Zusätzliche Sicherheit durch den MAC-Adressenfilter

Ein zusätzlicher Schutz wird durch den MAC-Adressenfilter (MAC = Media Access Control) erreicht. Jedes Gerät, das eine WLAN-Funkverbindung aufbauen kann, hat eine eindeutige MAC-Adresse. Um andere daran zu hindern, sich in das eigene WLAN einzuklinken, kann im Router eine Liste der autorisierten MAC-Adressen eingerichtet werden, die Zugriff auf das WLAN bekommen sollen. Alle anderen WLAN-Geräte – mit MAC-Adressen, die nicht auf der Liste stehen – werden abgewiesen.

Um die MAC-Adressen der eigenen Geräte herauszufinden, sind verschiedene Wege denkbar. Der einfachste führt wieder über das Webinterface des Routers. Hier gibt es einen Menüpunkt «Angeschlossene Geräte», unter dem eine Liste mit allen aktuell verbundenen Geräten angezeigt wird. Nun sollten Sie alle Geräte, die eine Berechtigung erhalten sollen, mit dem WLAN verbinden, damit sie in der Liste auftauchen. Dann kopieren Sie die MAC-Adressen und fügen sie unter

dem Menüpunkt «Erweiterte WLAN-Konfiguration» in die Liste der «zugriffsberechtigten WLAN-Geräte» ein. Abschließend müssen Sie nur noch die Zugriffssteuerung unter dem gleichen Menüpunkt aktivieren. Danach haben nur noch die Geräte aus der Liste Zugriff auf das WLAN. Ein neues Gerät fügen Sie hinzu, indem Sie es ebenfalls in die Liste eintragen. Es gibt auch andere Möglichkeiten, die MAC-Adresse eines Geräts herauszufinden, und die Menüpunkte des Routers lauten je nach Router unterschiedlich. Weitere Informationen erhalten Sie im Workshop «MAC-Adressenfilter» unter Softlink 412.

TIPP: MAC-Adressenfilter

Nutzen Sie den MAC-Adressenfilter, um festzulegen, welche WLAN-Geräte Zugriff auf Ihr WLAN bekommen dürfen. Das erhöht die Sicherheit Ihres WLANs zusätzlich. Der MAC-Adressenfilter alleine bietet jedoch keinen ausreichenden Schutz.

Öffentliche WLANs (Hotspots)

WLAN in den eigenen vier Wänden macht Schluss mit Kabelchaos und schafft optimale Mobilität, aber so richtig interessant wird es erst unterwegs. Schnell am Bahnhof noch E-Mails abrufen oder gemütlich im Straßencafé surfen – das sind doch die echten Vorteile. Die WLANs an öffentlichen Plätzen werden als Hotspots bezeichnet. Sie werden zum Beispiel von der deutschen Telekom an Bahnhöfen und in einigen ICEs installiert und fallen unter deren Abrechnungssystem. Geschäfte oder Cafés stellen dagegen eine eigene Infrastruktur für den Zugang ins Internet zur Verfügung. Und bei beiden ist Vorsicht geboten, denn die Access Points werden

von Fremden betrieben und sind für jeden zugänglich. Nicht verschlüsselte Daten können «mitgeschnitten» werden, und selbst Angriffe auf verschlüsselte Daten sind theoretisch möglich, wenn ein Angreifer Zugriff auf den Access Point besitzt. Manche Angreifer stellen sogar extra eigene Access Points auf, die als «offizielle» Access Points getarnt sind.

TIPP: Vorsicht bei öffentlichen WLANs (Hotspots)
Geben Sie keine sicherheitskritischen Daten – zum Beispiel Ihre Kreditkartenummer – bei einer Internetanwendung ein, wenn Sie in einem öffentlichen WLAN surfen. Insbesondere Onlinebanking ist von öffentlichen WLANs aus tabu.

Bluetooth – der «Blauzahn»

Der für eine Technologie durchaus ungewöhnlich anmutende Name stammt von dem dänischen Wikingerkönig Harald Blauzahn, der im 10. Jahrhundert lebte und für seine Kommunikationsfähigkeit bekannt war. Und genauso kommunikativ gibt sich der heutige Blauzahn – vor allem bei kurzen Entfernungen (je nach Ausführung bis 100 Meter, wobei er eher für Entfernungen bis 10 Meter gedacht ist). Inzwischen kennt fast jeder die schnurlosen Bluetooth-Headsets für ein kabelfreies Telefonieren. Auch Handys lassen sich über Bluetooth mit dem Computer synchronisieren oder als Fernbedienung für elektronische Geräte verwenden.

Insgesamt gesehen ist Bluetooth eine prima Sache – solange Sie im Umgang damit einige Tipps beherzigen und die Hersteller bei der Umsetzung alles richtig machen. Denn es gab bereits einige Vorfälle, bei denen aufgrund falscher Imple-

mentierung, also einer fehlerhaften Umsetzung der Bluetooth-Spezifikation, Sicherheitslücken in Handys entstanden sind. Über die betroffenen Handys konnte mithilfe eines einfachen Angriffs eine SMS verschickt oder das Telefonbuch ausgelesen werden. Ist das schlimm? Wenn der Angreifer vor jede Nummer im Telefonbuch eine Mehrwertnummer (0900) für 3,50 Euro setzt und es wieder in das Handy hochlädt, schon.

Der richtige Umgang mit Bluetooth – So schützen Sie sich

Allerdings ist der Nutzer solchen Angriffen nicht hilflos ausgeliefert, weil es einfache Gegenmaßnahmen gibt. Bevor der Angreifer versuchen kann, ein Telefonbuch aus einem Handy herunterzuladen, muss er das Telefon technisch «sehen» können. Das bedeutet, er muss die eindeutige Kennung (MAC-Adresse) des Bluetoothgeräts herausbekommen. Zwar kann die Umgebung mit einem bluetoothfähigen Notebook oder Handy relativ einfach nach aktiven Bluetoothgeräten «gescannt» werden, fündig wird der Suchende aber nur, wenn sich das Bluetoothgerät im sogenannten Sichtbarkeitsmodus befindet. Diesen Modus benötigen Bluetoothgeräte jedoch ausschließlich, wenn sie sich das erste Mal verbinden (auch Pairing genannt), also beispielsweise das Handy mit dem Notebook oder das Handy mit dem Headset. In diesem Moment geben die Geräte der unmittelbaren Umgebung ihre eindeutige Kennung öffentlich preis, damit sie sich gegenseitig finden können. Werden Bluetoothgeräte zum ersten Mal verbunden (gepairt), wird zur Absicherung eine PIN ausgetauscht, die in beide Geräte eingegeben werden muss. Diese PIN kann bis zu 16 Stellen lang sein – und die sollten auch

genutzt werden. Denn es gilt: Je mehr Stellen, desto sicherer ist die Verbindung. Danach kann das Bluetoothgerät sofort zurück in den «Unsichtbarkeitsmodus» gestellt werden und ist damit nicht mehr für alle sichtbar. Waren zwei Geräte einmal verbunden, müssen sie für eine erneute Verbindung eigentlich nicht mehr gepairt werden; bei manchen günstigen Geräten kann das automatische erneute Verbinden allerdings manchmal Probleme bereiten.

Im Sichtbarkeitsmodus wird außerdem der Name des Bluetoothgeräts übertragen. Handys tragen als Namen im Allgemeinen ihre Typenbezeichnung, solange der Nutzer ihn nicht ändert. Ist Bluetooth «sichtbar» geschaltet, kann der Name ausgelesen werden, und der Angreifer sieht anhand der Typenbezeichnung sofort, ob ein Gerät dabei ist, das angreifbar ist. Das gilt natürlich genauso für Geräte, deren Name identisch mit dem Namen des Eigentümers ist. Der beste Name für ein Bluetoothgerät ist daher eine für einen Fremden völlig zusammenhangslose Zeichenfolge.

