Uli Ries / Tombo Mörgenthaler

Know-how ist blau.

Das inoffizielle facebook-Buch

Wie Sie Betrugsversuche erkennen und sich davor schützen

> Clickjacking, Scareware, Phishing & Co.:
Die häufigsten Angriffe auf der größten Social-Media-Plattform der Welt

> Sicher ist sicher: Die optimalen Sicherheitseinstellungen für Ihr Facebook-Konto

> Es geht nur ums Geld: So arbeiten Cyber-Kriminelle

FRANZIS

Uli Ries / Tombo Mörgenthaler

Das inoffizielle facebook-Buch

Uli Ries / Tombo Mörgenthaler

Das inoffizielle facebook-Buch

Wie Sie Betrugsversuche erkennen und sich davor schützen

Mit 141 Abbildungen

Bibliografische Information der Deutschen Bibliothek

Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie;
detaillierte Daten sind im Internet über http://dnb.ddb.de abrufbar.

Herausgeber: Ulrich Dorn
Satz: DTP-Satz A. Kugge, München
art & design: www.ideehoch2.de
Druck: Bercker, 47623 Kevelaer
Printed in Germany

ISBN 978-3-645-60101-6

Vorwort

Eines will dieses Buch ganz sicher nicht: Ihnen die Freude an Facebook & Co. verderben. Wir wollen durch diese Sammlung von Betrugsversuchen keine Horrorszenarien zeichnen und die – unbestritten vorhandenen – Probleme auch nicht größer darstellen, als sie sind.

Aber insbesondere Facebook ist aufgrund seiner gigantisch hohen Zahl an Nutzern nicht nur bei den freundlich gesinnten Zeitgenossen beliebt, sondern auch bei Onlinebetrügern. Letztere treiben sich natürlich dort herum, wo viele potenzielle Opfer warten – ähnlich einem Taschendieb, der von überfüllten Fußgängerzonen und Touristenattraktionen angelockt wird. Und kein Ort im Internet versammelt derzeit und sicherlich auch in absehbarer Zukunft mehr Menschen, als es das soziale Netzwerk Facebook tut.

Wie immer im Leben gilt auch beim Umgang mit Onlinediensten die viel zitierte Binsenweisheit »Gefahr erkannt, Gefahr gebannt«. Daher wollen wir Ihnen in diesem Buch möglichst viele der derzeit bekannten Gefahren aufzeigen. Einige dieser Betrugsversuche – wie die »Klick hier, um zu sehen wer auf deinem Profil war«-Wellen – mögen Ihnen schon selbst untergekommen sein, manch andere noch nicht. Nachdem die Muster der Attacken aber immer die gleichen sind, können Sie nach dem Lesen der betreffenden Kapitel dieses Buchs auch bislang unbekannte Betrügereien in Zukunft zielsicher erkennen.

Schlagen Sie den Onlinegaunern mit unserer Hilfe ein Schnippchen. Sie schützen so nicht nur Ihren eigenen PC und Ihr eigenes Bankkonto. Indem Sie andere auf Betrugsversuche aufmerksam machen und selbst auch gar nicht erst bei der Verbreitung der Abzocke helfen, tragen Sie auch zum Schutz Ihres digitalen Freundeskreises bei.

Sie erfahren nicht nur, wie die Betrugsmaschen aussehen und warum auch Nutzer von Smartphones oder Apple-Computern auf der Hut sein sollten, sondern auch, wie Sie Ihren Computer bestmöglich gegen alle Arten von Cyber-Attacken schützen können.

München, im Juli 2011

Tombo Mörgenthaler & Uli Ries

Inhaltsverzeichnis

1 Willkommen im Netz

Ganz egal, ob man in sozialen Netzwerken einen Segen oder einen Fluch sieht – ihre Beliebtheit ist riesig. Allen voran Platzhirsch Facebook, der mit weltweit etwa 600 Millionen Mitgliedern wohl die populärste Webseite aller Zeiten ist. Allein in Deutschland haben über 20 Millionen Menschen (Stand: Juni 2011) ein Facebook-Konto. Eine erstaunliche Zahl angesichts der 50 Millionen Deutschen, die überhaupt einen Internetzugang haben. Facebook gibt die Nutzerzahlen halbwegs realistisch an, da nur die Konten gezählt werden, die binnen der letzten 30 Tage zumindest einmal aktiv waren.

Bild 1.1: Gigantisch: Mit 600 Millionen Mitgliedern ist Facebook die am stärksten frequentierte Website überhaupt. (Bild: Facebook)

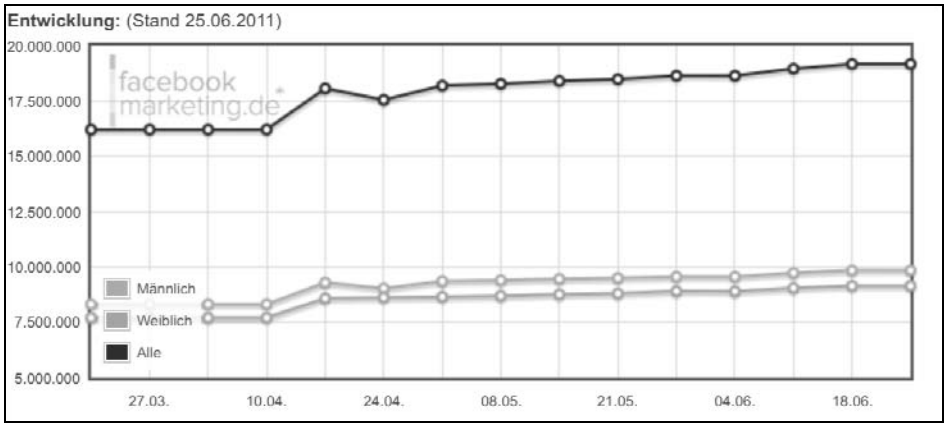

Bild 1.2: Stattlich: Beinahe 20 Millionen Deutsche haben ein Facebook-Konto. (Bild: facebookmarketing.de)

Bild 1.3: Gezwitschert: Twitter ist der Urvater der Microblogging-Dienste und für viele Millionen Internetnutzer zum bevorzugten Kommunikationskanal geworden. (Bild: Twitter)

Twitter wird hierzulande zwar nur von knapp einer halben Million Menschen genutzt – der Einfluss des Microblogging-Diensts ist dennoch immens. Nicht nur bei den Aufständen in der arabischen Welt drang vieles per Twitter nach außen. Auch Unternehmen nutzen den Dienst, um schnell und unkompliziert mit ihren Kunden in Kontakt zu treten. Insbesondere in schwierigen Zeiten wie beispielsweise den Flugausfällen durch die Aschewolke war Twitter ein immenser Gewinn – für Fluglinien und Passagiere

gleichermaßen. Aber auch Angenehmes wie Sonderangebote oder Gewinnspiele lassen sich vorzüglich per Twitter bekannt machen.

1.1 Angriff und Verteidigung

So vielfältig die Betrugsversuche sind, die jeweiligen Hintermänner wollen letztendlich alle nur eines: Geld verdienen. Wir beschreiben Ihnen, wie die Cyber-Gauner an (Ihr) Geld kommen wollen und wie Sie sich vor der Onlineabzocke schützen können. Es ist wichtig zu wissen, dass die Angriffe in der Regel immer ähnlich starten (siehe Kapitel 2 »Angriffsvielfalt«). Was die Betrüger aber letztendlich mit dem in die Falle getappten Anwender genau anstellen, variiert. Mal wird über eine Welle aus Spam-Pinnwandeinträgen eine merkwürdige Umfrage propagiert, mal wird Schadsoftware auf den PC des Anwenders geschleust, und wieder ein anderes Mal werden persönliche Daten per Formular abgefragt – mitunter sogar Kreditkarteninformationen.

1.2 Trau deinen Freunden nur bedingt

Facebook ist nicht nur aufgrund der riesigen Anzahl von Nutzern – aus Sicht der Betrüger: potenziellen Opfern – ein attraktives Ziel für Onlinekriminelle. Gleichzeitig bietet die Webseite den Angreifern auch noch zahlreiche technische Möglichkeiten, die vielfältige Betrügereien möglich machen: klassischer Spam per Facebook-Nachricht, vermeintliche Videos per Pinnwandeintrag, Phishing-Versuche per Facebook-Chat.

Bild 1.4: Hier ist Misstrauen angebracht: Auch auf den Fanseiten von bekannten Unternehmen kann sich merkwürdiger Inhalt finden. In diesem Fall hat ein Administrator der Lufthansa-Fanpage auf eine betrügerische Anwendung geklickt und so einen Eintrag an der Pinnwand der offiziellen Unternehmensseite innerhalb von Facebook erzeugt.

Außerdem missbrauchen die Webgauner die Grundidee von Facebook und Twitter: das soziale Geflecht zwischen den Anwendern. Gelingt es den Kriminellen, einen Facebook- oder Twitter-Nutzer zum (ungewollten) Verbreiten ihrer Spam- oder Phishing-Nachrichten zu motivieren, ist der Erfolg dieser Betrugswelle ungleich größer als bei herkömmlichen Spam-Kampagnen. Denn Nachricht, Tweet oder Pinnwandeintrag wurde ja von einem Freund oder Bekannten verschickt. Insofern trauen die Empfänger der Botschaft eher, als wenn sie von einem Unbekannten mit afrikanischem Nachnamen in schlechtem Englisch verschickt wurde. Wie die Betrüger ihre Opfer zum Verbreiten von Nachrichten bewegen, erfahren Sie in Kapitel 2, »Angriffsvielfalt«.

1.3 Facebook ist nicht gratis

Facebook verlangt von seinen Nutzern keinen monatlichen Beitrag oder sonstige Gebühren. Gratis ist die Nutzung des Diensts dennoch nicht. Wir alle, die wir Facebook nutzen, bezahlen mit unseren Daten. Der Kryptografie- und Sicherheitsexperte Bruce Schneier brachte es, an Facebook-Nutzer gewandt, auf den Punkt:

»Macht nicht den Fehler zu glauben, ihr wärt die Kunden von Facebook. Ihr seid es nicht – ihr seid das Produkt. Die Kunden des Unternehmens sind die Werbetreibenden.« (Im Original: *"Don't make the mistake of thinking you're Facebook's customer, you're not – you're the product. Its customers are the advertisers."*)

Bild 1.5: Altbekannt: Wie überall im Internet sind auch innerhalb von Facebook Werbeanzeigen zu sehen. Damit erzielt das soziale Netzwerk einen Großteil seines Umsatzes.

1.3.1 Was verkauft Facebook an seine Werbekunden?

Facebook verkauft hauptsächlich die auch von anderen Webseiten bekannten Banner. Sie sind rechts außen zu sehen und können – ähnlich wie Werbebanner innerhalb von Google Mail – in Abhängigkeit vom gerade Geschriebenen angepasst werden. Hat man also gerade einen Pinnwandeintrag über das neue Apple iPad oder den New-York-Urlaub geschrieben, erscheinen nach Klick auf *Senden* rechts außen Anzeigen zu diesem Themen. Facebook erkennt also Schlagwörter in den Texten und sucht die passenden Einblendungen aus.

Facebook verkauft aber auch Informationen. Und zwar Informationen über seine Nutzer – die von diesen zuvor selbst ein- und freigegeben wurden. Will ein Kunde eine Kampagne innerhalb des sozialen Netzwerks schalten, kann er sehr fein justieren, wer die Anzeige überhaupt zu sehen bekommen. Nicht nur nach Geschlecht und Alter kann gefiltert werden, sondern auch nach bestimmten Interessen oder bereits vorhandenen Verbindungen zu anderen Fanseiten innerhalb von Facebook.

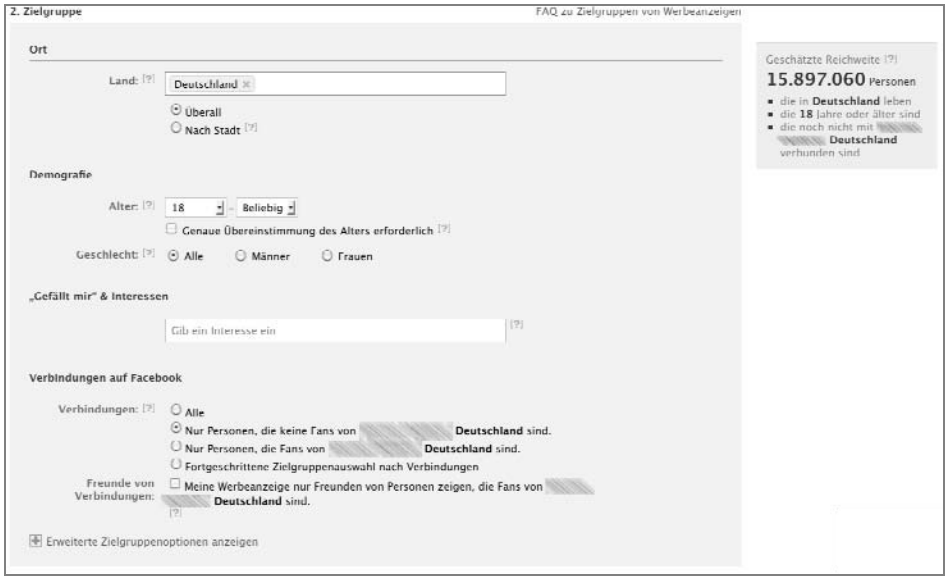

Bild 1.6: Gezielt: Werbekunden können haargenau bestimmen, wer ihre Anzeige zu sehen bekommt.

Für viele Datenschützer ist die Sammel- und Verkaufswut von Facebook ein rotes Tuch. Und in der Tat sollten alle Nutzer vorsichtig mit dem umgehen, was sie im Netz – nicht nur bei Facebook, aber insbesondere dort – über sich preisgeben. Nicht nur, um nicht zur verkaufbaren Verhandlungsmasse zu werden, sondern auch, um Identitätsdiebstahl oder peinliche Momente zu verhindern. Peinlich deswegen, weil beispielsweise wenig rühmliche Bilder mit dem eigenen Namen verknüpft werden und mangels korrekter *Privatsphäre-Einstellungen* auch von Google gefunden und jedem beliebigen Webnutzer angezeigt werden.

