KEINE CHANCE OHNE SCHUTZ

Der PCtipp hat sich unbekümmert und ohne Schutz ins Internet gewagt. In kurzer Zeit landeten zig Schädlinge auf unserem Computer. **Wir erklären, wo Sie die Hebel ansetzen müssen, damit Ihr PC garantiert sicher ist.**

VON RETO VOGT

Wer sich im Internet nicht schützt, erlebt eine böse Überraschung. Das zeigt ein Selbstexperiment: Uns interessierte, wie viel Schaden das Surfen ohne Antivirenprogramm und ohne andere Sicherheitsmassnahmen anrichtet, von welchen Webseiten die gefährlichsten Schädlinge stammen und welche Daten soziale Netzwerke wie Facebook sammeln. Das Ergebnis war verheerend: PCtipp fing sich in dem Experiment in wenigen Stunden Tausende von **Cookies** i, 2 **Trojaner** i, 3 Trojaner-Installer, 3 **Adware**-Programme i und 1 **Backdoor**-Tool i ein.

Das Experiment wurde in Zusammenarbeit mit der Schweizer Sicherheitsfirma OneConsult (www.oneconsult.com) durchgeführt. Dabei surften die PCtipp-Redaktoren Janis Berneker und Reto Vogt mit einem Windows-XP-Rechner und einem Windows-7-Computer ohne Viren-

Hintergrund

Schutzlos im Web – das Experiment

Wir führten unser Experiment in den Räumen des Schweizer Sicherheitsunternehmens OneConsult in Thalwil durch. Unsere beiden Notebooks stellten die Internetverbindung über einen **Proxyserver** i her, damit der Netzwerkverkehr überwacht werden konnte. System Nummer eins war mit einem nicht aktualisierten Windows XP sowie dem Internet Explorer 6 ausgerüstet. Auf dem zweiten Laptop lief ein aktuelles Windows 7 sowie der Internet Explorer 8. Auf beiden Geräten war kein Virenschutz installiert. Das Experiment dauerte ca. 6 Stunden. Ausgewertet hat die Daten OneConsult. Einen Auszug mit den interessantesten Ergebnissen finden Sie auf www.pctipp.ch mit Webcode **virenprotokoll** (Info zum PCtipp-Webcode, S. 16).

Janis Berneker, Redaktor

Reto Vogt, Redaktor

FOTO ISTOCKPHOTO

schutz im Internet. Sie besuchten verschiedenste Webseiten – von harmlosen News-Portalen bis zu dubiosen Download-Seiten. Alle Details zu den Testbedingungen lesen Sie in der Box links unten «Schutzlos im Web – das Experiment».

Ohne einen Virenschutz setzt man seinen Computer also sehr grossen Gefahren aus. In unserem Experiment zeigte sich aber auch, dass die Antiviren-Software zwar ein wichtiges, aber nur kleines Teil im Schutzpanzer des Rechners ist. Wir helfen Ihnen, in sieben Schritten Ihren Computer gegen alle grossen Internetbedrohungen effizient abzusichern.

Ausserdem verraten Jan Alsenz und Christoph Baumgartner von OneConsult im Interview auf S. 25, was sie bei der Auswertung des Experiments überraschte und was Gratisvirenprogramme im Vergleich mit der kostenpflichtigen Konkurrenz taugen.