Wie bei allen Kommunikationstechnologien gilt auch hier das Credo: Schalten Sie Bluetooth vollständig ab, wenn Sie es nicht verwenden. Das spart obendrein Strom und verlängert somit die Akkulaufzeit.

TIPP: Der richtige Umgang mit Bluetooth

- Schalten Sie Bluetooth immer auf «unsichtbar». Nur für die erste Verbindung mit einem anderen Gerät muss das Bluetoothgerät «sichtbar» sein. Aktuelle Geräte schalten sich deshalb automatisch nach kurzer Zeit wieder auf «unsichtbar».
- Ändern Sie die voreingestellte Typenbezeichnung eines Bluetoothgeräts auf einen unscheinbaren, auf den ersten Blick nichtssagenden Namen – aber nicht auf den eigenen.

- Deaktivieren Sie die Bluetoothfunktion, wenn Sie diese nicht benutzen.

Das Bluetooth-Headset – Vorsicht Wanze

Ein wichtiges Gespräch mit dem Chef steht an, in dem Dinge besprochen werden, die nicht unbedingt für die Öffentlichkeit bestimmt sind. Natürlich wird das Handy in solchen Fällen ausgeschaltet. Wenn aber das Bluetooth-Headset neben dem Handy liegt und noch angeschaltet ist, wird es mit der Geheimhaltung eventuell schwierig. Das Headset findet «sein» Handy, mit dem es eine verschlüsselte Verbindung hatte, jetzt nicht mehr und verfällt in einen Modus, in dem es nach einem Gegenstück sucht. In diesem Moment ist es dem Angreifer möglich, sich mit dem Headset zu verbinden und es abzuhören, es also als Wanze zu benutzen. Sehr unschön bei einem geheimen Meeting. In diesem speziellen Fall, in dem es kein Tastenfeld an dem Gerät gibt, verwenden die Hersteller eine voreingestellte Standard-PIN der Art 0000, 1111 oder 1234. Der Angreifer muss lediglich diese Kombinationen ausprobieren und die Kennung (MAC-Adresse) des Headsets wissen, um sich zu verbinden. Die Hersteller könnten jedem Headset eine eigene PIN geben und vielleicht auf das Headset schreiben, aber diese Maßnahmen sind einerseits wohl zu teuer und andererseits ist der Nutzer zu bequem, um diese Absicherung zu nutzen. Der Schutz gegen den dargestellten Lauschangriff ist einfach:

TIPP: Bluetooth-Headsets

Schalten Sie Ihr Headset immer dann aus, wenn Sie auch Ihr Handy ausschalten. Solange das Handy oder ein Computer mit

dem Headset verbunden ist, kann ein Angreifer die Verbindung nicht abhören.

UMTS – State of the Art beim mobilen Internet

«Überall-Internet» ist die Parole für die Zukunft. Egal, wo sich ein Nutzer befindet, soll er Zugang zum Internet bekommen. Dafür extra eine Kabelverbindung oder ein WLAN zu suchen, ist unpraktisch. UMTS (Universal Mobile Telecommunications System) ist ein Mobilfunkstandard der dritten Generation (3G), der das Internet auf das Handy oder auch ins Wohnzimmer bringt. Im Grunde handelt es sich dabei um den Nachfolger von GSM, dem Standard, mit dem auch heute noch die meisten Handys funken.

Entscheidend bei UMTS ist die höhere Übertragungsrate und damit die Datengeschwindigkeit. Durch UMTS werden Geschwindigkeiten vergleichbar mit denen von DSL erreicht – aktuell bis zu 7,2 (10,2) Mbit/s. Die Datenübertragung von UMTS ist zwischen dem Handy und der Basisstation auf dem physikalischen Übertragungsweg gut verschlüsselt, weshalb die Nutzung von UMTS auch für sicherheitsrelevante Daten möglich ist. Natürlich muss auf der Anwendungsebene trotzdem eine SSL/TLS-Verschlüsselung (siehe Seite 36 ff.) verwendet werden, da die Daten nach der Basisstation im Klartext über das Kommunikationsnetz und ins Internet übertragen werden.

UMTS findet nicht nur in Handys Anwendung, sondern oft auch in Notebooks. Für den UMTS-Empfang wird eine SIM-Karte – wie sie auch für Mobiltelefone üblich ist – von einem Mobilfunkanbieter benötigt, der diesen Standard be-

reitstellt. Die Angebote reichen dabei von Zeit- und Volumentarifen bis hin zu Flatrates.

TIPP: UMTS und Sicherheit

UMTS ist mit einer guten Verschlüsselung ausgestattet. Es kann daher auch für sicherheitskritische Vorgänge wie Einkäufe im Internet verwendet werden. Natürlich muss auf Anwenderebene weiterhin eine SSL/TLS-Verschlüsselung verwendet werden (siehe Seite 36ff.).

Ihre Rechte und Pflichten als Internetnutzer – der aktuelle Stand

Sie sind ein guter Bürger? Sie zahlen pünktlich Ihre Steuern und halten sich an die Gesetze? Das ist gut – aber tun Sie das auch im Internet? Die Einschätzung von Recht und Unrecht im Internet ist keine leichte Aufgabe. Dafür gibt es sehr viele Gründe.

Erstens stimmt der Spruch: «Wenn du zwei Anwälte um eine rechtliche Einschätzung bittest, dann bekommst du drei verschiedene Antworten.» Dazu kommt, dass viele unterschiedliche Rechtsgebiete im Internet eine Rolle spielen (Zivilrecht, Urheberrecht, Wettbewerbsrecht, Strafrecht, Datenschutzrecht, Medienrecht, Markenrecht, Telekommunikationsrecht …) und diese sich aufgrund der ständig neuen Anforderungen kontinuierlich verändern.

Zweitens ist die Dezentralität des Internets ein Problem, das heißt, es gibt keine zentrale Instanz, die für alles die Verantwortung trägt beziehungsweise zuständig ist. Das Internet ist ein Verbundnetz aus vielen eigenständigen Organisationen, die alle unterschiedliche Strategien und Ziele verfolgen (Softlink 505). Viele Dinge passieren heute über temporäre Kommunikationsverbindungen (Peer-to-Peer) direkt zwischen den Computern, ohne dass jemand Buch darüber führt und verantwortlich gemacht werden kann.

Drittens ist die Internationalität des Internets eine enorme Herausforderung. Das Internet hat einen hohen globalen

Aktionsradius, aber in jedem Land/Staatenverbund gelten andere Gesetze, die oftmals auf unterschiedlichen Rechtsgrundlagen beruhen. Da sich nicht immer sofort feststellen lässt, welcher Dienst von welchem Land aus angeboten wird, ist die rechtliche Einschätzung häufig schwierig – besonders für den Durchschnittsnutzer. Auch die Tatsache, dass das E-Commerce-Recht innerhalb der Europäischen Union immer mehr angeglichen wird, führt zu ständigen Veränderungen.

Das Internet sorgt zudem für eine starke Abstraktion zwischen Handlung und Wirkung – anders als in der realen Welt, in der die Wirkung einer Handlung unmittelbar wahrgenommen werden kann. Das verlangt einen wesentlich bewussteren Umgang mit den Möglichkeiten des Internets, die jedoch noch nicht jeder kennt. Es ist aber festzustellen, dass das Unrechtsbewusstsein im Internet schwächer ausgeprägt ist als im realen Leben. Das unrechtmäßige Kopieren und Nutzen eines Programms zum Beispiel wird eher als Kavaliersdelikt wahrgenommen denn als Straftat. Deshalb soll durch stärkere Aufklärung und den Aufbau einer Internetkultur ein klares Bewusstsein für die Schäden geschaffen werden, die einige Delikte verursachen.