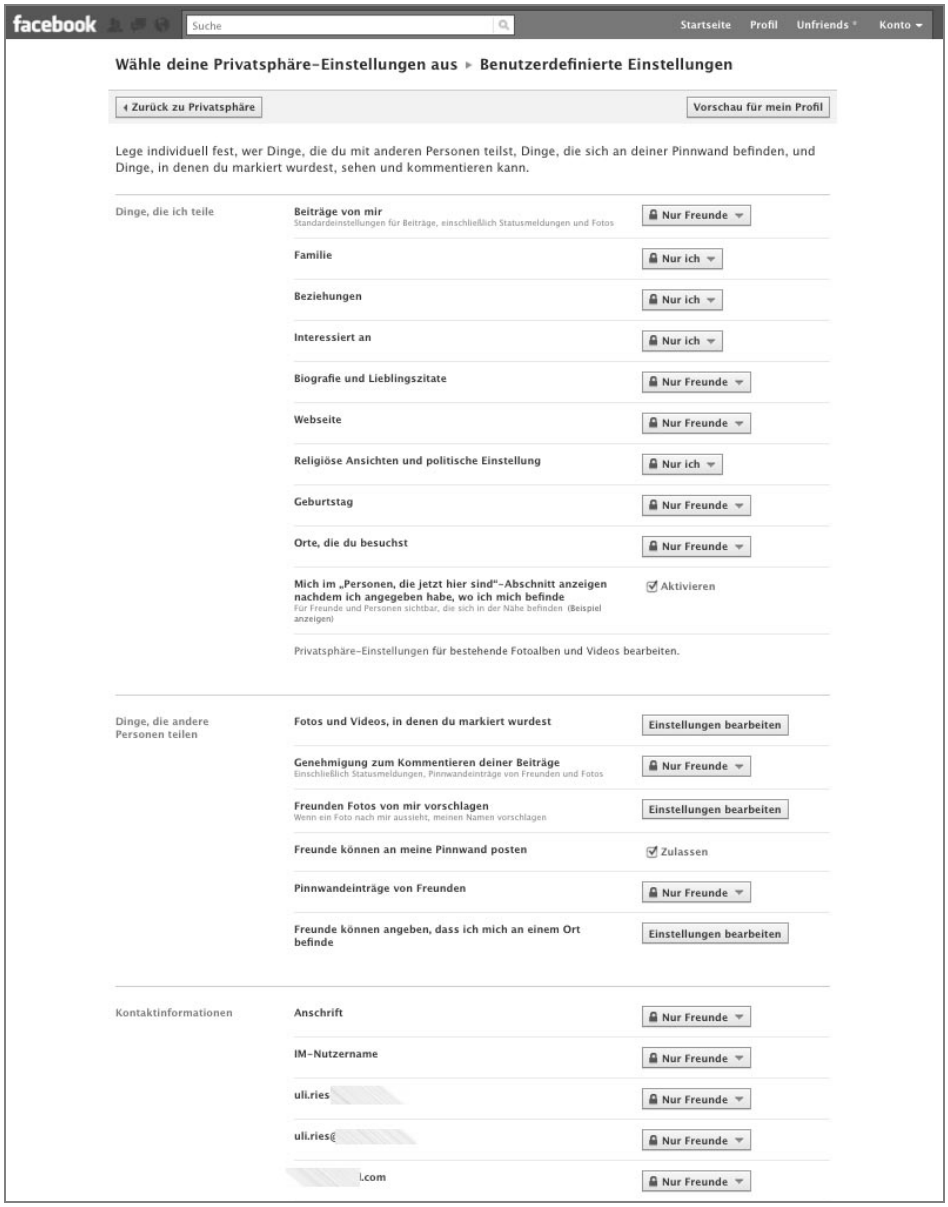

Bild 1.7: Lange Liste: die Facebook-Datenschutzeinstellungen.

Obwohl das Thema Datenschutz überaus relevant ist: In diesem Buch soll es nicht darum gehen. Weder wollen wir schildern, an welchen Ecken eventuell Gefahr durch das kommerzielle Treiben von Facebook droht, noch beschreiben wir in aller Detailtiefe, wie Sie Ihr Facebook-Profil gegen allzu aufdringliche Schnüffler schützen können. Zum einen würde das den Rahmen dieses Buchs sprengen – Facebook ist ein durchaus komplexer Dienst, der ebenso komplexe Einstellungen erfordert –, zum anderen ändert Facebook in unregelmäßigen Abständen auch die Einstellungsmöglichkeiten beziehungsweise fügt neue Optionen hinzu. Die Gefahr, dass unsere Anleitung also schon mit

Erscheinen dieses Buchs veraltet wäre, ist demnach zu groß. In Kapitel 11, »Facebook, aber sicher«, haben wir dennoch einige grundsätzliche Ratschläge aufgeführt und nennen auch Quellen im Internet, die Tipps rund um die Sicherheit und die Privatsphäre geben.

1.4 Gefällt mir – oder doch nicht?

Der *Gefällt mir*-Button mit dem nach oben gereckten Daumen ist auf dem besten Weg, zu einem weltweit bekannten Symbol zu werden. Selbst Google ahmt die Funktion mit seinem »+1« genannten Konzept nach, mit dem Nutzer ihren Freunden die per Suchmaschine gefundenen Links weiterempfehlen können.

Bild 1.8: Allseits bekannt: Der nach oben gereckte Daumen steht für »Gefällt mir« – und kann ein Datenschutzproblem sein.

Das Original von Facebook findet sich schon seit Längerem auf einer riesigen Anzahl von Webseiten. Nachrichten- und Shoppingangebote gehören genauso dazu wie Reiseportale oder private Blogs außerhalb des sozialen Netzwerks. Klickt ein Nutzer dieser Seiten auf den Button, erscheint automatisch eine Meldung an seiner Pinnwand, dass ihm das betreffende Webangebot gefällt.

1.4.1 Ein Klick mit Folgen

So bequem der Klick auch sein mag, er ist aus Sicht des Datenschutzes problematisch. Denn Facebook bekommt durch den auf fremden Seiten platzierten Button eine Menge Informationen: Damit das *Gefällt mir*-Symbol auf externen Webangeboten erscheint, müssen diese Angebote einen sogenannten iFrame einbinden. iFrames sind Miniwebseiten innerhalb einer größeren Seite. Sie können auch gänzlich unsichtbar bleiben. Im Fall des Buttons ist das iFrame, dessen Quelltext gänzlich von Facebook kontrolliert wird, sichtbar. Bei jedem Aufruf einer Webseite, die den Button besitzt, wird also ohne weiteres Zutun des Anwenders der Facebook-Code aufgerufen – auch ohne Klick auf *Gefällt mir*.

Der Webbrowser wird durch den Facebook-Code dazu veranlasst, die gerade geöffnete Seite an Facebook zu übermitteln. Das ist an sich kein Problem – es sei denn, der Facebook-Nutzer ist in einem anderen Browsertab parallel bei Facebook eingeloggt. Denn dann kann das soziale Netzwerk die externen Seitenaufrufe mit dem Namen des Anwenders verknüpfen. Im Laufe der Zeit bekommt Facebook so ein ziemlich stimmiges Bild über das Surfverhalten und die Interessen seiner Mitglieder.

Noch nicht einmal Google weiß derart viel, außer wenn man einen Google-Account besitzt und beim Surfen permanent bei diesem angemeldet ist. Andernfalls sind die von Google ermittelten Daten anonym. Nachdem Facebook seinen Werbekunden eine

zielgenaue Profilierung ihrer Anzeigen bietet, würde es doch sehr erstaunen, wenn nicht auch diese per *Gefällt mir* gesammelten Daten an die Anzeigenkunden weitergereicht würden – gegen Bezahlung.

Wie das Onlineportal heise security schreibt, kann die automatische Datenübermittlung vom Anwender unterbunden werden. So bietet beispielsweise Firefox eine Option, um den Transfer von Cookies von Drittanbietern – in diesem Fall das Facebook-Cookie – zu verhindern. Wie das genau funktioniert, erklärt eine Hilfeseite von den Firefox-Machern von Mozilla (*http://bit.ly/lULnzE*).

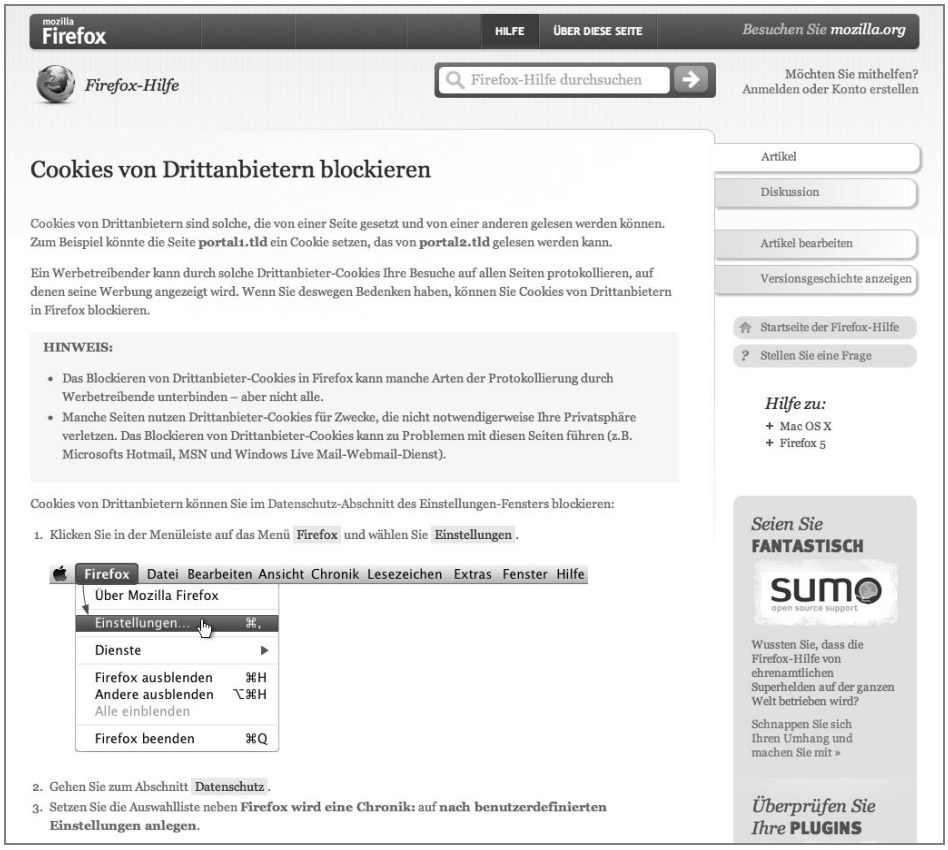

Bild 1.9: Sie surfen bevorzugt mit Firefox? Dann erfahren Sie hier, wie Sie den Transfer von Cookies von Drittanbietern unterbinden.

6 Nächstes Ziel: Handys

Was haben Smartphones mit den Angriffen zu tun, die per Facebook und Twitter passieren? Derzeit glücklicherweise noch nicht allzu viel, ähnlich wie beim Mac. Zwar gibt es Facebook-Apps für alle gängigen Smartphone-Betriebssysteme, und auch die Browser der modernen Mobiltelefone sind in der Lage, den Betrugsversuchen eine hinreichend leistungsfähige Grundlage zu bieten. Und natürlich könnten unbedarfte Nutzer per Smartphone ihre privaten Daten auch in eines der nur vermeintlich zweckmäßigen Formulare eingeben, die nach Klick auf einen bösartigen Pinnwandeintrag erscheinen – in der Hoffnung, beim angepriesenen Gewinnspiel abzuräumen.

Bild 6.1: Im Fadenkreuz: Smartphones wie das Apple iPhone oder das auf Google Android basierende Samsung Galaxy 550 sind für Malware-Programmierer lohnende Ziele. (Bilder: Apple/Samsung)

6.1 Massiver Zuwachs an Schädlingen

In einem Punkt herrscht aber zumindest derzeit noch vergleichsweise Ruhe im Umfeld der cleveren Telefone: Es gibt kaum Schadsoftware. Insofern sind die Malware-Attacken aus den sozialen Netzwerken noch keine große Gefahr für die Datensicherheit von Mobiltelefonen. Aber: Die Anzahl der Schädlinge hat massiv zugenommen im letzten Jahr. Laut des aktuellen »Mobile Threats Report« des Juniper Network Global Threat Center ist die Anzahl der Smartphone-Schädlinge von 2009 auf 2010 um 250 Prozent gestiegen.

Insofern ist es jetzt an der Zeit, sich als Nutzer eines solchen Geräts auch mit den möglichen Gefahren zu beschäftigen. Dass dies noch zu wenige tun, belegt eine Umfrage des auf IT-Sicherheit spezialisierten SANS Institute: Im Jahr 2010 hatten lediglich 15

Prozenzt aller befragten Smartphone-Nutzer eine Schutzsoftware auf ihren Geräten installiert.

Solche Software dürfte aber über kurz oder lang unvermeidbar werden, genau wie in der Windows- und Mac-Welt. Denn eines steht fest: Um die Malware auf die mobilen Begleiter zu bringen, setzen die Onlinekriminellen mit Sicherheit auf die bewährten Wege. Und kein Weg ist derzeit attraktiver als der über Facebook.