Der Rechtsrahmen im Internet – Der Klügere denkt nach

Da sich die Gesetzgebung aufgrund der immer neuen Entwicklungen ständig erweitert und verändert, kann in diesem Buch nur ein rechtlicher Rahmen abgesteckt werden. Sie erhalten einen grundsätzlichen Leitfaden sowie einige Tipps an die Hand, die Ihnen einen rechtskonformen Umgang mit

dem Internet ermöglichen. In konkreten Einzelfällen sollten Sie jedoch einen Juristen befragt, der auf dieses Rechtsgebiet spezialisiert ist.

Die informationelle Selbstbestimmung

Das Recht auf informationelle Selbstbestimmung ist das Recht des Bürgers, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen.

Daten sind personenbezogen, wenn sie eindeutig einer bestimmten natürlichen Person zugeordnet sind oder diese Zuordnung zumindest mittelbar erfolgen kann.

Das informationelle Selbstbestimmungsrecht ist eine Ausprägung des allgemeinen Persönlichkeitsrechts und wurde vom Bundesverfassungsgericht im sogenannten Volkszählungsurteil vom 15. Dezember 1983 als Grundrecht anerkannt. Das informationelle Selbstbestimmungsrecht ist die Grundlage für das Bundesdatenschutzgesetz sowie die Landesdatenschutzgesetze und in einer Reihe von spezifischen Gesetzen geregelt.

Datenschutz steht für die Idee, dass jeder Mensch grundsätzlich selbst entscheiden kann, wem und in welchem Umfang seine persönlichen Daten zugänglich sein sollen. Der Datenschutz will den gläsernen Menschen verhindern!

Die Bedeutung des Datenschutzes wird in der vernetzten Informations- und Wissensgesellschaft immer wichtiger. Durch das Internet werden zunehmend mehr personenbezogene Daten erzeugt, verarbeitet, weitergegeben und gespeichert. Sowohl private Unternehmen als auch staatliche Stellen haben Interesse an den personenbezogenen Daten. Private

Unternehmen wollen damit zum Beispiel Waren versenden, Rechnungen erstellen und Kundenprofile generieren, die es ihnen ermöglichen, ein effektives Marketing zu entwickeln, Preise zu optimieren und die Zahlungsfähigkeit der Kunden besser einzuschätzen. Die staatlichen Stellen wollen in erster Line die Verbrechensbekämpfung verbessern.

Datenschutzgesetze

Der Zweck des Bundesdatenschutzgesetzes ist, den Einzelnen davor zu schützen, dass er durch den Missbrauch seiner personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird.

Das Bundesdatenschutzgesetz regelt den Datenschutz für die Bundesbehörden und den privaten Bereich, zum Beispiel wenn Wirtschaftsunternehmen und Privatpersonen personenbezogene Daten verwenden.

Der Bundesdatenschutzbeauftragte sowie die Landesdatenschutzbeauftragten geben eine Menge wertvoller Tipps zum Thema Datenschutz und dazu, wie Sie Ihre Daten schützen, beziehungsweise ihre Rechte durchsetzen können (Softlink 501).

Das Urheberrecht

Das Urheberrecht bezeichnet das Recht, das die ideellen und materiellen Interessen des Urhebers an seinem Geisteswerk schützt. Geisteswerke im Internet oder Medien sind zum Beispiel Filme, Musikstücke, Bücher oder Computerprogramme.

Eine Urheberrechtsverletzung im Internet ist strafbar – genau wie in der realen Welt. Gegen das Urheberrecht wird

häufig verstoßen, indem Kopien von urheberrechtlich geschützten Medien rechtswidrig hergestellt oder verbreitet werden.

Diese werden von der Unterhaltungs- und Softwareindustrie häufig als Raubkopien bezeichnet. Das Problem bei der Urheberrechtsverletzung ist, dass die normalerweise beim Kauf einer legalen Kopie erfolgende Bezahlung des Urhebers oder des Rechteinhabers nicht stattfindet. Verstöße gegen das Urheberrecht sind im Internet sehr stark verbreitet.

Das Erstellen von Privatkopien

Jede Person darf nach dem Gesetz von rechtmäßig erworbenen Inhalten (Musik, Filmen etc.) eine Kopie erstellen. Dabei dürfen aber keine wirksamen technischen Schutzmaßnahmen umgangen werden. Die Kopie kann zum Beispiel die Erstellung eines persönlichen Best-of-Albums von gekauften Original-CDs sein. Dieses Best-of-Album darf auch von Freunden und der Familie genutzt werden. Die Weitergabe an Fremde und das öffentliche Abspielen sind hingegen untersagt. Erst recht, wenn dafür eine finanzielle Gegenleistung verlangt wird.

Das Mitschneiden von Onlinestreams

Das Mitschneiden von Onlinestreams aus «legalen» Quellen, das heißt das Abspielen von Bild und Ton direkt aus dem Internet (Webradio, Internetfernsehen, YouTube usw.), ist erlaubt. YouTube beispielsweise hat mit den wichtigsten Firmen, die Inhalte wie Musik und Filme herstellen, ein Lizenzabkommen geschlossen.

Um die Onlinestreams mitschneiden zu können, bietet der Markt eine Vielzahl von sehr einfachen und komfortablen Softwareprogrammen beziehungsweise Zusatzfunktionen für Browser an.

Legale Webportale

Es gibt natürlich auch viele Künstler und Vermarktungsorganisationen, die ihre Werke im Internet frei und völlig rechtmäßig anbieten. Jamendo zum Beispiel ist eine Internetplattform für freie Musik (Softlink 502). Musiker können dort ihre Lieder unter einer der Creative-Commons-Lizenzen (siehe Seite 93 f. sowie Softlink 503) veröffentlichen. Jeder Nutzer kann diese Musik kostenlos und legal herunterladen. Die Musiker erhoffen sich so eine höhere Popularität.

Die Nutzung von anonymen Tauschbörsen

Das Herunterladen von illegaler Musik und Filmen aus Tauschbörsen, bei denen nicht festgestellt werden kann, wo die Inhalte herkommen, ist in der Regel verboten. Und eigentlich sollte jedem klar sein, dass die neusten Kinofilme und die aktuellen Top-Ten-Alben nicht kostenlos im Internet zur Verfügung gestellt werden. Das gilt nicht nur für Tauschbörsen, sondern auch für andere Webseiten, die diese Inhalte anbieten.

Einigen Nutzern scheint zudem nicht bewusst zu sein, dass manche Tauschbörsen beim Herunterladen von Inhalten gleichzeitig die eigenen Inhalte (Musik und Filme auf dem eigenen Computer) anderen Nutzern anbieten. Hier haben schon viele unbedarfte Nutzer plötzlich eine Abmahnung für

das illegale Verbreiten von Inhalten erhalten, obwohl sie «nur etwas heruntergeladen haben». Und dieses Vergehen wird schwer bestraft!

TIPP: Die Fahndung im Internet

Da die Internetprovider alle Aktivitäten loggen (speichern) müssen und auch die Webseiten- und Maildienstanbieter Aktivitäten über Logdateien festhalten, können unbedarfte Beteiligte im Verdachtsfall sehr schnell durch die Strafverfolgungsbehörden ermittelt werden. Der verwendete Computer, der illegal Inhalte heruntergeladen oder verbreitet hat, kann über die verwendete IP-Adresse und die geloggten Aktivitäten der Internetprovider identifiziert werden. Das ist auch der Grund, warum es so viele Verfahren wegen Urheberrechtsverletzungen gibt.

Das Hochladen von Inhalten auf Webseiten

Internetnutzer dürfen nur Inhalte (zum Beispiel Texte, Bilder, Musik und Videos) auf die eigenen Webseiten laden, wenn sie die Rechte dafür besitzen, beziehungsweise die Inhalte selbst erstellt haben.