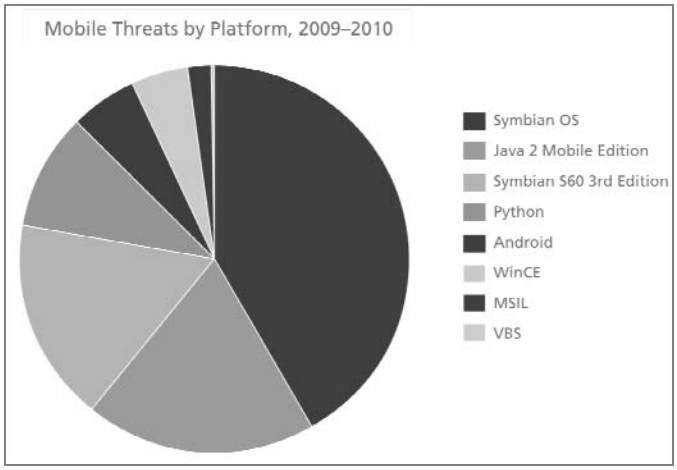

Bild 6.2: Schädlingsverteilung: Laut einer Untersuchung von McAfee wurden zwischen 2009 und 2010 für das Smartphone-Betriebssystem Symbian die meisten Schädlinge entwickelt und freigesetzt. (Bild: McAfee)

6.2 Androiden in Gefahr

Nach und nach zeigt sich, dass die Erwartung der Virenexperten leider richtig ist. Vor allem Googles offenes Mobil-Betriebssystem Android scheint die Malware-Macher in letzter Zeit anzulocken. Im Vergleich zu Handybetriebssystemen wie Symbian oder der Java-Plattform ist Googles Smartphone-Betriebssystem ein Newcomer. Dennoch haben sich Onlinekriminelle derart schnell auf Android eingeschossen, dass die hierfür programmierte Malware nach Symbian und Java am dritthäufigsten verbreitet ist. Dies geht aus der aktuellen Malware-Statistik von McAfee für das erste Quartal 2011 hervor, in dem laut McAfee die größte jemals bisher ermittelte Anzahl von Schädlingen auftauchte.

Im genannten Quartal belegte die Android-Malware sogar den zweiten Rang hinter der Schadsoftware für Symbian OS. Die Antivirenexperten von Kaspersky vergleichen die Sicherheitslage der Android-Welt sogar mit der von Microsoft Windows – und Letztere ist ja durchaus als desolat zu bezeichnen.

Das Problem der alten Betriebssysteme
Im Zusammenhang mit der Schädlingsuntersuchung für Android stellte Kaspersky in seinem Sicherheitsbericht für das erste Quartal 2011 fest, dass sich die in freier Wildbahn entdeckten Android-Trojaner über eine Betriebssystemlücke verbreiteten. Betroffen waren ausschließlich Smartphones, auf denen ein älteres System als die seit Dezember 2010 erhältliche Version 2.3 (Gingerbread) installiert war. Ein Vierteljahr nach Veröffentlichung lief Gingerbread laut Google nur auf 2 Prozent aller Android-Smartphones weltweit. Hauptsächlich verantwortlich hierfür sind die Hersteller der Geräte. Sie passen das von Google gelieferte System noch an ihre Geräte an, wodurch Zeit verloren geht. Außerdem ist der Prozess teuer, sodass für ältere Modelle wahrscheinlich sehr bald gar keine Updates mehr erscheinen. Die sonst so attraktive Offenheit des Android-Systems wird in Sachen Sicherheit somit zum Problem für die Anwender.

Nachdem im vergangenen Jahr hauptsächlich IT-Sicherheitsforscher durch diverse Malware-Demonstrationen für Android auf sich aufmerksam machten, legen nun die wahren Virenschreiber nach. Denn Anfang 2011 ist mit »Gemini« der erste echte Schädling im Netz und auf Smartphones aufgetaucht. Ganz im Stil der vom PC bekannten Botnet-Trojaner verbindet sich auch Gemini nach der Installation mit einem Server, um so Kommandos vom Kontrolleur des Botnets zu empfangen.

Bild 6.3: Im Visier: Auf Googles Smartphone-Betriebssystem Android haben es die Programmierer von Malware besonders abgesehen. (Bild: Google)

Das ist ein Botnet
Botnets sind Zusammenschlüsse von PCs, die weltweit mit dem gleichen Schädling infiziert wurden. Die Malware nistet sich unbemerkt auf dem Computer ein und wartet auf Kommandos, die der Kontrolleur – im Englischen »Bot-Herder« genannt – an die Software schickt. Die infizierten PCs heißen Zombies, und der Server, von dem die Kommandos ausgehen, wird als Command & Control-Server (C&C-Server) bezeichnet.
Die Zombies werden in der Folge beispielsweise dazu missbraucht, Spam zu verschicken. Schätzungen zufolge stammen weit über 90 Prozent aller weltweit versandten Spam-E-Mails von Zombie-PCs. Auch groß angelegte Attacken, mit denen selbst leistungsfähige Webserver von Internetunternehmen in die Knie gezwungen werden, werden mithilfe der gekaperten PCs geritten.

Gemini versteckt sich in legitimen Anwendungen oder auch in geknackten Versionen von ansonsten kostenpflichtiger Software (siehe Abschnitt »Schadsoftware huckepack«). Auf diese Weise findet der Schädling den Weg auf die Smartphones, in dem er hucke-

pack mit installiert wird. Der Trojaner wandert also in jedem Fall nur durch Zutun des Anwenders auf das Telefon.

Beschrieben wurde Gemini unter anderem von IT-Sicherheitsexperten der Firma Lookout, eines Herstellers von Sicherheitssoftware für Android. Auch diesen Fachleuten ist unklar, was das eigentliche Ziel von Gemini ist. Die Erklärungsversuche reichen von einem mobilen Botnet bis hin zu einem gekaperten Werbenetzwerk. Letzteres könnte den Gemini-Machern – oder deren Kunden – dazu dienen, mit ihrem Geschöpf Geld zu verdienen. Außerdem lassen sich auf diesem Weg Links zu manipulierten Webseiten auf dem Display des Geräts anzeigen – ein weiterer Weg, um später neue Varianten der Malware auf das Smartphone zu schleusen.

Fest steht: Der Schädling kann die aktuelle Position des Smartphones auslesen und die GPS-Daten zum C&C-Server schicken. Ebenfalls ausgelesen werden die zum Identifizieren von Endgeräten und SIM-Karten verwendeten Kennungen IMEI und IMSI und die auf dem infizierten Smartphone installierten Anwendungen. Um sich selbst mit neuen Funktionen zu erweitern, lädt Gemini verschiedene Applikationen im Hintergrund herunter und fordert den Handynutzer anschließend auf, diese App zu installieren. Um eventuell gefährliche Anwendungen wie Antivirensoftware loszuwerden, fordert Gemini vom Nutzer das Entfernen dieser Programme.

Bild 6.4: Alternative: Neben Googles offiziellem Android Marketplace gibt es noch zahlreiche andere Quellen zum Download von Anwendungen für Android-Smartphones.

6.3 Trojaner hört auf Kreditkartennummern

In keinem App-Store zu finden ist der Trojaner namens Soundminer. Denn er ist – einmal mehr – das Resultat einer Forschungsarbeit, in diesem Fall von Experten der Universitäten in Hongkong und Bloomington (Indiana University, USA). Die Schadsoftware ist nicht im Netz zu finden, lediglich in einem Dokument beschreiben die Forscher die Malware. Außerdem ist auf YouTube ein Video zu finden, in dem die Programmierer Soundminder demonstrieren.

Die Besonderheit des Android-Demoschädlings: Er analysiert die mit dem infizierten Telefon geführten Gespräche. Durch eine Spracherkennung reagiert Soundminer auf vom Sprecher übermittelte Kreditkartennummern. Die Software reduziert den Sprachstrom durch clevere Analyseverfahren auf die relevanten Informationen (in diesem Fall die Kreditkartendaten) und sendet dann nur diesen kleinen Teil des Gesprächs per Datennetzwerk an seine Schöpfer. Die Forscher betonen, dass sie diese Funktionen unter praxisnahen Bedingungen erfolgreich getestet haben.

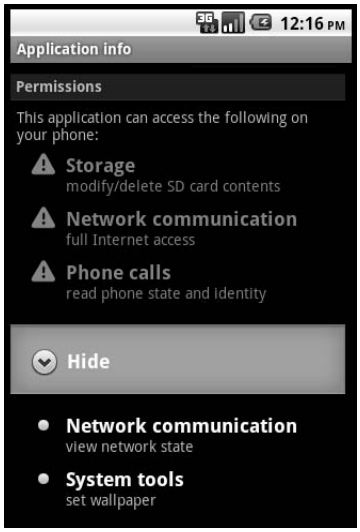

Bild 6.5: Fragerunde: Android-Anwendungen weisen während der Installation darauf hin, welche Rechte sie später für sich beanspruchen. Der Anwender kann dies zulassen oder unterbinden.

Einmal mehr könnte das potenzielle Opfer während der Installation der Malware Verdacht schöpfen, wenn die Software nach den notwendigen Berichtigungen fragt. Um hier möglichst dezent aufzutreten, verlangt Soundminer – beziehungsweise die legitime App, auf der der Schädling ins System reiten will – lediglich den Zugriff auf das Mikrofon. Das ist beispielsweise bei Spielen nichts Außergewöhnliches. Verdächtige Zugriffe wie Netzwerkzugriff oder Auslesen des Adressbuchs unterbleiben.

Den Versand der mitgeschnittenen Daten erledigt eine zweite Schad-Komponente, von den Forschern Deliverer genannt. Der Deliverer könnte sich als Wetter-App tarnen, die zum Funktionieren unbedingt Netzwerkzugriff benötigt. Da Android prinzipiell den Datenaustausch zwischen zwei Anwendungen unterbinden kann, bedienen sich die Malware-Forscher eines Umwegs über die Einstellungen für den Vibrationsalarm. Änderungen an diesen Einstellungen werden an beliebige Applikationen kommuniziert.

Soundminer versteckt die Kreditkarteninformationen in Daten, die den Werten des Vibrationsalarms gleichen. Der Deliverer wandelt die Daten zurück und schickt sie dann zum wartenden Hintermann.

Die Malware-Forscher wollen ihren Schädling nicht veröffentlichen. Daher bleibt die Hoffnung, dass wahre Schadsoftware-Autoren mangels Kopiervorlage auch in Zukunft mit weniger Raffinesse – Sprachanalyse in Echtzeit auf einer vergleichsweise schwachbrüstigen Hardware ist eine beachtliche Leistung – ans Werk gehen.

6.4 Auch Rootkits im Angebot

Bereits Mitte 2010 zeigten die beiden IT-Sicherheitsforscher Nicholas Percoco und Christian Papathanasiou das nach ihrer Auskunft erste Rootkit für Android. Sinn und Zweck der Demonstration: aufzuzeigen, wie leicht sich ein solches Vorhaben umsetzen lässt. Die Forscher nannten das Demo-Rootkit Mindtrick und konzipierten es so, dass es sich vor anderen Prozessen wie einem Virenscanner verstecken kann.

Das ist ein Rootkit
Rootkits sind Schädlinge oder Teile von Schädlingen, die bestimmte Vorgänge auf dem infizierten PC oder Smartphone unsichtbar machen. Dazu gehören beispielsweise Anmeldevorgänge des Angreifers und natürlich die Schadsoftware selbst. Letzteres ist entscheidend, damit Antivirensoftware die Schadsoftware nicht entdeckt. In der Regel öffnen Rootkits dem Angreifer auch eine Hintertür, sodass er jederzeit aus der Ferne Zugriff auf den infizierten PC bekommt.

Installiert würde das Rootkit über eine noch zu findende Schwachstelle in Googles Handybetriebssystem – wobei Mindtrick genau wie die zuvor beschriebenen Schädlinge auch in einer vermeintlich legitimen Android-App versteckt werden kann. Diese müsste zur Installation des versteckten Schädlings zwar Administratorrechte vom Anwender anfordern, wie Tests von Forschern mit einer gefälschten Wetter-App belegten, sind Nutzer hierzu aber nur allzu gern bereit.

Ist das Rootkit installiert, wird es durch einen eingehenden Anruf des infizierten Handys von einer zuvor festgelegten Nummer aktiviert. Da Mindtrick weitreichende Systemrechte hat (es läuft auf Ebene des Kernels), kann es ein Klingeln bei diesem Anruf genauso unterdrücken wie die Anzeige des Anrufs im Display. Nach dem Aktivieren baut das Rootkit einen Rückkanal (Reverse Shell) zum Rechner des Angreifers auf, sodass dieser aus der Ferne sämtliche SMS oder auf dem Android-Gerät gespeicherte Kontakte auslesen kann.

Auch die aktuellen Koordinaten des Smartphones liest Mindtrick aus. Hierzu muss der Zugriff auf das GPS-Modul zuvor jedoch von einer Anwendung wie Google Maps angefordert und vom Handybesitzer bestätigt worden sein. Was wiederum leicht machbar ist, wenn sich das Rootkit in einer Software versteckt, die angeblich Ortungsdienste nutzt.

Perfide: Der Angreifer kann aus der Ferne auch ausgehende Anrufe starten. Betrüger könnten so unbemerkt von ihnen betriebene teure Sex-Telefondienste anrufen und auf Kosten der Opfer Umsätze generieren.

Bild 6.6: Wächter: Norton Smartphone Security ist eine Antivirensoftware, die Smartphones vor Schädlingen schützen soll. (Bild: Symantec)

Zwar existiert Antivirensoftware für Android, beispielsweise von Lookout (Lookout Mobile) oder Symantecs Norton Smartphone Security for Android. Beide Programme entdeckten Mindtrick jedoch nicht, und wahrscheinlich hat Schutzsoftware auch in Zukunft einen schweren Stand: Das Rootkit versteckt sich mittels seiner Rechte vor sämtlichen anderen Prozessen. Auch ein Löschen aus der Ferne, wie es Google bereits in der Praxis großflächig angewandt hat, um bösartige Apps nachträglich zu entfernen, nützt nichts. Denn der Löschvorgang wirkt – höchstwahrscheinlich – nur auf Anwendungsebene des Systems, nicht aber auf Kernelebene.

Den beiden Mindtrick-Machern zufolge ließe sich eine Schadsoftware, die aufgebaut ist wie Mindtrick, sehr leicht blockieren: Die Smartphone-Hersteller müssten das System lediglich anweisen, ausschließlich von ihnen selbst digital signierte Module zu akzeptieren. Als Mindtrick entwickelt wurde, waren solche Checks auf den Handys nicht zu finden.

6.5 Schadsoftware huckepack

Die Smartphone-Sicherheitsexperten von Lookout Software haben im Rahmen des App-Genome-Projekts über 500.000 Apps für Googles Android-Betriebssystem und Apples iOS analysiert. Neben verschiedenen interessanten Statistiken – Anzahl der kommerziellen Apps, Anzahl neuer Apps und so weiter – brachte die automatische Untersuchung auch zutage, dass insbesondere beim Download aus alternativen App-Stores Gefahr droht.

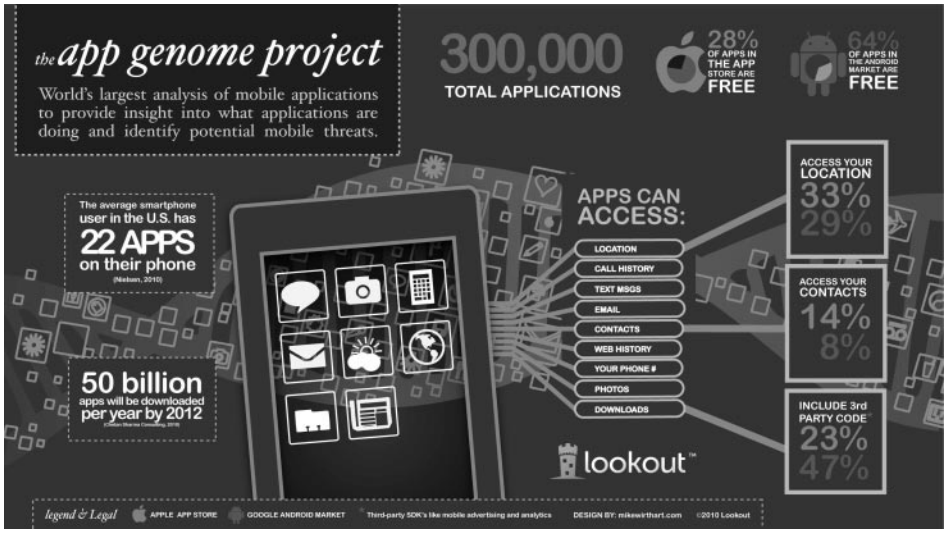

Bild 6.7: Untersucht: Für das Projekt App-Genome hat Lookout Software Hunderttausende von Smartphone-Anwendungen unter die Lupe genommen und ihre genaue Funktionsweise analysiert. (Bild: Lookout Software)

Dies sind die Anwendungssammlungen, die nicht von Google (Android Marketplace) oder Apple (App Store innerhalb des iTunes Store) direkt betrieben werden. In der Android-Welt haben Smartphone-Besitzer ganz generell Zugriff auf diese Sammlungen, die iOS-Geräte (iPad, iPhone, iPod touch) müssen zuvor per Jailbreak entsperrt werden. Dann bietet die durch den Jailbreak installierte Anwendung Cydia Zugriff auf Anwendungen, die nicht von Apple geprüft und freigegeben wurden.

Im Rahmen von App-Genome untersuchte Lookout Software von insgesamt vier alternativen App-Märkten. Im Fall der beiden inoffiziellen Android-App-Sammlungen gab es eine interessante Entdeckung: Eine große Menge an Apps, die auch im Android Marketplace zu finden sind, tauchten in den alternativen Sammlungen ebenfalls auf. Über 10 Prozent dieser Anwendungen wurden jedoch neu paketiert oder nicht vom eigentlichen Entwickler in die alternativen Märkte hochgeladen. Aber auch im offiziellen Google-Angebot fanden sich mit Schadcode verseuchte Apps. So hat Google nach Angabe von Lookout Security im Juni 2011 34 mit Schadcode infizierte Android-Apps aus seinem Market entfernt. Die Apps wurden nach Schätzungen bis zu 120.000 Mal heruntergeladen.

Auffällig waren beispielsweise von einem Entwickler namens RSX hochgeladene Apps, die durch die Bank unschuldige Titel trugen wie »System Utilities«. De facto übertragen die Anwendungen im Hintergrund aber Daten an die Domain *mobilespylogs.com*. Ein Viertel dieser Apps verlangte während der Installation zudem nach mehr Zugriffsrechten auf dem Smartphone als das Original.

Zu diesen erweiterten Zugriffsrechten gehören die Angabe über den momentanen Aufenthaltsort, Adressbuchinformationen, Gerätezustand, Zugriff aufs Internet und auch die Fähigkeit, Telefonate initiieren zu können. Einige der Anwendungen konnten laut Lookout auch als Sprungbrett für nicht Legales dienen, wie beispielsweise zum

Banner-Ad-Betrug, für Raubkopien oder auch als Träger für Malware. Die Experten entdeckten den Android-Trojaner Gemini in 50 verschiedenen neu paketierten Anwendungen.

In den alternativen App-Stores für iPhones finden sich vor allem raubkopierte Apps (88 Prozent). Lookout zufolge repräsentieren die entdeckten Anwendungen knapp 8 Prozent aller kommerziellen Apps im offiziellen App Store. Im iTunes Store wurden keine bösartig manipulierten Anwendungen entdeckt. Offensichtlich ist Apples rigorose Prüfung aller eingereichten Apps erfolgreich beim Aussortieren merkwürdiger Anwendungen.

Laut Lookout-Experten kam es erst einmal vor, dass eine vermeintlich legitime Anwendung einen versteckten Zweck hatte: Dem 15-jährigen Nick Lee gelang es, seine Anwendung Handy Light – die durch Erleuchten des Displays aus dem iPhone einen Taschenlampenersatz machen soll – im App Store unterzubringen. De facto war in Handy Light aber eine Funktion versteckt, mit der sich das von den Mobilfunkprovidern bis vor Kurzem verpönte Tethering, also das Nutzen des iPhones als UMTS-Modem für ein Notebook oder einen PC, bewerkstelligen lässt.

6.6 Das Handy als Wanze

Immer wieder geistern Berichte durch Presse und Internet, dass aus Smartphones perfekte Abhörwerkzeuge gemacht werden können. Zumeist ist dann von Geheimdiensten oder zumindest ausgefuchsten Polizeieinsätzen die Rede.

Das quasi jeder Techniklaie aus einem beliebigen fremden Mobiltelefon eine Wanze machen kann, bleibt oftmals unerwähnt. Das dazu notwendige Werkzeug – sprich, die Spionagesoftware – gibt es käuflich im Internet zu erwerben, beispielsweise unter dem Namen FlexiSpy.

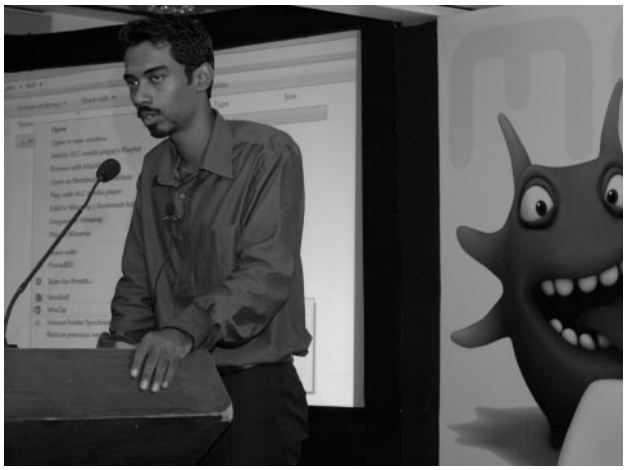

Bild 6.8: Gehackt: Der indische Smartphone-Experte Atul Alex hat eine Software geschrieben, mit der sich die extrem weit verbreiteteten Symbian-S60-Smartphones in Wanzen verwandeln lassen. (Foto: Uli Ries)

Es gibt die Software auch gratis: Der indische Hacker Atul Alex hat sich an der Betriebssoftware für Symbian-S60-Smartphones zu schaffen gemacht und ihr eine Hintertür

eingepflanzt. Er modifizierte die Version 5 der Originalsoftware – die beispielsweise auf Geräten läuft wie Nokia 5800, Nokia X6, Nokia 5530XM, Sony Ericsson Satio oder Sony Ericsson Vivaz – und integrierte eine Hintertür. Wird diese vom Angreifer genutzt, kann er alle Funktionen der Smartphones aus der Ferne steuern, inklusive der Kamera.

Glücklicherweise klappt die Installation der modifizierten Betriebssoftware nicht per Internet. Ein Angreifer muss das zu infizierende Smartphone stattdessen für einige Minuten in die Hände bekommen und etwa per USB-Kabel mit einem Rechner verbinden. Einmal installiert, meldet sich die Backdoor beim Angreifer per Funkschnittstelle (WLAN, UMTS) und überträgt die aktuelle IP-Adresse des Geräts, sodass der Angreifer es per Netzwerk ansprechen kann. Ist er erst einmal mit dem infizierten Gerät verbunden, kann er auch weitere Anwendungen installieren lassen.

Zentrale Funktion der Wanzensoftware: Auslesen der E-Mail-, Telefonlisten- und SMS-Speicher, Anfertigen von Screenshots oder Fotografieren mit der integrierten Digitalkamera des Smartphones sowie Mitschneiden von Telefonaten. Übertragen werden die geklauten Daten per GPRS/UMTS oder WLAN auf einen Server des Angreifers.

Der Programmierer hat die Wanze so konzipiert, dass sie vom Smartphone selbst nicht entdeckt werden kann. Eine Zusatzsoftware würde sie zwar aufspüren, kann die Spionagekomponente aber nicht beenden. Entfernen lässt sich das Einfallstor laut Atul Alex nur durch ein Überschreiben der Betriebssoftware mit der Originalsoftware von Symbian.

6.7 Wie schützt man sich und sein Smartphone?

Allen oben beschriebenen Smartphone-Schädlingen ist eines gemeinsam: Sie werden vom Anwender selbst installiert. Kein mobiler Malware-Vertreter kann derzeit ein Smartphone ohne Zutun des Anwenders infizieren. Damit unterscheiden sich die Schädlinge erheblich von den aus der Windows-Welt bekannten Verwandten. Denn die verbreiten sich zum großen Teil nur durch das Öffnen einer infizierten Webseite durch den Anwender.

Smartphone-Trojaner reisen entweder huckepack auf legitimen, von bösartigen Hackern modifizierten Apps, oder die Malware-Schreiber erfinden die vermeintlich harmlose App gleich selbst und schieben dieser den Schadcode unter.

Für Smartphone-Nutzer bedeutet dies: Vorsicht bei der Installation von Anwendungen. Insbesondere dann, wenn nicht der offizielle Google-Download-Store benutzt wird, sondern eine der alternativen App-Sammlungen. Denn bei Letzteren wird längst nicht so konsequent nach gefährlichen Applikationen gesucht wie bei Google.

Schutz vor einer Infektion finden Sie, indem Sie solche App-Sammlungen meiden und Anwendungen bevorzugt aus dem offiziellen App Market beziehen. Vorsicht ist auch geboten, wenn zwei Apps mit gleichem – oder zumindest sehr ähnlichem – Namen in den App-Sammlungen auftauchen, die Produzenten aber verschieden sind. In diesem Fall hat ein Malware-Verteiler eine legitime App modifiziert und erneut in den App-Store geschickt. Eine von beiden Apps ist also gefälscht und gefährlich. Hier hilft es, sich

die Bewertungen der Anwendungen anzusehen. Die legitime App dürfte erheblich mehr Urteile gesammelt haben – die zudem hoffentlich auch positiv ausfallen.

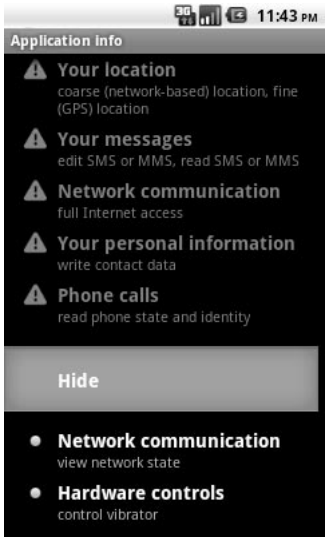

Bild 6.9: Vorsicht: Wenn eine Android-Anwendung während der Installation nach auffällig vielen Rechten fragt, lauert die Gefahr, sich einen Trojaner einzufangen. (Bild: F-Secure)

Ein weiterer wichtiger Punkt: Anwender sollten prüfen, welche Berechtigungen die jeweilige Applikation bei der Installation einfordert. Während des Vorgangs erscheint auf Android- und auch Blackberry-Geräten ein Fenster mit den angeforderten Rechten. Wenn beispielsweise eine Wetterberichtsanwendung SMS verschicken will, ist Vorsicht geboten. Warum sollte sie das tun, welchen legitimen Zweck hätte diese Funktion? Ähnliches gilt für ein vermeintliches Spiel: Warum sollte es Zugriff auf das Adressbuch des Telefons bekommen?

Außerdem ist eventuell die Installation einer Antivirenanwendung sinnvoll. Zwar sind die verfügbaren Programme längst nicht so ausgereift wie ihre PC-Geschwister. Aber angesichts der noch relativ überschaubaren Anzahl an Schädlingen haben die Beschützer auch noch vergleichsweise leichtes Spiel. Aber Vorsicht: Es sind bereits Android-Trojaner aufgetaucht, die ganz gezielt Antivirensoftware täuschen. Die bösen Buben haben das Wettrennen also schon aufgenommen.