Fotos, Videos usw., auf denen Dritte, wie Freunde, Kollegen oder Nachbarn, gezeigt werden, dürfen nur mit vorheriger Zustimmung der entsprechenden Personen verwendet werden. Ohne Einverständnis der gezeigten Person ist diese Vorgehensweise strafbar! Jeder, der ein Bild von sich im Internet findet oder von Bekannten erfährt, dass eines im privaten oder öffentlichen Bereich eines sozialen Netzwerks eingestellt ist, kann rechtlich dagegen vorgehen. In der Praxis ist es allerdings nicht so einfach, diese Inhalte aus dem Internet zu verbannen, da teilweise Kopien von Webseiten angelegt werden

(siehe Seite 96) oder aufgrund anderer Mechanismen die Inhalte mehrfach vorliegen. Daher kommt auch der Spruch: «Das Internet vergisst nie.» Es ist also klüger, private Fotos von anderen erst gar nicht in das Internet zu stellen.

Grundsätzlich sollten Sie bei privaten Fotos sicherstellen, dass nur Freunde oder Verwandte über das Internet auf diese zugreifen können. Das kann in sozialen Netzwerkseiten auf zwei Arten geschehen.

Entweder legen Sie in den Einstellungen fest, dass nur eine bestimmte Gruppe auf die Dateien zugreifen darf, oder Sie vergeben ein Passwort für den Zugriff, das nur eine definierte Gruppe von Personen kennt. Das ist wie im realen Leben. Fotos von Freunden und Verwandten zeigt auch niemand wildfremden Leuten. Außerdem sollten im Internet keine kompromittierenden Fotos zur Schau gestellt werden, denn im Prinzip kann jeder diese ungeschützten Fotos sehen, der im Internet surft und zufällig nach einem Begriff sucht, der im Namen des Fotos enthalten ist. Besonders wichtig ist dieser Aspekt für Bewerber. Es ist nämlich inzwischen gang und gäbe, dass diese von den Personalverantwortlichen «gegoogelt» werden.

Das Vorbereiten des Ausspähens und Abfangens von Daten (Hackerparagraph)

Wer eine Straftat vorbereitet, indem er Passwörter oder sonstige Sicherungscodes, die den Zugang zu Daten ermöglichen, oder Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich oder einem anderen verschafft, verkauft, einem anderen überlässt, verbreitet oder sonst zugänglich macht, macht sich strafbar.

Virtueller Hausfriedensbruch

Das unbefugte Eindringen in fremde Computer (der «virtuelle Hausfriedensbruch»), das Ausspähen, Löschen oder Austauschen von Dateien ist nach § 202a StGB strafbar. Das gilt auch, wenn ein geschütztes fremdes WLAN geknackt und anschließend auf fremde Kosten im Internet gesurft wird oder Daten manipuliert werden. Ist der Computer oder das WLAN nicht gesichert, ist das «unerwünschte» Eindringen keine Straftat. Sichern Sie also stets Computer und WLAN!

TIPP: Rechtliche Belange im Internet

- Laden Sie nur Daten aus dem Internet herunter, wenn Sie eindeutig feststellen können, dass die angebotenen Inhalte bezahlt werden oder dass der Anbieter die Rechte hat, diese für den Download freizugeben (Jamendo …).
- Stellen Sie nur Bilder, Videos und Texte ins Internet, bei denen die Rechte und Lizenzen dies zulassen – weil Sie diese gekauft oder die Inhalte selbst erstellt haben.
- Wollen Sie Inhalte veröffentlichen, bei denen Personen identifizierbar sind, benötigen Sie die Zustimmung der Betroffenen. Stellen Sie diese Inhalte nur einem geschlossenen Kreis zur Verfügung, zum Beispiel Freunden und Verwandten.

Die Verbraucherpflichten – Das fordert der Gesetzgeber von Ihnen

Im Folgenden werden einige Pflichten aufgezeigt, die der Internetnutzer von Rechts wegen erfüllen muss und die zum Gemeinwohl beitragen.

Den eigenen WLAN-Zugang sichern

Jeder, der einen WLAN-Zugang für seinen Internetanschluss hat, muss dafür sorgen, dass die Kommunikation zwischen dem WLAN-Router und dem angeschlossenen Computer im verschlüsselten Modus abläuft. Denn wer sein WLAN unverschlüsselt lässt, ermöglicht es Fremden, darüber ins Internet zu gelangen und anonym Straftaten zu begehen. Der WLAN-Besitzer muss dann damit rechnen, dass er für die begangenen Straftaten verantwortlich gemacht wird.

So hat das Oberlandesgericht Düsseldorf beispielsweise einen Rentner wegen einer Urheberrechtsverletzung verurteilt, weil er sein WLAN nicht gesichert hatte. Hintergrund dieses Urteils ist, dass die Richter der Meinung sind, dass der verschlüsselte WLAN-Zugang eine zumutbare Sicherungsmaßnahme darstellt. Der Rentner hat durch den offenen WLAN-Zugang Dritten ermöglicht, sich hinter seiner Person zu verstecken und im Schutze der von ihm geschaffenen Anonymität eine Urheberrechtsverletzung zu begehen.

Den eigenen Computer absichern

Auch muss jeder Besitzer dafür sorgen, dass sein Computer mit Anti-Malware-Produkten und einer Personal Firewall ausgerüstet ist und diese Software regelmäßig aktualisiert wird. Entspricht Ihr Computer diesen Anforderungen nicht, verletzen Sie Ihre Sorgfaltspflicht. Das ist insbesondere bei der Haftungsfrage von Bedeutung. Es gibt Urteile, bei denen die Bank für eine Phishing-Attacke haften musste, weil der Kunde nachweisen konnte, dass er für einen ausreichenden Basisschutz gesorgt hatte. Umgekehrt ist es sehr wahrscheinlich,

dass ein Richter eine Mitschuld sieht, wenn jemand den Basisschutz nicht umgesetzt hat.

Verantwortung für die Kinder

Natürlich haben Eltern auch bei der Nutzung des Internets eine Aufsichtspflicht für ihre Kinder. Aus diesem Grund sollten sich Eltern genau überlegen, was ihre Kinder im Internet tun dürfen und welche Internetkompetenz sie dafür brauchen. Eltern müssen mit ihren Kindern über die Gefahren sprechen, damit diese sich richtig verhalten können (siehe Seite 135 ff.).

Verbotene Inhalte im Internet

Entdeckt jemand zufällig verbotene Inhalte im Internet, sollte er diese bei der Internet-Beschwerdestelle melden (www.internet-beschwerdestelle.de).

Aufgabe der Internet-Beschwerdestelle ist es, die Anwender vor Sicherheitsproblemen und Kriminalität im Internet zu schützen. Außerdem soll die Stelle zu einem bewussten Umgang mit der Informationstechnologie motivieren und das Vertrauen in neue Technologien stärken. Oftmals fehlt es für eine Strafverfolgung an Hinweisen auf die Fundstellen illegaler Inhalte.

Die Internet-Beschwerdestelle arbeitet mit Strafverfolgungsbehörden, den Serviceprovidern und weltweiten Partnern zusammen, damit kriminelle Inhalte aus dem Netz verschwinden und Täter identifiziert werden können. Jeder kann mithelfen, damit das Internet sicherer und sauberer wird.

TIPP: Pflichten des Internetnutzers

- Sorgen Sie stets für einen ausreichenden Basisschutz (siehe Seite 10ff.), um zu verhindern, dass Dritte Ihren Computer missbrauchen.
- Sichern Sie Ihr WLAN (siehe Seite 149ff.).
- Melden Sie strafbare Inhalte der Internet-Beschwerdestelle oder der Polizei.
- Erfüllen Sie Ihre Aufsichtspflicht als Eltern gegenüber Ihren Kindern auch bei der Internetnutzung.