13 Sicherer Umgang mit Internetbrowsern

Den Internetbrowsern kommt eine besondere Bedeutung zu. Und nicht nur die ständige Kommunikation über das Internet macht sie zu einem beliebten Einfallstor für Angriffe und Infektionen. Auch verlagern immer mehr Anbieter ihre Dienste und Serviceangebote ins Internet – Stichwort Cloud. Durch diese Verschiebung gewinnt vor allem der Browser auch weiterhin zunehmend an Bedeutung. Und wenn man sich die ihm übertragenen Aufgaben sowie seinen Einsatzbereich und Funktionsumfang genauer betrachtet, kann man ihn sicher schon heute als Miniaturausgabe eines Betriebssystems bezeichnen.

Neben dem wohlüberlegten Handeln beim Arbeiten beziehungsweise Surfen im Internet ist also ein frisch geschliffenes Handwerkszeug in Form eines aktuellen Internetbrowsers mit aktualisierten Erweiterungen die wichtigste Voraussetzung, um einer generellen Ausnutzung durch Cyber-Kriminelle bestmöglich zu entgehen.

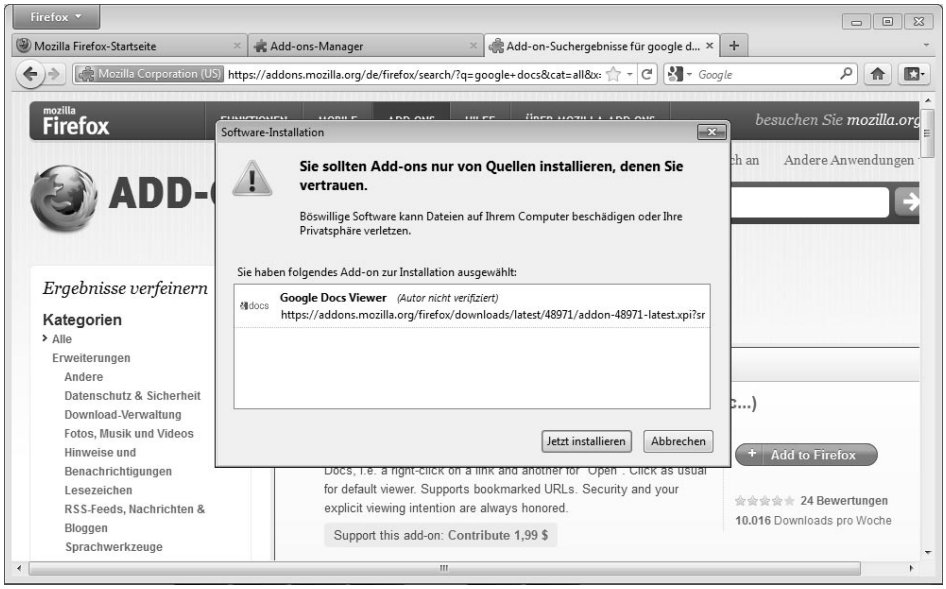

Bild 13.1: Herunterladen und Installieren eines Firefox-Add-ons über eine *https*-gesicherte Verbindung.

13.1 Internetbrowser up to date halten

Auch wenn Überwachungsprogramme, wie der zuvor bereits vorgestellte Personal Software Inspector von Secunia, eine veraltete Browserversion nun sicherlich umgehend melden würden, möchte ich Ihnen die automatischen Update-Einstellungen und die Möglichkeiten der manuellen Überprüfung in den verschiedenen Browsern dennoch nicht vorenthalten. Nicht zuletzt, weil die Aktualisierung von Browsererweiterungen wie Add-ons oder Plug-ins leider nicht immer automatisch erfolgt.

Im Folgenden betrachten wir vorrangig die Sicherheitsfunktionen aktueller Browser. Seien Sie daher also bitte nicht irritiert, sollten Ihnen einige der Darstellungen des Internet Explorer 9 oder des Firefox 5 nicht sofort bekannt vorkommen. Während die jüngsten Browserversionen von Mozilla Firefox und Google Chrome sowohl für Mac und Linux als auch für alle Windows-Versionen erhältlich sind, bleibt eine Installation des Internet Explorer ausschließlich Benutzern von Windows Vista oder Windows 7 vorbehalten. Der Safari-Browser von Apple hingegen lässt sich nicht nur auf einem Windows-PC installieren, sondern natürlich auch auf einem Mac oder einem iPhone sowie auf nahezu allen Apple-Produkten.

13.1.1 Neue Browser-Versionen suchen und finden

Auf der Suche nach neuen Programmversionen bedient sich der Internet Explorer der im Betriebssystem integrierten Update-Funktion von Windows. Daher lassen sich im Internet Explorer selbst keine Einstellungen zur Suche nach Sicherheitsupdates finden oder anpassen. Alle Updates für den Microsoft-Browser werden bei aktivierter Auto-Update-Funktion also immer vom Betriebssystem gesucht und, falls verfügbar, beim Herunterfahren mit installiert.

Auch Apple Safari nutzt auf einem Mac die hauseigene Update-Funktion von Apple. Unter Windows verwendet der Apple-Browser das bei seiner Installation automatisch mit installierte Programm Apple Software Update. Hier sollte man allerdings darauf achten, dass die Häufigkeit der Update-Suche im Zeitplan des Einstellungsmenüs (unter *Bearbeiten*) auf *täglich* gesetzt ist. Zudem lässt sich bei Safari im Menü des Browsers unter *Einstellungen* auch noch ein Haken für das automatische Aktualisieren der Erweiterungen setzen.

Google Chrome wiederum bietet weder bei seiner Installation noch im nachfolgenden Betrieb die Möglichkeit an, irgendwelche Update-Einstellungen anzupassen. Der Google-Browser sucht regelmäßig automatisch im Hintergrund nach neuen Sicherheitsupdates. Wird er fündig, zeigt er die Verfügbarkeit einer neueren Version als Pfeil neben dem Schraubenschlüssel in der Symbolleiste des Browsers an. Die Installation beziehungsweise Aktualisierung erfolgt dann automatisch. Über das Schraubenschlüsselsymbol gelangen Sie im Übrigen auch zum Menüpunkt *Info zu Google Chrome*. Beim Abruf dieser Information wird dann aber nicht nur die aktuelle Versionsnummer des Browsers angezeigt, sondern auch eine manuelle Suche nach aktuelleren Versionen ausgelöst.

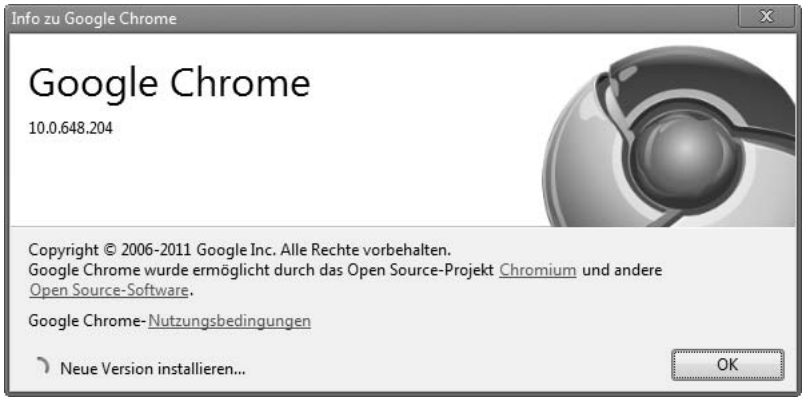

Bild 13.2: Die Infoabfrage in Google Chrome löst eine manuelle Update-Suche aus.

Beim Mozilla Firefox findet man die Update-Einstellungen unter der Rubrik *Erweitert* im Register *Update*. Hier lässt sich dann auch festlegen, ob die automatische Suche nach Updates nur für den Browser selbst oder auch für Add-ons und Suchmaschinen durchgeführt werden soll. Findet der Firefox bei seiner regelmäßigen Überprüfung eine aktuellere Version, bietet er diese ebenso zur Installation an wie neuere Versionen von verwendeten Browsererweiterungen.

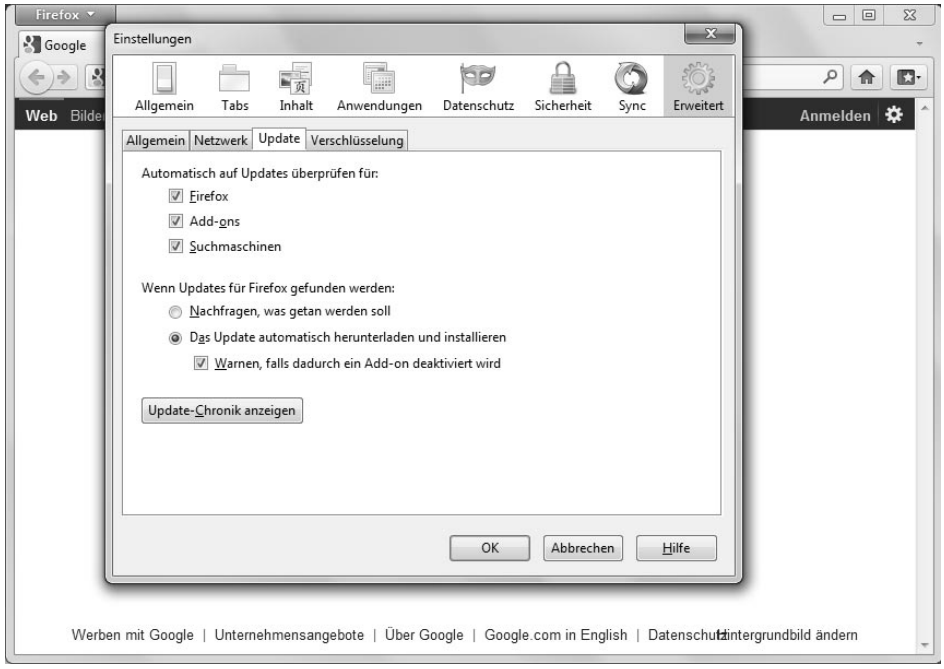

Bild 13.3: Die Update-Optionen im Mozilla Firefox 5.

Da einige Browser zur Installation von Updates administrative Rechte benötigen, ist es generell ratsam, sich in regelmäßigen Abständen auch direkt mit diesen erhöhten Rechten am Computer anzumelden. Neben den entsprechenden Aktualisierungen der Pro-

gramme können dann auch allgemeine Sicherheitsüberprüfungen oder Anpassungen an den Computereinstellungen vorgenommen werden.

Browsererweiterungen up to date halten
Alle hier beschriebenen Internetbrowser bieten zwar die Möglichkeit, die installierten Add-ons zu verwalten, aber nicht zwangsläufig diese auch (automatisch) zu aktualisieren. Prüfen Sie also regelmäßig die Aktualität Ihrer Browsererweiterungen.

13.2 Zeigen Sie bitte Ihren Ausweis

Sichere Webseiten erkennen Sie in der Regel am »s«. Und zwar am »s« hinter »http«. Denn mit SSL (Secure Socket Layer) geschützte Webseiten – gängig beim Onlinebanking und Onlineshopping – machen aus dem unverschlüsselten *http* das sichere *https*. Sie sollten streng darauf achten, dass Sie persönliche Daten oder andere extrem sensible Informationen (wie zum Beispiel Benutzername und Passwort, Kreditkartennummern oder PINs und TANs fürs Onlinebanking etc.) nur auf Webseiten eingeben, die SSL zur sicheren Datenüberragung benutzen.

Neben dem »s« ist bei manchen Browsern ein Symbol in Form eines kleinen gelben Vorhängeschlosses ein Indiz dafür, dass Sie sich gerade auf einer Webseite befinden, die SSL-verschlüsselt mit Ihnen kommuniziert. Dieses Symbol finden Sie bei älteren Browsern in der unteren Statusleiste und bei neueren vorwiegend im Bereich der Adressleiste oben.

Stellen Sie sich eine SSL-gesicherte Verbindung zwischen zwei Computern einfach als eine Art geschlossenen Tunnel mit jeweils nur einer Öffnung an jedem Ende vor. Eine Nachricht, die also an einer Seite dieses Kanals hineingeschickt würde, könnte nur von dem Teilnehmer am anderen Endpunkt gelesen werden. Selbst oder gerade wenn dieser Tunnel durch die halbe Stadt führen würde, könnten Personen, die diese Kommunikation (unbefugt) abfangen würden, nur den Tunnel selbst beziehungsweise die darin hin- und hergeschickten Nachrichtenpakete, nicht aber den Inhalt der übermittelten Nachrichten sehen.

Was bei der Kommunikation von zwei derart verbundenen Computern technisch im Hintergrund abläuft, braucht aber nicht weiter zu interessieren, um die folgende (warnende) Beschreibung dennoch zu verstehen: Die Eingabe von sensiblen Daten auf einer durch SSL gesicherten Webseite stellt grundsätzlich nur sicher, dass die Daten zwischen Ihrem Computer und einer Webseite verschlüsselt (und somit für Dritte nicht lesbar) übertragen werden. Ein simples SSL-Zertifikat bestätigt auch nur die Identität (also in der Regel nur die Internetadresse) der Webseite.

Ein solches Zertifikat gibt keinen Aufschluss darüber, ob es sich hierbei nun um die offizielle Webseite eines Herstellers, Diensts oder Anbieters handelt. Und ein solches Zertifikat gibt Ihnen leider auch keine Auskunft darüber, ob es sich beim Betreiber der Webseite um eine seriöse Firma, Organisation oder Person handelt.

Eine solche Infokarte gibt lediglich Auskunft darüber, wie sich eine Person nennt und über welche Kontaktdaten sie erreichbar ist. Wenn man also davon ausgeht, dass die

abgedruckte Telefonnummer und die Adresse wirklich existieren, wäre damit aber noch nicht zweifelsfrei sichergestellt, wer bei einem spontanen Besuch oder Anruf am anderen Ende anzutreffen wäre.

Bild 13.4: Ein einfaches SSL-Zertifikat bestätigt nicht, wer eine Webseite betreibt.