Die in diesem Kapitel angegebenen Gesetze beziehen sich auf das deutsche Recht. Quellen mit vertiefenden Informationen über Rechte und Pflichten des Internetnutzers in Deutschland, Österreich und der Schweiz finden Sie unter Softlink 504.

Dringend nötig: die Schaffung einer Internet-Sicherheitskultur

Eine Internet-Sicherheitskultur ist deshalb spannend, weil sie sich auf ein globales Feld bezieht. Zur Internet-Sicherheitskultur gehört die Übertragung der gewohnten realen (Sicherheits-)Kultur auf das digitale Leben. Dazu zählt nicht nur das Verständnis für Sicherheit und Vertrauenswürdigkeit im Internet, sondern auch das Wissen darüber, wie Probleme gemeistert werden können, und die Einsicht, dass Hilfestellungen von Fachleuten auch im digitalen Leben nicht kostenlos zu haben sind.

Vom realen zum digitalen Leben – Sicherheit und Vertrauenswürdigkeit im Internet

Wie viel Sicherheit ist im Internet generell erreichbar? Wo ist wie viel Sicherheit angemessen? Wie kann Vertrauen in das Internet gestärkt werden? Dem Sicherheitsbedürfnis entsprechend besteht das Ziel darin, vor dem Surfen im Internet alle denkbaren negativen Folgen auszuschließen. Doch das Surfen ist immer mit einem Risiko verbunden, da das Internet neben vielen Vorteilen eben auch Gefahren birgt. Genau genommen gilt das aber für alle Aktivitäten im Leben. Die meisten Alltagshandlungen, zum Beispiel das Autofahren, würde niemand als besonders riskant bezeichnen, auch wenn man nie völlig

sicher sein kann, dass sie im Sinne des Handlungsziels gelingen – so sterben beispielsweise jedes Jahr mehrere Tausend Menschen im Straßenverkehr.

Analog ist das Buchen von Flügen im Internet eine sehr einfache und sinnvolle Sache. Es besteht aber die Gefahr, dass dabei Kriminelle ihre Finger mit im Spiel haben, die dafür sorgen, dass der Nutzer zwar den Flugpreis bezahlt, aber kein Ticket erhält. Wenn jemand Internetdienste nutzt, tut er das, ohne genau zu wissen, was letztlich dabei herauskommt.

Von einem Risiko spricht man, wenn etwas aufs Spiel gesetzt wird. Dabei sollte bedacht werden, welche Auswirkungen bestimmte Handlungen haben können, welche Faktoren auf ihren Ausgang Einfluss nehmen und welche möglichen Resultate erreicht werden können. Im Alltag werden diese Aspekte zumeist intuitiv beurteilt, so auch beim Autofahren: Der potenzielle Schaden beim Autofahren ist kein Risiko, das davon abhält, das Auto zu nutzen.

Wie sieht der Alltag aus?

Eine sichere Welt gibt es nicht! Aber der moderne Mensch hat gelernt, mit dieser Tatsache verantwortungsvoll umzugehen und sich mithilfe geeigneter Mittel ein Mindestmaß an Sicherheit zu schaffen. Was also ist nötig, um das auch im digitalen Leben zu erreichen?

In einer idealen Welt würden Vertrauen und Freundlichkeit regieren, wären alle Informationen frei für jeden verfügbar, würde sich niemand zulasten anderer bereichern, würden alle den gewünschten und angemessenen Preis für Waren und Dienstleistungen zahlen, wäre der Wettbewerb transparent, fair und ausgeglichen. Doch das reale Leben sieht anders aus:

Information und Wissen – und damit Macht – sind ungleich verteilt, Einbruch und Diebstahl gefährden das private Eigentum, Betrug und Verrat gehören zum Leben, Terror und Gewalt bedrohen den Alltag. Dennoch haben wir gelernt, mit diesen Gefahren zu leben und umzugehen und uns, so weit es möglich ist, zu schützen.

Welchen Schutz gibt es im realen Leben?

Die Wohnung wird abgeschlossen, sodass kein Unbefugter sie betreten und das private Eigentum stehlen kann. Verschlossene Schränke und Safes dienen zur sicheren Aufbewahrung wertvoller Güter (Geld, Sachwerte usw.). Der geschlossene Kofferraum des Autos schützt die eingekauften Waren während des Transports, sodass kein Dieb sie während eines Stopps entwenden kann. Verschlossene Briefumschläge sorgen für den vertraulichen Austausch von Informationen, die eigenhändige Unterschrift für Verbindlichkeit, zum Beispiel bei Kaufverträgen.

Reales versus digitales Leben

Ein besonders wichtiger Punkt in einer funktionierenden Gesellschaft ist die Vertrauenswürdigkeit – in der Geschäftswelt wie im alltäglichen Umgang miteinander.

Im realen Leben lernt jeder, welche Bedeutung eine Unterschrift unter einem Vertrag hat und wie er anhand äußerer Merkmale und mithilfe intuitiver Einschätzung die Vertrauenswürdigkeit seines Gegenübers im täglichen Leben bewerten kann, um mehr Sicherheit zu erlangen. Im digitalen Leben, zum Beispiel bei der indirekten Kommunikation über

das Internet, ist es jedoch nicht möglich, auf diese bewährten Mechanismen zurückzugreifen. Man kann nicht sicher sein, mit wem man tatsächlich kommuniziert und ob die Kommunikation nicht abgehört oder manipuliert wird.

Das heißt, dass die grundlegenden Sicherheitsbedürfnisse im digitalen Leben anders als im realen Leben befriedigt werden müssen.

Welche Herausforderungen stellt das digitale Leben?

In einer vernetzten Informations- und Wissensgesellschaft spielt die IT-Sicherheit und Vertrauenswürdigkeit eine immer bedeutendere Rolle. Die Werte, die als Bits und Bytes auf unseren Computern und im Internet zur Verfügung stehen, und die Abhängigkeit von den angebotenen IT-Dienstleistungen werden immer größer.

Ebenso wächst aufgrund immer leistungsfähigerer Software und immer komplexerer Zusammenhänge zwischen Protokollen, Diensten und Infrastrukturen die Angriffsfläche beständig. Daher verwundert es nicht, dass auch die Angriffe immer raffinierter, differenzierter und routinierter erfolgen; die IT-Kriminalität erfährt eine zunehmende Professionalisierung und wird damit zu einer nicht zu unterschätzenden Gefahr. Damit nimmt auch die Notwendigkeit zu, IT-Sicherheitsmaßnahmen in angemessener Weise anzuwenden. Nur so kann im digitalen Leben eine Vertrauensbasis geschaffen werden.

Eine weitere Herausforderung ist das häufig mangelnde Unrechtsbewusstsein im digitalen Leben. Wer im realen Leben Gegenstände entwenden will, der muss über Zäune klettern, Türen und Fenster aufbrechen, vielleicht sogar Tresore spren-

gen. Jedem, der so etwas tut, ist bewusst, dass er eine Straftat begeht! Im digitalen Leben sitzen die Hacker beziehungsweise Cracker mit Kaffee und Keksen vor dem Bildschirm und machen das Gleiche, aber sie haben dabei häufig nicht das Gefühl, etwas Unrechtes zu tun. Die Hemmschwelle ist niedriger, wodurch die Wahrscheinlichkeit von Angriffen im Internet steigt. Aber das muss sich durch eine Sicherheitskultur im Internet grundlegend ändern.

Ein ganz wesentlicher Unterschied zum realen Leben besteht darin, dass das Internet global ist, während die Gesetze in ihrer Wirkung derzeit meist noch national oder europaweit begrenzt sind. Das heißt, der Staat kann zurzeit keinen angemessenen rechtlichen Schutz bieten, obwohl das dringend nötig wäre.