13.2.1 Ein amtlicher Ausweis fürs Web

Damit kommen wir nun, der Analogie folgend, zur Identifizierung mithilfe eines amtlichen Personalausweises: eines SSL-Zertifikats mit erweiterter Überprüfung (engl. Extended Validation, kurz EV). Um ein solches EV-Zertifikat für seine Webseite zu erhalten, muss ein Antragsteller ein standardisiertes Verfahren durchlaufen, bei dem er eine Reihe definierter Angaben zur Überprüfung seiner Identität an eine ausstellende Behörde, eine sogenannte Zertifizierungsstelle (engl. Certificate Authority, kurz CA), übermitteln muss.

Generelles Ziel dieser erweiterten Überprüfung ist es, Kriminellen die Beschaffung eines solchen vertrauenswürdigen Zertifikats zu erschweren beziehungsweise gänzlich unmöglich zu machen. Gerade im Kampf gegen sogenannte Daten-Phisher stellt die erweiterte Überprüfung bei der Beantragung eines EV-SSL-Zertifikats eine wichtige Hürde dar, die ein nachweislich nicht vertrauenswürdiger Antragsteller sicherlich nicht so schnell überwinden könnte.

Hinzu kommt, dass Anträge für normale SSL-Zertifikate vorwiegend maschinell abgearbeitet werden und die Vergabe von manchen Anbietern sehr lax gehandhabt wird, also sehr oft ohne die eigentlich auch hier vorgeschriebene Überprüfung des Antragstellers. Ein Grund mehr für Internetkriminelle, sich zur Absicherung ihrer zwielichtigen Machenschaften ein normales SSL-Zertifikat zu besorgen. Getreu dem Motto: Wenn

man schon illegal fremde Daten abgreift, dann sollen sie wenigstens sicher beim Datenhändler am anderen Ende ankommen.

Im Gegensatz dazu bietet Ihnen eine EV-SSL-gesicherte Webseite also nicht nur eine verschlüsselte und damit sichere Datenverbindung an, sondern Sie erhalten neben diversen Angaben zum Webseiteninhaber auch die Bestätigung der Zertifizierungsstelle, dass die wahre Identität des Antragstellers verifiziert wurde und implizit auch dass er als vertrauenswürdig angesehen wird. In der Regel verwenden vor allem Banken, Bezahldienste, Onlineshops etc. solche »Webseitenzertifikate erster Klasse«.

13.3 Bunte Adressleisten: Farben für Ihre Sicherheit

Moderne Internetbrowser können die Stufen der Vertrauenswürdigkeit einer Webseite visuell durch eine Art Ampel darstellen. So muss sich der Anwender nicht erst im Detail über eine Seite informieren, sondern kann beim Aufruf bereits an der Farbe der Adressleiste erkennen, welchen Vertrauensstatus die aufgerufene Webseite genießt. Wir möchten nachfolgend die individuellen Darstellungsweisen der einzelnen Browser etwas vernachlässigen und Ihnen vorrangig das Sicherheitsprinzip dieser Ampelfarben anhand der beiden meistgenutzten Internetbrowser Firefox und Internet Explorer erläutern.

13.3.1 Weiß: leer wie die nackte Wand

Eine durchgängig weiße Adressleiste im Internetbrowser bedeutet, dass die aufgerufene Webseite keine Informationen zur Identifikation an den Browser übermittelt hat. Die Kommunikation zwischen Ihrem Rechner und der Webseite ist in der Regel unverschlüsselt oder nur zu Teilen verschlüsselt. Generell sollten Sie auf solchen (ungesicherten) Webseiten niemals vertrauliche Daten eingeben.

13.3.2 Teils weiß, teils blau: nicht zwingend vertrauenswürdig

Sollte eine Webseite nun eine SSL-Verschlüsselung anbieten, ändert sich beim Internet Explorer farblich zwar (noch) nichts, dafür erscheint in der weiterhin weißen Adresszeile nun aber ein kleines Vorhängeschloss. Ein Klick auf dieses – zuerst graue, beim Berühren mit dem Mauszeiger dann goldgelbe – Symbol legt Ihnen nun weitere Informationen zur Verschlüsselung der Verbindung und gegebenenfalls auch zur Webseite selbst dar.

Bild 13.5: Über das Schlosssymbol kommen Sie beim Internet Explorer zur Webseitenidentifizierung.

Beim aktuellen Firefox 5 ist ein solches Symbol hinter der nun blau eingefärbten und deutlich verbreiterten Schaltfläche zur Webseitenidentität versteckt. Beim Klick auf dieses Element erscheinen der jetzt ebenfalls blau gefärbte Passkontrolleur sowie die Schaltfläche *Weitere Informationen*. Dahinter finden Sie dann eine weitere Schaltfläche, die Sie zum Zertifikat und den darin enthaltenen Informationen führt.

Bild 13.6: Temporäre Fehlermeldung beim Überprüfen einer ansonsten vertrauenswürdigen Webseite.

13.3.3 Gelb: Überlegt handeln!

Färbt sich die Adressleiste des Internet Explorer gelb ein, hat der Browser die aufgerufene Webseite als verdächtig eingestuft. Das kann verschiedene Gründe haben. Bestenfalls konnte »nur« die Echtheit des Zertifikats gerade nicht bestätigt werden; schlimmstenfalls handelt es sich um eine verdächtige Phishing-Seite. In jedem Fall sollte diese Farbe, wie im Straßenverkehr auch, bei Ihnen zu einer erhöhten Aufmerksamkeit führen. Am besten verschieben Sie Ihren Besuch zur eigenen Sicherheit einfach um ein paar Stunden oder Tage, bis der Betreiber das Problem gegebenenfalls gelöst hat oder die Zertifizierungsstelle wieder verlässlich erreichbar ist.

Bild 13.7: Webseite und SSL-Zertifikat passen nicht zueinander.

13.3.4 Rot: Finger weg!

Ein sehr ähnliches Verhalten zeigen Internetbrowser, wenn die aufgerufene Webseite nachweislich als betrügerisch oder infizierend eingestuft wurde und somit eine akute Bedrohung darstellt. In diesem Fall färbt sich die Adresszeile direkt beim Aufruf der Webseite rot ein, und/oder es erscheint eine entsprechende Warnmeldung im Browserfenster. Ein sicheres Zeichen, dass mit der Webseite etwas ganz und gar nicht stimmt. Die Webseite wurde offenbar vom Dienstanbieter oder Browserhersteller bereits in sogenannte Filterlisten aufgenommen, aus denen der Browser nun diese Warnung bezogen hat.

Ein Grund für eine rote Adressleiste kann auch sein, dass das verwendete Sicherheitszertifikat nicht zur Webseite passt beziehungsweise mit deren Adresse nicht übereinstimmt. Das wäre dann der Versuch, ein gestohlenes SSL-Zertifikat zur Absicherung einer fremden Webseite zu missbrauchen.

Wer jetzt trotz ausdrücklicher Warnung des Browsers dennoch mit dem Laden einer offenbar derart betrügerischen oder gefährlichen Webseite fortfährt, sollte sich der potenziellen Gefahr und ihrer Folgen entsprechend bewusst sein.

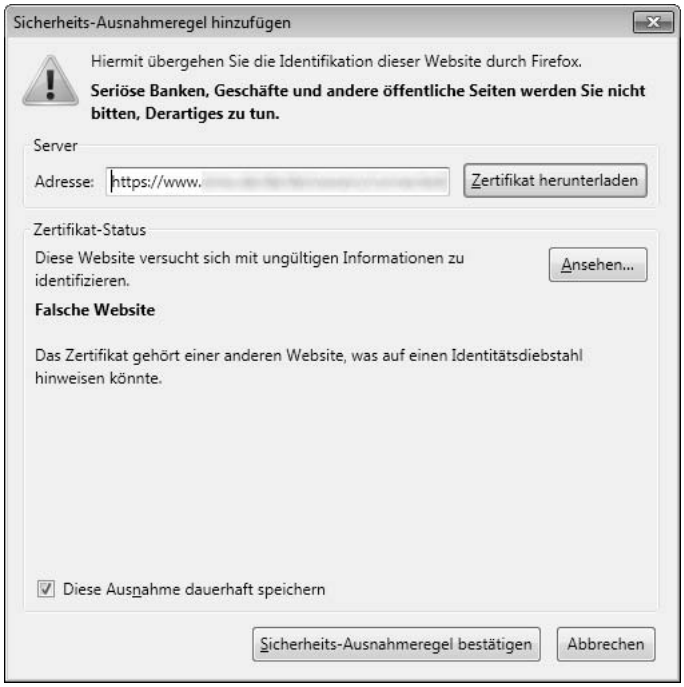

Bild 13.8:
Legen Sie eine Sicherheitsausnahmeregel nur an, wenn Sie sich absolut sicher sind.

13.3.5 Grün: Allseits gute Fahrt!

Das Beste, was Ihnen beim Surfen im Internet nun also passieren kann, ist, dass sich beim Aufruf einer Webseite der Site Identity Button des Firefox grün einfärbt – oder auch die Adresszeile des Internet Explorer. Für diese Darstellungsform wird häufig die englische Bezeichnung »Green Address Bar« verwendet. Aber auch andere Browser verhalten sich hier vorbildlich. So bietet z. B. Google Chrome gut sichtbar auf der linken Seite der Adresszeile eine grün gefärbte Schaltfläche an, die bei Bedarf und auf Mausklick weiterführende Informationen zu einer EV-SSL-verschlüsselten Seitenverbindung preisgibt. Einzig Safari verhält sich hier eher neutral und bietet diese Informationen sehr dezent über eine weiße Schaltfläche mit grüner Schrift auf der rechten Seite der Adresszeile an.

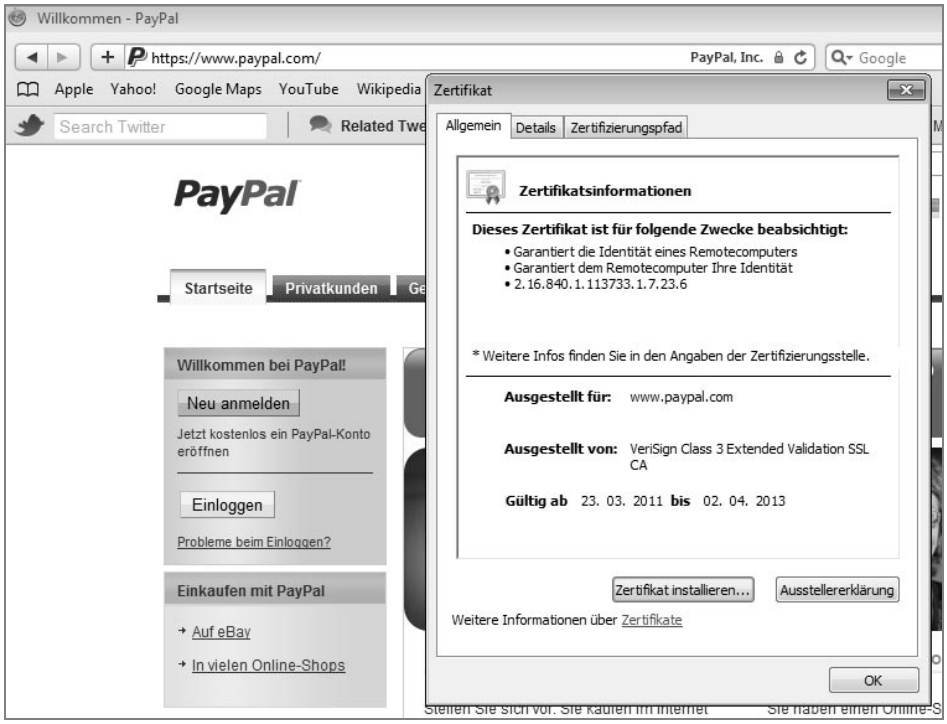

Bild 13.9: Hinweis auf ein EV-SSL-Zertifikat und weiterführende Informationen bei Safari.

Domänenhervorhebung in der Adressleiste
Nicht nur für Webseiten, die über kein digitales Sicherheitszertifikat zur Anzeige ihrer Identität verfügen, bieten einige Browser eine Funktion an, die ebenso simpel wie nützlich erscheint: die Domänenhervorhebung (engl. Domain Highlighting). Hierbei stellt der Browser in der Adressleiste immer nur den Teil einer Webadresse deutlich sichtbar dar, der die eigentliche Domäne bildet, umgangssprachlich also den Namen der Webseite. Ein Anwender kann somit auch bei einer extrem langen Zeichenfolge in der Adressleiste des Browsers immer auf einen Blick erkennen, auf welcher Webseite er sich tatsächlich gerade befindet. Während der Internet Explorer diese Funktion standardmäßig mitbringt, lassen sich andere Browser hierfür über entsprechende Add-ons nachrüsten. Diese Funktion ersetzt sicherlich in keinem Fall ein digitales Sicherheitszertifikat, sie kann den Anwender aber sehr effektiv dabei unterstützen, sogenannte Phishing-Webseiten zu erkennen und einen solchen Angriff somit abzuwehren, vor allem wenn die Webseite bislang noch nicht gemeldet wurde.

13.4 Filter und Referenzlisten

Wie Sie vielleicht schon ahnen, bilden verschiedene Filter und Referenzlisten immer wieder die Entscheidungsgrundlage dafür, ob eine Webseite oder Datei aus dem Internet nun vertrauenswürdig oder gefährlich ist. Auch in Verbindung mit Problemen oder

Fehlern bei Webseitenzertifikaten ergeben sich so die oben beschriebenen gelben und roten Adressleisten beziehungsweise gleichbedeutende Warnmeldungen der Browser.

Bei solchen Filtern zum Schutz vor gefährlichen oder betrügerischen Inhalten aus dem Internet handelt sich in der Regel fast immer um eine Kombination aus lokal auf dem Rechner hinterlegten Listen und Echtzeitüberprüfungen. Die Basis stellen dabei Listen mit verdächtigen Webseiten und Dateien dar, die vom Anbieter des Filters beziehungsweise des Diensts (engl. Service) im Hintergrund erstellt, fortwährend aktualisiert und dann regelmäßig an den Rechner beziehungsweise Internetbrowser übermittelt werden.

Findet sich beim Aufruf der Webseite in diesen Listen ein Verweis auf eine potenzielle Gefahr, werden beim Anbieter weitere Informationen und gegebenenfalls aktualisierte Informationen über diese Seite angefragt. Zum durchgängigen Schutz ist es hier durchaus eine übliche Praxis, dass alle angefragten Webseiten zur Überprüfung an den Anbieter des Schutzfilters übermittelt werden. Da im Rahmen einer solchen Überprüfung in der Regel aber nur die Adressen der Webseiten und keine Informationen über den Anwender oder dessen Computer übertragen werden, ist dies datenschutztechnisch noch vertretbar. Google bietet mit seinem Safe Browsing Service zum Beispiel einen solchen Dienst an, der in Safari, Chrome und Firefox schon länger seinen Einsatz findet.

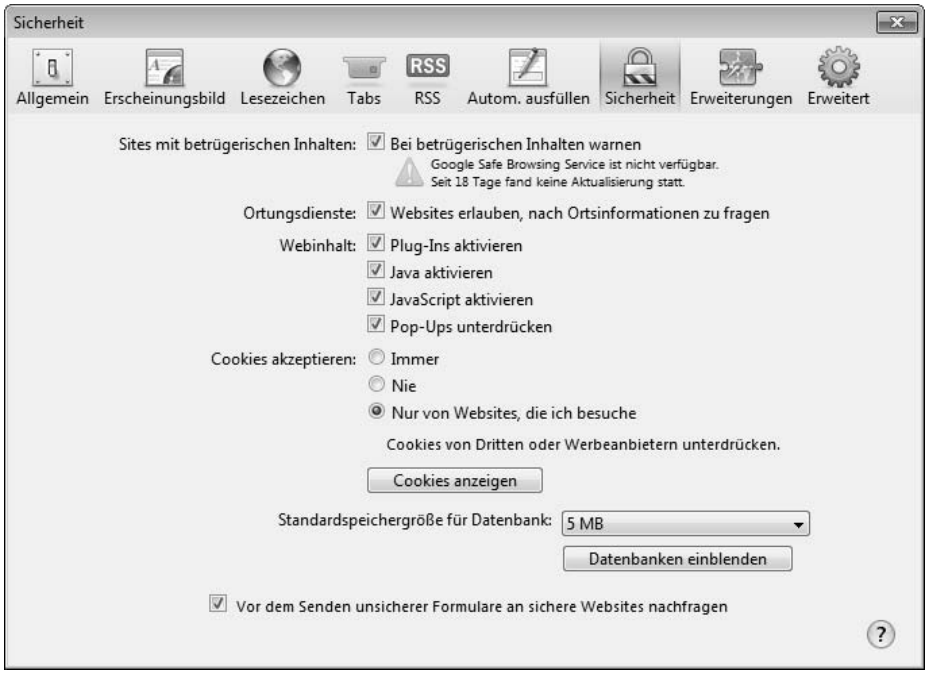

Bild 13.10: Safari nutzt zum Schutz vor betrügerischen Webseiten den Safe Browsing Service von Google.

Und auch wenn ein Browser in seiner lokal vorgehaltenen Referenzliste einmal keine Informationen über eine vorliegende verdächtige Datei oder Webseite findet, kann er die Seite überprüfen lassen: Er schickt die Datei beziehungsweise deren Hashwert (eine

Art anonymisierte ID) an seinen Hersteller, Dienstanbieter oder dessen Partner und lässt sie dort auf ihr Gefahrenpotenzial hin untersuchen.

Bild 13.11: Es können auch eigentlich seriöse Dateien unter Verdacht geraten.

Mit einer Kombination aus solchen Schutztechniken im Gepäck lassen sich nun also große Teile der Internetlandschaft in Freund und Feind einteilen. Microsoft nennt seine Allzweckwaffe im Kampf gegen Malware und Betrug beim Internet Explorer zum Beispiel »SmartScreen-Filter«. Im Firefox läuft die Verwendung einer entsprechenden Filterliste unter der Bezeichnung »Phishing-Schutz«. Mozilla gibt hierzu an, dass sich Firefox bis zu 48-mal am Tag, also ca. alle 30 Minuten, dazu eine aktualisierte Liste vom Server herunterlädt.

13.4.1 Blacklists und Whitelists

Sie merken schon: Je nach Browserhersteller unterscheiden sich die Filter mehr oder weniger deutlich in ihren Bezeichnungen und auch im Funktionsumfang. Was manche Hersteller nun allerdings etwas großspurig mit Marketingsätzen wie

»Der […] Filter bietet einen Rundum-Schutz vor digitalen Schädlingen und Phishing.«

beschreiben, könnte leicht den Verdacht nahelegen, dass man sich die Verwendung eines Antivirenprogramms grundsätzlichen sparen kann, wenn man den richtigen Internetbrowser benutzt. Dazu gibt es aber ein ganz klares Nein. Es gibt hier sicherlich Redundanzen bei den Schutzfunktionen und gegebenenfalls auch identische Quellen bei der Informationsbeschaffung, aber solche Schutzfilter können ein vollwertiges Antivirenprogramm nicht ersetzen.

Falls in solchen Filterlisten nun ausschließlich schädliche oder betrügerische Webseiten beziehungsweise Dateien aufgeführt sind, spricht man von einer Blacklist, also einer Art Sperrliste. Bei Kindersicherungen, Familien- oder Jugendschutzfiltern handelt sich dagegen häufiger um sogenannte Whitelists. Denn hier ist es oftmals sinnvoller, den Kindern oder Jugendlichen über Positivlisten ganz gezielt ausgesuchte Webseiten beziehungsweise sichere und vor allem dem Alter angemessene Inhalte freizugeben, als endlos lange Sperrlisten von dem zu erstellen, was sie nicht sehen oder aufrufen dürfen.

Oftmals wird der Schutzfilter innerhalb der Produktpalette eines Herstellers natürlich auch mehrfach verwendet. So kommt der SmartScreen-Filter nicht nur beim Surfen mit dem Internet Explorer, sondern auch beim Herunterladen einer Datei oder beim Onlineabruf von E-Mails über die webbasierte Version des Microsoft Mail-Programms zum Einsatz. Bei Anzeichen für eine Infektion oder Verdacht auf Betrug oder Manipulation würde der Internet Explorer die Anzeige der Webseite beziehungsweise des betroffenen Webseitenbereichs umgehend blockieren. Der Microsoft Download Manager hingegen würde eine verdächtigte Datei zuerst melden und dem Anwender dann die

Entscheidung überlassen, ob er den Download abbrechen beziehungsweise löschen oder die verdächtigte Datei wirklich ausführen oder speichern möchte.

13.4.2 Cross-Site-Scripting-Filter

Einige Browser der jüngsten Generation bieten nun auch einen Filter zum Schutz gegen eine weitere sehr gefährliche Angriffsform, das sogenannte Cross-Site-Scripting. Sowohl der Internet Explorer 9 als auch der Firefox 5 stellen eine solche Filterfunktion derzeit bereit. Der Schutzmechanismus ist standardmäßig aktiv und lässt sich zum Schutz des Anwenders in der Regel auf normalem Weg auch nicht ausschalten.

Bei einer Cross-Site-Scripting-Attacke muss ein Angreifer einen verwundbaren Server im Internet finden, auf dem er seinen Angriffscode platzieren kann. Die »Eingabe« eines solchen bösartigen Skripts, das oft nur aus wenigen Zeilen Code besteht, könnte dann zum Beispiel als Rezension oder Anzeige getarnt über das Formularfeld einer Webseite erfolgen, die auf diesem Server betrieben wird. Wenn der Server nun beim Abspeichern die eingegebenen Informationen nicht überprüft, ist der Angreifer schon fast am Ziel. Er muss jetzt nur noch warten und hoffen, dass möglichst bald möglichst viele Benutzer seine Bewertung oder Anzeige über die Webseite dieser ansonsten eigentlich vertrauenswürdigen Internetplattform aufrufen.

Bei jedem Aufruf (also Betrachten) dieses manipulierten Webseiteneintrags wird der bösartige Programmcode dann auf den Computer eines Opfers übertragen und dort mit den Rechten des angemeldeten Benutzers ausgeführt. Schlimmstenfalls ist dies ein Benutzer mit administrativen Rechten. Je nach Absicht des Angreifers beziehungsweise Gestaltung seines Schadcodes könnte er jetzt zum Beispiel Daten vom angegriffenen Rechner stehlen und so die Identität des Opfers übernehmen, um dann in dessen Namen weiterhin online zu agieren.

Wie Sie sicher bemerkt haben, wurde das Opfer bei dieser Angriffsform vom Angreifer nicht direkt, sondern indirekt über die Eingabe und erneute Ausgabe des schädlichen Skripts ausgekontert. Der Angriff lief also über verschiedene Webseiten – sozusagen cross-site – eines eigentlich vertrauenswürdigen Servers. In Kombination mit dem verwendeten bösartigen Skript ergibt das den Namen des Angriffs: Cross-Site-Scripting.

Browser, die einen Filter gegen derartige Angriffe anbieten, prüfen zum Schutz des Anwenders alle Inhalte, die nicht von der jeweils bsuchten Website stammen, auf ihre Vertrauenswürdigkeit. Vereinfacht ausgedrückt, lässt sich der Browser dabei von der aufgerufenen Webseite mitteilen, für welche Inhalte sie sich verbürgen kann und für welche nicht. Die Übertragung von tendenziell unsicheren Elementen wird vom Browser dann entsprechend übersprungen beziehungsweise unterbunden.

Falls Sie weiterführende Informationen zum Thema Cross-Site-Scripting suchen, können wir Ihnen die Webseite *http://bit.ly/hatGMo* empfehlen. Dort finden Sie als Einstieg ein sehr gut und verständlich aufbereitetes Videotutorial.

13.4.3 Jugendschutz und Kindersicherungen

Wenn Sie einen Computer mit Mac OS X 10.5 oder höher oder Windows 7 benutzen, können Sie, unabhängig vom verwendeten Internetbrowser, eine Betriebssystemfunktion aktivieren, die sich Kindersicherung beziehungsweise Jugendschutz nennt. Auch viele Sicherheitsprogramme bieten eine solche Funktion mit an. Hierbei können Sie festlegen, welche minderjährigen Benutzer den Computer zu welchen Uhrzeiten benutzen und welche Programme und welche Spiele mit welchen Altersfreigaben sie in dieser Zeit verwenden dürfen.

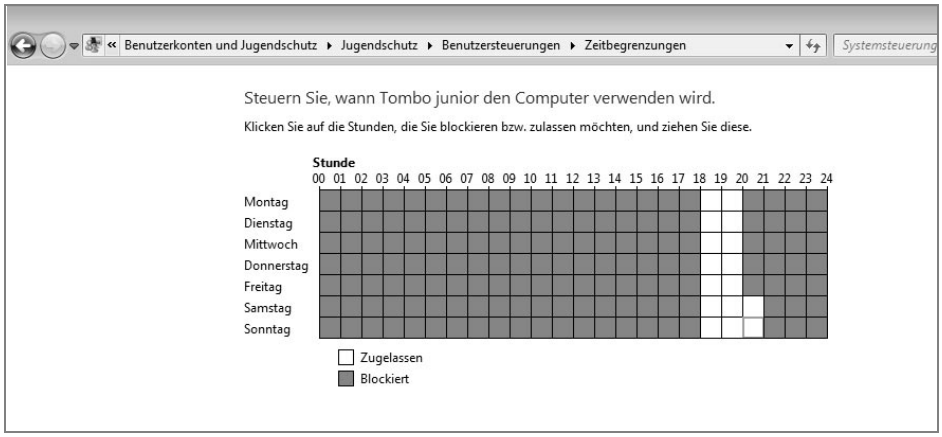

Bild 13.12: Die Benutzung des Computers ist nur in der Zeit von 18 bis 20 Uhr (beziehungsweise 21 Uhr am Wochenende) möglich.

Zur Aktivierung beziehungsweise Anpassung der Jugendschutz-Einstellungen in Windows gehen Sie über die *Systemsteuerung* und dort weiter zu *Benutzerkonten und Jugendschutz*. Unter Verwendung von administrativen Rechten können Sie dann für ausgewählte Benutzer an Ihrem Computer die Jugendschutz-Funktion aktivieren und Ihren Vorgaben entsprechend einstellen. Auch beim Mac können Sie nach der Eingabe von Name und Passwort eines Administrators den Punkt Kindersicherung in den Systemeinstellungen aktivieren.

13.5 Private Sitzungen – Anonymität wahren

Sie merken vielleicht schon, dass wir uns zwischenzeitlich etwas in Richtung Schutz der Privatsphäre bewegt haben. Getreu dem Motto »Bloß keine Spuren hinterlassen!« bieten einige Browser auch zu diesem Zweck entsprechende Schutzfunktionen an: das Surfen im sogenannten privaten Modus und die Verwendung von Filtern zum Schutz der Privatsphäre. Auch wenn die beiden Funktionen von der Bezeichnung her scheinbar die gleichen Ziele verfolgen, so unterscheiden sie sich in ihrer Ausrichtung doch klar voneinander. Während das Surfen im privaten Modus eher den Schutz der Privatsphäre auf einem gemeinsam genutzten PC zum Ziel hat, richten sich die Filter zum Schutz der Privatsphäre vorwiegend gegen externe Inhaltsanbieter, die sehr an Ihrem Surfverhalten interessiert sind.