Welcher Schutz ist im digitalen Leben angemessen?

Die genannten Sicherheitsmechanismen aus dem realen Leben (siehe Seite 176) sind analog auch im digitalen Leben verfügbar:

Anti-Malware-Programme und Personal Firewalls – als Haus- und Wohnungstür – verhindern den unerlaubten Zugriff von außen auf die Daten im Computer. Datei- und Festplattenverschlüsselung sorgen als digitaler Tresor für eine sichere Aufbewahrung der elektronischen Informationen, während eine Kommunikationsverschlüsselung wie SSL/TLS die Daten während des Transports im Internet schützt. Darüber hinaus ermöglichen verschlüsselte E-Mails einen vertraulichen «Briefverkehr», und digitale Signaturen gewährleisten die Verbindlichkeit und damit eine höhere Rechtssicherheit. Wer die Vorteile des digitalen Lebens ausschöpfen will, muss,

ähnlich wie im realen Leben, das Risiko begrenzen. Das heißt, geeignete Sicherheitslösungen müssen eingesetzt und regelmäßig aktualisiert und angepasst werden.

Ein Blick in die Zukunft

Egal ob Handys, Computer, Spielzeug, Videogeräte oder Autos, das Leben wird immer digitaler. Dabei stellen die vielen Möglichkeiten, die das Internet heute schon bietet, gerade mal den Anfang der digitalen Revolution dar. Vermutlich werden schon in naher Zukunft die Tische in Cafés zu Touchscreen-Monitoren, welche die Speisekarte anzeigen, Bestellungen aufnehmen und es dem Nutzer ermöglichen, während des Essens und Trinkens im Internet zu surfen oder Fotos anzuschauen. In zehn Jahren wird es billiger sein, eine Wand als Monitor einzurichten, als eine Holzvertäfelung anfertigen zu lassen. Das «Internet der Dinge» wird Teile des Haushalts, wie zum Beispiel den Kühlschrank, die Heizung und die Jalousien, digital steuern. Wenn ein heutiger Computer die Intelligenz einer Fliege hat, dann werden die Computer in zehn Jahren die Intelligenz eines Menschen aufweisen. Intelligente Softwareagenten übernehmen Arbeiten wie das Beantworten von E-Mails, das Buchen von Reisen, das Einkaufen von Lebensmitteln und das Führen von Bankkonten.

Doch egal, was die Zukunft auch bringen wird, stets müssen das Recht auf die Privatsphäre und der Schutz des wirtschaftlichen Gutes gewährleistet sein. Dazu muss der Internetnutzer das digitale Leben als natürlichen Teil seiner Lebenswirklichkeit wahrnehmen und für die digitale und reale Welt die äquivalente Verantwortung übernehmen – eine Sicherheitskultur entwickeln und etablieren.

Hilfe zur Selbsthilfe – Probleme managen

Das Problem an den neuen Medien, Technologien und Diensten ist, dass sie sich rasend schnell entwickeln und der normale Nutzer kaum in der Lage ist, alle Funktionen der Technologie, die er nutzen könnte, zu beherrschen. Für die meisten sind der Computer und das Internet ein notwendiges Mittel zum Zweck. Sobald aber etwas nicht funktioniert, ist guter Rat teuer. Wie gilt es sich hier zu verhalten?

Im realen Leben haben sich verschiedene Mechanismen für Problemfälle etabliert. Ist etwas im Haus defekt, wird ein Handwerker gerufen oder das eigene handwerkliche Geschick unter Beweis gestellt. Bei einem Mangel am Auto wird je nach Vorfall der Pannendienst gerufen oder das Auto zur Werkstatt gefahren. Auch «Vorsorgeuntersuchungen» wie Inspektionen sind üblich, und jedem Autofahrer ist bewusst, dass dies mit Kosten verbunden ist. Im Internet und in der digitalen Welt gibt es diese Abläufe noch nicht. So gut wie niemand kommt auf die Idee, Geld für eine Computerinspektion zu bezahlen oder bei Fehlern einen Fachmann zu rufen. Dabei sollte jedem bewusst sein, dass die digitalen Dienste heute bereits so wichtig sind, dass kostenpflichtige Hilfe ab und an nötig sein wird.

Erste Schritte zur Selbsthilfe

Ehe allerdings der Computerfachmann aus dem Freundeskreis oder aus dem Computerladen gerufen werden muss, gibt es einige Möglichkeiten im Internet, die bei der Fehleranalyse helfen. Fast alle Fehler sind schon einmal aufgetreten, weshalb es im Allgemeinen auch für die meisten Probleme eine

Lösung gibt. Das Internet bietet den Vorteil, dass sehr viele Nutzer ihre Erfahrungen im Internet veröffentlichen und sie so jedermann zur Verfügung stellen. Wenn ein Programm eine Fehlermeldung liefert, kann diese in eine Suchmaschine eingegeben werden, und fast immer finden sich auf der ersten Seite Suchergebnisse, die beschreiben, wie das Problem gelöst werden kann. Liegt eine Fehlfunktion vor, die keine direkte Fehlermeldung auslöst, können die wichtigsten Begriffe im Zusammenhang mit dem Problem in eine Suchmaschine eingegeben werden. Auch dies führt meist zum gewünschten Erfolg.

Es gibt im Internet bereits einige interessante Webseiten, die sich diesem Thema auf humorvolle Weise nähern. GIDF.de zum Beispiel ist eine Webseite, die lediglich die Suchmaschine Google eingebettet hat und für «Google Ist Dein Freund» steht. Dies soll zeigen, dass es sich lohnt, einen Fehler erst einmal zu googeln, bevor ein Dritter zurate gezogen wird. Etliche Probleme lassen sich relativ leicht auch durch eigene Recherche lösen.

Andere Probleme sind schwer zu erklären und nicht einfach über die Eingabe in eine Suchmaschine zu formulieren oder zu finden. In diesem Fall ist es sinnvoll, in einem Forum Rat zu suchen.

Dazu muss sich der Nutzer in einem entsprechenden Forum anmelden und hat dann die Möglichkeit, dort zu bestimmten Themengebieten Fragen zu stellen. Einige Foren umfassen sehr viele Bereiche (zum Beispiel www.wer-weiss-was.de, http://forum.chip.de), weshalb sich fast alle Fragen durch die Mitgliedschaft in ein bis drei Foren klären lassen (Hilfe-Foren siehe Softlink 621). In den Foren werden die Probleme geschildert, und die Internetcommunity antwortet. Dies ist ein

hilfreicher und genialer Effekt des Internets. Es ist möglich, mit wenigen Klicks sehr viele Nutzer um Hilfe zu bitten. Natürlich sollte auch in diesen Foren ein Nickname verwendet werden.

Führen diese Möglichkeiten nicht zum Ziel, muss ein Computerexperte eingeschaltet werden, der sich des Problems annimmt und es meist rasch und professionell löst – gegen eine angemessene Bezahlung versteht sich, denn der Mechaniker in der Autowerkstatt arbeitet auch nicht umsonst …

Glossar

Access Point: Zugangspunkt zu einem WLAN
Account: Benutzerkonto, Zugang zu einem Internetdienst. Üblicherweise muss ein Nutzer sich beim Login mit Benutzername und Passwort authentisieren.
ActiveX: eine von Microsoft entwickeltes Softwarekomponenten-Modell, mit dem unter anderem kleine Programme für den Browser geschrieben werden können (vergleichbar mit JavaSkript). ActiveX funktioniert nur in der Microsoft-Welt.
Add-on: Erweiterungsmöglichkeiten für den Browser, zum Beispiel um lästige Werbung zu blocken; wird auch als Plug-in bezeichnet
AES (Advanced Encryption Standard): symmetrisches Verschlüsselungsverfahren mit einer variablen Schlüssellänge von 128, 192 oder 256 Bit. AES bietet ein sehr hohes Maß an Sicherheit (siehe Softlink 326).
AJAX (Asynchronous JavaScript and XML): ein Konzept der asynchronen Datenübertragung zwischen einem Webserver und dem Browser
Aktive Inhalte: Sammelbezeichnung für Technologien, die innerhalb eines Browsers ausführbar sind und den Nutzer in die Lage versetzen, mit einem Webserver zu interagieren
Authentifikation: Verifizierung der Echtheit des Nutzers
Back-up: Sicherungskopie von Computerdateien auf einem externen Speichermedium
Blog: Internettagebuch, Bestandteil des Web 2.0

Bluetooth: Funkverbindung über kurze Distanzen zwischen mobilen Kleingeräten sowie zwischen Computer und Peripheriegeräten

Browser: spezielles Computerprogramm zum Betrachten von Webseiten im World Wide Web (WWW) oder allgemein von Dokumenten und Daten. Webbrowser stellen die Benutzeroberfläche für Webanwendungen dar.