13.5.1 Teil 1: Die interne Anonymität

Die im Firefox als privater Modus (engl. Private Browsing) bezeichnete Funktion wird im Internet Explorer InPrivate-Browsen genannt. Trotz leichter Unterschiede im Namen wird durch diese Funktion in beiden Browsern bestmöglich sichergestellt, dass beim Surfen im Internet keine Informationen über Ihre sogenannte Browsersitzung (engl. Session) lokal auf dem Rechner gespeichert werden. Dies ist vor allem dann relevant, wenn mehrere Personen gemeinsam an einem Computer arbeiten oder sogar über dasselbe Benutzerkonto im Internet surfen. Das könnte zum Beispiel an einem gemeinsam genutzten Familien-PC oder einem Rechner im Internetcafé der Fall sein oder auch an einem frei zugänglichen PC in einer Hotellobby.

Um auf solchen Computern die Privatsphäre jedes einzelnen Benutzers entsprechend zu schützen, muss der Browser bei aktiviertem Modus folgende Punkte sicherstellen:

- Dass keine Chronik, also kein Verlauf von besuchten Webseiten, angelegt wird.
- Dass der Computer auch keine Offlineversionen von besuchten Webseiten »cacht«, also temporär zwischenspeichert.
- Dass sämtliche in Formularfelder eingegebene Passwörter oder sonstige Angaben inklusive Suchanfragen nicht behalten werden.
- Dass keine Cookies angenommen und gespeichert werden, die Webseiten zur Wiedererkennung gern auf den Computern der Besucher ablegen.

Der Browser versucht beim Surfen im privaten Modus, die Speicherung aller zuvor genannten Informationen von vornherein zu unterbinden oder diese mit Beenden des Modus beziehungsweise Schließen des Browserfensters automatisch zu löschen. Auf dem Computer lassen sich dann keine oder nur noch sehr wenige Spuren der Internetaktivitäten eines Anwenders finden. Nur so wird der Privacy-Filter seinem Namen einigermaßen gerecht, der in Insiderkreisen auch gern als »Pornofilter« bezeichnet wird.

Je nach Browser werden dennoch auch bei einer Surfsession im privaten Modus beispielsweise hinzugefügte Lesezeichen (oder Feeds) oder die Namen von heruntergeladenen Dateien im Download-Manager abgelegt.

Die Verwendung des InPrivate-Modus zeigt der Internet Explorer durch eine blaue Schaltfläche links von der Adresszeile an. Der Firefox hingegen signalisiert die Aktivierung des privaten Modus anhand einer Farbänderung seiner Menüschaltfläche von standardmäßig Orange zu Lila.

Bild 13.13: Der private Modus beim Firefox und das InPrivate-Browsen beim Internet Explorer im Vergleich.

Egal mit welchem Browser und für welchen Zweck Sie einen Privacy-Filter nun auch einsetzen – ein paar Dinge dürfen Sie dabei nicht verwechseln und in keinem Fall unterschätzen: Beim privaten Surfen am Arbeitsplatz können Netzwerkadministratoren Ihre Ausflüge ins Internet auch bei aktivierten Filtern sehr genau verfolgen. Und auch zu Hause im eigenen Netzwerk kann Ihr Internetanbieter sehr genau protokollieren, auf welchen Seiten Sie zuletzt im Internet unterwegs waren.

Eine wirkliche Anonymität kann hier nicht erreicht werden. Es geht bei dieser Funktion vielmehr darum, Familienmitgliedern oder Dritten, die Zugang zu Ihrem Rechner oder Ihrem Benutzerkonto haben, grundsätzlich möglichst wenige Informationen über Ihre Surfgewohnheiten preiszugeben.

13.5.2 Teil 2: Die externe Anonymität

Kommen wir nun zur zweiten der beiden oben erwähnten Funktionen zum Schutz der Privatsphäre und damit zu einer Funktion, die ich für wesentlich interessanter halte als den privaten Surfmodus: den sogenannten Tracking-Schutz.

Diese Schutzfunktion nannte sich beim Internet Explorer in Version 8 noch InPrivate-Filterung, ein Name, der zwangsläufig zu Verwechslungen mit der zuvor beschriebenen Funktion InPrivate-Browsen führen musste. Im aktuellen Internet Explorer 9 ist die Bezeichnung dieses nach extern gerichteten Schutzfilters nun schon aussagekräftiger: Tracking-Schutz. Und genau das bietet diese Funktion auch – einen Schutz(filter), der verhindert, dass Webseiten zu viel über das persönliche Surf- beziehungsweise Nutzungsverhalten eines Anwenders herausfinden können.

Beim Besuch einer Webseite sind Ihnen sicherlich schon oftmals Banner, Werbeeinblendungen, Anzeigen oder andere Inhalte aufgefallen, die teilweise seitenfremd erscheinen, also offenbar nicht wirklich zur Webseite gehören. Derartige Inhalte oder auch sogenannte Zählpixel stammen dann sicher nicht vom Betreiber der Webseite, sondern von Dritten, also sogenannten Inhaltsanbietern oder Drittanbieterwebseiten. Das Gefährliche daran ist, dass diese Inhalte, neben ihrer Werbebotschaft oder ihrem Informationsgehalt, auch dazu verwendet werden können, Daten darüber zu sammeln, welche Webseiten Sie wann und wie oft besuchen.

Stellen Sie sich einfach vor, Sie würden in der Stadt ausführlich einkaufen und zwischendurch immer wieder essen gehen. Und stellen Sie sich weiter vor, an jedem Geschäft oder Restaurant, das Sie betreten, würden Mitarbeiter von ein und demselben Marktforschungsinstitut stehen, die Ihr Erscheinen ganz unauffällig aus dem Augenwinkel heraus protokollieren. Ein derart angefertigtes Bewegungsprofil Ihrer Person wäre dann sicherlich extrem detailliert und sehr aussagekräftig, aber vor allem von Ihnen sicherlich nicht erwünscht.

Und auch im Internet lässt sich die beste Auswertung über Ihr Nutzungsverhalten dann erstellen, wenn Ihnen auf verschiedenen Webseiten, die Sie besuchen, mehrfach Inhalte von ein und demselben Inhaltsanbieter angezeigt werden. So werden Sie als Webseitenbesucher in Ihren Surfgewohnheiten besonders »gläsern« für diesen Anbieter.

Um den digitalen Verfolgern diese Transparenz aber nun weitgehend zu verweigern, können Sie den Tracking-Schutzfilter einsetzen, der im Internet Explorer 9 einmalig aktiviert werden muss und dabei einen Schwellenwert für das Erfassen solcher Inhalte festsetzt.

Rufen Sie hierzu im Menü des Internet Explorer über *Extras* den Punkt *Sicherheit* und dann *Tracking-Schutz* auf. Markieren Sie im Fenster der Add-on-Verwaltung Ihre personalisierte Liste und klicken Sie dann auf *Einstellungen* beziehungsweise *Einstellungen für diese Liste*. Beide Wege führen zur selben, nachfolgend dargestellten Übersicht.

Lassen Sie sich nicht davon irritieren, dass Ihr Tracking-Schutzfilter zu Beginn noch leer ist. Er wird sich im Laufe der Zeit mit den Namen von verschiedenen Inhaltsanbietern füllen.

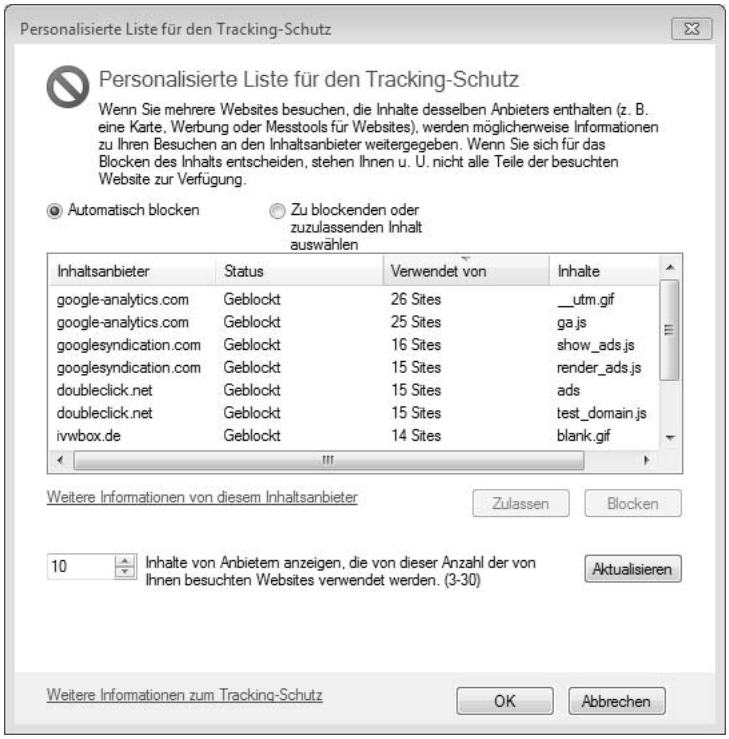

Bild 13.14: Entscheiden Sie, welchen Inhaltsanbieter Sie blocken oder zulassen möchten.

Wie Sie in der Abbildung sehen, ist beim Tracking-Schutz standardmäßig ein Schwellenwert von *10* eingetragen. Das bedeutet, dass vom Datenschutzfilter des Internet Explorer nur Inhaltsanbieter erfasst und angezeigt werden, deren Inhalte Ihnen öfter als zehnmal auf verschiedenen Webseiten angezeigt werden. Sie können diesen Wert nach Belieben zwischen *3* und *30* festlegen. Bestätigen Sie Ihre Eingabe mit *OK*, und der Tracking-Schutz des Internet Explorer 9 ist aktiv.

Der so aktivierte Datenschutzfilter beginnt sofort damit, die von Ihnen besuchten Webseiten zu analysieren und sie auf Fremdinhalte zu prüfen. Findet er dabei mehr spionierende Inhalte eines einzigen Anbieters auf unterschiedlichen Webseiten, als Sie im Filter als Wert angegeben haben, wird er Ihnen diese beim nächsten Öffnen des Tracking-Schutzes in der Liste anzeigen. Sie können dann entscheiden, ob Sie alle erfassten Anbieter automatisch blockieren oder das für jeden Inhaltsanbieter einzeln festlegen möchten.

Vorbereitete Tracking-Schutz-Listen
Falls Sie nicht warten möchten, bis sich der Filter im Laufe der Zeit automatisch mit verschiedenen neugierigen Inhaltsanbietern füllt, können Sie sich auch fertige Listen aus der Internet Explorer Gallery herunterladen. Rufen Sie hierfür die Webseite *http://bit.ly/iL3Xyy* auf. Dort finden Sie derzeit knapp eine Handvoll vorbereiteter Tracking-Schutz-Listen verschiedener Unternehmen und Organisationen. Klicken Sie auf der Webseite neben der ausgewählten Tracking-Schutz-Liste auf die Schaltfläche *Hinzufügen* und schließen Sie den Vorgang ab, indem Sie im nun erscheinenden Dialogfenster des Internet Explorer die Schaltfläche *Liste hinzufügen* anklicken. Die meisten Listen sind eine Mischung aus Black- und Whitelists, also eine Kombination aus Verbots- beziehungsweise Sperrlisten und Listenbereichen, die ausgewählte Webseiten explizit als erlaubt aufführen. Beachten Sie, dass für die Pflege und Inhalte der Listen ausschließlich die jeweiligen Hersteller verantwortlich sind.

So geschützt, sollte zukünftig auch eine intensive Nutzung des Internets sowie von Facebook und anderen sozialen Netze Ihre Privatsphäre nicht mehr gefährden.

Stichwortverzeichnis

Uli Ries / Tombo Mörgenthaler

Das inoffizielle facebook-Buch

Wie Sie Betrugsversuche erkennen und sich davor schützen

Freunde, Fotos, Links, Nachrichten: Facebook ist für seine Millionen Nutzer zur zentralen Surf-, Mail- und Chat-Schaltstelle geworden. Und damit auch zum lohnenden Angriffsziel für Betrüger und Online-Kriminelle. Dieses Buch zeigt knallhart recherchiert, wie Cyber-Gauner versuchen, an Ihre Daten und Ihr Geld zu kommen, und wie Sie sie davon abhalten können!

▶ **Angriffsvielfalt: Alte Gefahren und neue Tricks**

Auch per Facebook laufen Sie Gefahr, sich Viren einzufangen und Opfer von Spam- und Phishing-Attacken zu werden. Das Neue und gleichzeitig Gemeine daran ist, wie diese Angriffe auf Facebook ausgeführt werden. Hier erfahren Sie, mit welchen Tricks Online-Gauner Ihre Log-in-Daten stehlen, den Gefällt mir-Button entführen und Sie dazu bringen, Ihren Rechner selbst zu infizieren.

▶ **Alarm für Handys und Macs: Nicht nur Windows-PCs sind bedroht**

Facebook läuft überall. Da es eine reine Internet-Plattform ist, spielt das Betriebssystem keine Rolle, und für Android und iOS gibt es passende Apps. Ein Klick auf den falschen Facebook-Link kann üble Folgen haben. Gerade für Android-Handys gibt es mittlerweile Trojaner und Rootkits, die sich Zugang zu Ihren Daten verschaffen. Auch die bislang so sicheren Mac-Rechner werden rasch mit spezieller Schadsoftware infiziert, die besonders über Facebook angepriesen wird.

▶ **Facebook – aber sicher!**

Die Sicherheits-Einstellungen von Facebook sind nicht gerade besonders übersichtlich – hier bekommen Sie die entscheidenden Tipps, wie Sie nicht nur Facebook, sondern auch Ihren Browser und Ihren Rechner optimal absichern. Aber sichere Passwörter, Firewall und Virenscanner hin oder her – die wichtigsten Waffen gegen Betrügereien auf Facebook sind Ihr gesundes Misstrauen und Ihr gesunder Menschenverstand. Schlagen Sie den Online-Gaunern mit dem Wissen aus diesem Buch ein Schnippchen!

Aus dem Inhalt:

9 783645 601016

19,95 EUR [D]
ISBN 978-3-645-60101-6

Besuchen Sie unsere Website
www.franzis.de