Brute-Force-Angriff: Angriff auf den Computer, bei dem der Angreifer alle möglichen (Zeichen-)Kombinationen durchprobiert, um zum Beispiel Passwörter zu ermitteln

ClickandBuy: ein Zahlungssystem im Internet

Cracker: Hacker, der unbefugt in fremde Computersysteme eindringt und gespeicherte Daten und Programme in böser Absicht beziehungsweise zu seinem persönlichen Vorteil manipuliert, inspiziert oder zerstört

Creative-Commons-Lizenzen: Lizenzverträge, mittels derer Autoren der Öffentlichkeit Nutzungsrechte für ihre Werke (Texte, Bilder, Musikstücke usw.) einräumen können

Cross Site Scripting (XSS): das Ausnutzen von Sicherheitslücken, um unbemerkt Angriffe in einem für den Nutzer vertrauenswürdigen Umfeld (bekannte Webseiten) zu platzieren und durchzuführen

Domain: Name einer Internetseite (Webadresse), zum Beispiel www.internet-sicherheit.de

Domain Name Service (DNS): DNS löst als Internetdienst Domainnamen in IP-Adressen auf und umgekehrt.

ebay-Käuferschutz: Absicherung für Waren, die beim Internetauktionshaus ebay gekauft und mit PayPal bezahlt wurden. Wird die Ware nicht geliefert oder weicht diese erheblich von der Artikelbeschreibung ab, wird der bezahlte Kaufpreis zurückerstattet.

E-Commerce: Unter E-Commerce wird der elektronische Handel (Internethandel, Onlinehandel) verstanden.

FinTS (Financial Transaction Services): deutscher Standard für den Betrieb von Onlinebanking. FinTS ist eine Weiterentwicklung des Onlinebanking-Standards HBCI.
Firewall: elektronischer «Wächter» im Computer (oder in einem Netzelement wie einem Router), der sich darum kümmert, dass alle Ports, die nicht gebraucht werden, geschlossen sind
Flash: proprietäre Entwicklungsumgebung zur Erstellung multimedialer Inhalte. Flash wird auch für Animationen im Internet verwendet.
Flatrate: Pauschaltarif für Telekommunikationsdienstleistungen wie Telefonie und Internetverbindung
Freeware: kostenlose Programme aus dem Internet, die lizenzfrei genutzt werden können
FTP (File Transfer Protocol): Netzwerkprotokoll zur Übertragung von Dateien in einem Netzwerk
Gateway: Vermittlungsgerät, das es Netzwerken ermöglicht, miteinander zu kommunizieren, auch wenn diese auf völlig unterschiedlichen Protokollen basieren
GNU-Lizenz: Sammelbegriff für Lizenzen des GNU-Projekts. Das GNU-Projekt wurde mit dem Ziel gegründet, ein vollständig freies Betriebssystem zu entwickeln.
Hacker: Nutzer, der sehr vielfältige Kenntnisse im Umgang mit Computern besitzt. Der Begriff wird auch häufig für Personen verwendet, die sich unbefugt Zugang zu fremden Computersystemen verschaffen.
HBCI (Homebanking Computer Interface): eine standardisierte Schnittstelle für das Homebanking und Vorgänger von FinTS. Er wurde von verschiedenen Bankengruppen in Deutschland entwickelt und vom Zentralen Kreditausschuss (ZKA) beschlossen.
Helpdesk: Informations- und Hilfsdienst eines Herstellers oder innerhalb einer Organisation, der bei Problemen mit Soft- oder Hardware Unterstützung bietet

Hotspot: öffentlicher Internetzugang via WLAN

HTML (HyperText Markup Language): Auszeichnungssprache, mit der Webseiten beschrieben werden

HTTP (HyperText Transfer Protocol): Internetprotokoll, mit dem Daten zwischen Webserver und Browser ausgetauscht werden

HTTPS (HyperText Transfer Protocol Secure): Bei diesem Protokoll werden die Daten zwischen Webserver und Browser verschlüsselt und integritätsgesichert ausgetauscht.

IMAP (Internet Message Access Protocol): Anwendungsprotokoll, das den Zugriff auf und die Verwaltung von empfangenen E-Mails, die sich in einem Postfach auf einem Mailserver befinden, erlaubt

Internetauftritt: Gesamtheit der Funktionalitäten, die von einem Internetdienstanbieter in einer als zusammenhängend empfundenen Weise zur Verfügung gestellt werden, zum Beispiel ein Web- oder Chatserver

IPSec: ein Sicherheitsprotokoll, das Vertraulichkeit, Authentizität und Integrität bei der Übertragung von Datenpakten gewährleisten soll

IPv4/IPv6: Ein Internetprotokoll (IP) spezifiziert die Vorgänge, die zur Vermittlung von Datenpaketen durch das Internet notwendig sind, wie etwa die Adressierung der Computersysteme und Netzknoten. Zurzeit wird hauptsächlich die Version IPv4 eingesetzt, zukünftig soll die Version IPv6 verwendet werden.

iTAN (indizierte TAN): Onlinebanking-Verfahren, bei dem der Bankkunde seinen Auftrag nicht mehr mit einer beliebigen TAN (siehe «TAN») aus seiner Liste legitimieren kann, sondern von der Bank aufgefordert wird, eine bestimmte, durch eine Positionsnummer (Index) gekennzeichnete TAN zu verwenden.

Java-Applet: Programm, das in der Programmiersprache Java verfasst wurde und normalerweise in einem Browser ausgeführt wird

JavaScript: eine in HTML-Syntax integrierte Skriptsprache. JavaScript-fähige Browser interpretieren den in einer Webseite enthaltenen Code und führen ihn auf dem Computer aus.
JScript: Microsoft-eigene Skriptsprache für Browser
Key: Schlüssel, der für eine Verschlüsselung verwendet wird
Link (Kurzform von Hyperlink): Hyperlinks sind elektronische Verweise auf andere Webseiten, die sich überall auf der Welt befinden können. Der Nutzer folgt einem Link zum Beispiel durch Anklicken. Dieser Prozess kann unendlich oft wiederholt werden.
MAC-Adresse (Media-Access-Control-Adresse): Hardware-Adresse eines Netzwerkadapters (Computers) in einem Netz
Malware: Oberbegriff für «Schadsoftware» wie Viren, Würmer, Trojanische Pferde, Spyware usw.
mTAN (mobile TAN): Beim mTAN-Verfahren wird dem Onlinebanking-Kunden nach Übersendung der ausgefüllten Überweisung im Internet von der Bank per SMS eine nur für diesen Vorgang verwendbare TAN (siehe «TAN») auf sein Mobiltelefon gesendet. Das Verfahren wird auch als SMSTAN bezeichnet (siehe Softlink 342).
Nutzer: Person, die den Computer oder den Internetdienst für seine Zwecke nutzt
Nutzerprofil: Sammlung von Nutzerdaten eines Nutzers, zum Beispiel Cookies, Logins, Analyse von Logfiles und Bestell-/Interaktionsdaten
Onlineshop: Der Onlineshop stellt Waren und digitale Produkte im Internet zum Verkauf bereit.
Onlinestreaming/Onlinestreams: Übertragung von Realzeitanwendungen wie Radio und Fernsehen über das Internet
Patch: Aktualisierung eines Programms, um bestimmte Funktionen zu integrieren beziehungsweise zu korrigieren
PayPal: Bezahldienst mit Käuferschutz, bei dem Käufer und Verkäufer keine Kontodaten des jeweils anderen erhalten

Personal Firewall: Sicherheitsprogramm, das den ein- und ausgehenden Datenverkehr auf dem zu schützenden Computer filtert und reglementiert; erweitert die Firewallfunktionen um die Kontrolle von Anwendungen

Personensuchmaschine: Suchmaschine, die speziell nach personalisierten Einträgen im Internet sucht

Phishing: der Versuch, durch Vortäuschen einer fremden Identität mittels gefälschter E-Mails und Webseiten vertrauliche Passwörter zu ergaunern

PIN (persönliche Identifikationsnummer): eine nur einer oder wenigen Personen bekannte Zahl, mit der diese sich gegenüber einem Dienst authentisieren können (Anwendung bei Webseiten, ec-Karten, beim elektronischen Personalausweis ...).

POP3 (Post Office Protocol Version 3): Übertragungsprotokoll, über das ein Client E-Mails von einem E-Mail-Server abholen kann

Port: Ports sind interne und externe Schnittstellen eines Computers (Servers). Sie werden zum Beispiel von dem jeweiligen Transportprotokoll benutzt, um Anwendungen auf einem Server zu adressieren (beispielsweise über Port 80 einen Webserver und über Port 25 einen E-Mail-Server).

Pre-Shared Key: ein vorab vereinbarter beziehungsweise verteilter Schlüssel, zum Beispiel für die WLAN-Verschlüsselung

Programmcode: ein in einer Programmiersprache geschriebener Text eines Computerprogramms

Provider: Dieser Begriff bezeichnet einen Anbieter oder Dienstleister (zum Beispiel Telekommunikationsanbieter, Mobilfunkanbieter, Internetdienstanbieter).

Repeater: elektrischer Signalverstärker, der dazu dient, Netze zu erweitern, deren räumliche Ausdehnung aus physikalischen Gründen (Signaldämpfung und Signalverformung) begrenzt ist

Router: Netzwerkkomponente, die verschiedene Teilnetze koppelt beziehungsweise trennt

Server: Der Begriff Server bezeichnet eine Soft- und Hardware im Rahmen des Client-Server-Modells. Das Client-Server-Modell beschreibt eine Möglichkeit, Aufgaben und Dienstleistungen innerhalb eines Netzwerks, zum Beispiel dem Internet, zu verteilen. Der Client kann auf Wunsch eine Aufgabe vom Server anfordern. Der Server beantwortet die Anforderung.

Smartphone: modernes Mobiltelefon (Handy), das mit einem erweiterbaren Betriebssystem arbeitet, gut vernetzt ist (GSM, UMTS, WLAN, Bluetooth usw.) und die Nutzung von zusätzlicher Software (E-Mail-Client, Browser etc.) gestattet

SMTP-Server: Ein E-Mail-Anbieter stellt mindestens einen sogenannten SMTP- oder E-Mail-Server zur Verfügung. Das SMTP-Protokoll ist das Kommunikationsprotokoll, das für den Transfer der E-Mail vom Mail-Client zum Mail-Server und zwischen den Mail-Servern über das Internet sorgt.

Social Network/soziales Netzwerk: Webdienst, bei dem die Nutzer gemeinsam eigene Inhalte erstellen

SSL (Secure Socket Layer): vorherrschendes Protokoll für die Verschlüsselung der Datenübertragung im Web

Suchmaschine: Programm zur Recherche von Dokumenten, die in einem Computer oder im Internet gespeichert sind. Nach Eingabe eines Suchbegriffs liefert eine Suchmaschine eine Liste von Verweisen auf möglicherweise relevante Dokumente Die bekanntesten Suchmaschinen im Internet sind Google, bing und Yahoo.

Surfen: das Bewegen im Web beziehungsweise das Durchstöbern des Webs

TAN (Transaktionsnummer): Einmalpasswort, das üblicherweise aus sechs Dezimalziffern besteht und vorwiegend im Onlinebanking verwendet wird

TKIP (Temporal Key Integrity Protocol): Verschlüsselungsprotokoll für WLANs. TKIP wird in dem Standard WPA verwendet.

UMTS (Universal Mobile Telecommunications System): Mobilfunkstandard der dritten Generation (3G), mit dem deutlich höhere Datenübertragungsraten als mit dem Mobilfunkstandard der zweiten Generation (2G) und dem GSM-Standard möglich sind

URL (Uniform Resource Locator): URLs identifizieren und lokalisieren eine Ressource über das verwendete Netzwerkprotokoll (beispielsweise HTTP oder FTP) und den Ort der Ressource im Netzwerk.

USB-Stick: kompaktes Speichermedium mit hoher Kapazität und Zugriffsgeschwindigkeit mit integriertem USB-Stecker

Verschlüsselung: mathematische Transformation von Daten, die es einem Angreifer unmöglich machen soll, die Originaldaten zu rekonstruieren (Softlink 326).

Virensignatur: eindeutiges Erkennungsmerkmal von Viren, das von Anti-Virus-Programmen zu deren Identifizierung genutzt wird

Web 2.0: interaktives Internet, das es dem Nutzer ermöglicht, zum Beispiel Kommentare zu hinterlassen oder Spiele im Netz zu spielen

Webadresse: Adresse, mit der eine Webseite adressiert werden kann, zum Beispiel www.sicher-im-internet.de

Webbrowser: siehe «Browser»

Webserver: ein Server, der Webseiten anbietet

Zertifikat: Dieser Begriff bezeichnet eine Datenstruktur, die eine Identifikation des Besitzers, seinen öffentlichen Schlüssel, ein Ablaufdatum und die digitale Signatur einer Zertifizierungsstelle enthält und so die Integrität und Authentizität garantiert.

Zugangsdaten: Daten, die zur Überprüfung der Berechtigung verwendet werden (Nutzerkennung und Passwort)

Weitere Glossareinträge finden Sie unter Softlink 710.

Danksagung

In erster Linie möchten wir Ihnen, den Leserinnen und Lesern, danken, dass Sie dieses Buch gekauft haben. Ein Buch zu schreiben ist eine sehr spannende Aufgabe und der Beweis dafür, dass der Weg von einer Idee bis zu ihrer Umsetzung doch ein recht weiter ist. Die Idee war, das Internet und damit das digitale Leben ein bisschen sicherer zu machen, indem wir für jeden verständliche Tipps und Informationen in diesem Buch zusammentragen. Wir hoffen, dass uns dies gelungen ist. Der Weg war lang, aber er wäre viel länger gewesen, wenn uns nicht so viele wunderbare Menschen unterstützt hätten. Wir möchten hiermit all unseren tatkräftigen Weggefährten danken: den Mitarbeitern des Orell Füssli Verlags und von Ariadne-Buch, den fleißigen Probelesern Gertrud, Marian, Josef, Luisa, Alexander, Björn, Dirk, Boris, Gerda, Sven und Julia sowie Andrej und den if(is)-Mitarbeitern, insbesondere den «Live-Hacking-Team-Mitgliedern» Marian und Niklas. Ein besonderer Dank gilt unseren Partnerinnen Bettina und Britta für ihre Kritik, die unermüdliche Unterstützung und die aufmunternden Worte.