Schritt 1: Datenschutz

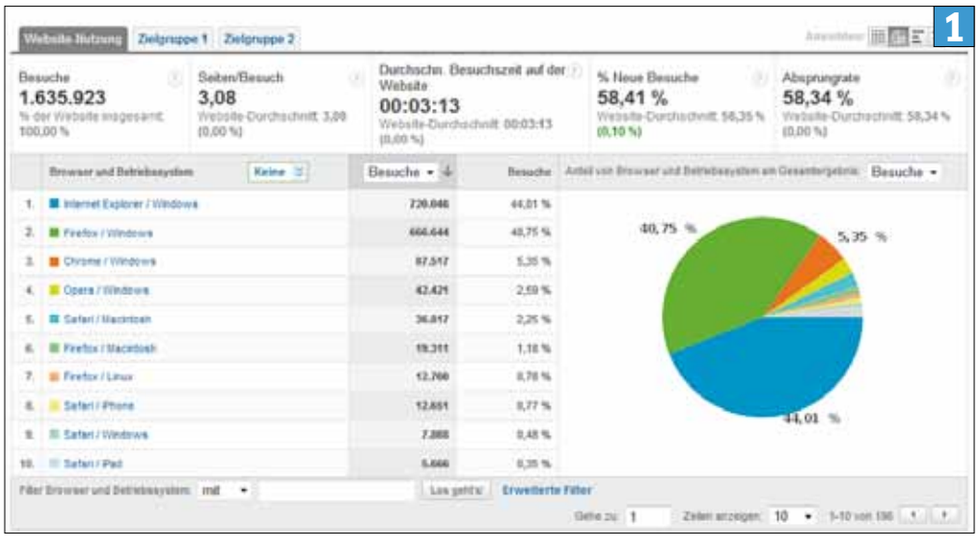
Wir starten unser Experiment ganz harmlos und surfen auf die News-Portale von 20 Minuten, Blick, PCtipp sowie Tages-Anzeiger. Schon hier laufen im Hintergrund 1800 Anfragen zu verschiedensten Seiten wie Werbung, Facebook etc. Sie beinhalten jedes Mal Benutzerinformationen zum verwendeten Betriebssystem, zur Browserversion, Herkunft und Sprache. Auch Bildschirmauflösung oder Internetgeschwindigkeit lassen sich auslesen. Darüber hinaus können die Seitenbetreiber den sogenannten Referrer einsehen. Er verrät, von wo die Anwender auf die Seite gelangen (zum Beispiel per Google-Suche oder durch Eintippen der Adresse).

Aber das ist noch nicht alles: Zusätzlich speichern die Webseiten auf jedem Besucher-PC eine kleine Datei, die in der Fachsprache Cookie heisst. Dank ihr wissen die Seitenbetreiber, wie lange die Nutzer die Seite besuchen und ob sie zurückkehren. Immerhin lässt sich von den Daten nicht auf die Identität schliessen. Die Seitenbetreiber werten die Infos allerdings statistisch aus. Das kann etwa so aussehen: 32 Prozent benutzen Windows 7, surfen mit dem Firefox und einer schnellen ADSL-Leitung, sprechen Deutsch, stammen aus der Schweiz und besitzen einen 24-Zoll-Monitor, **Screen 1**.

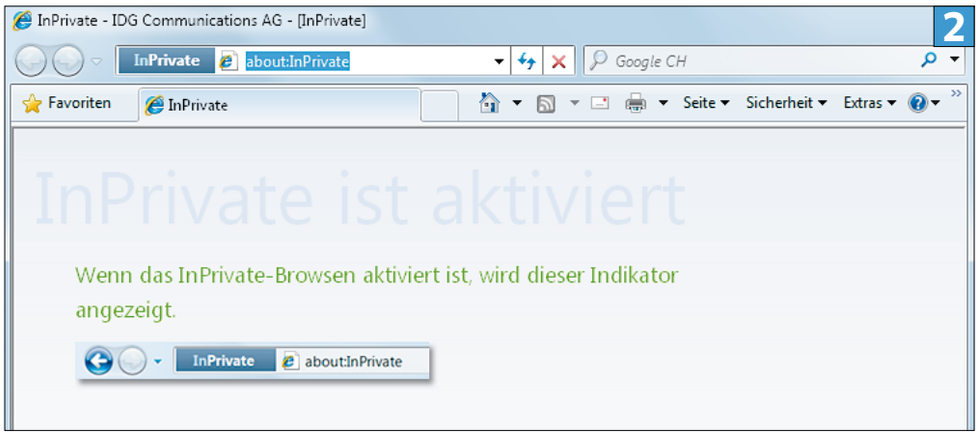
So schützen Sie sich: Das Surfen im Internet hinterlässt Spuren, die Webseitenbetreiber auswerten können. Wer das verhindern möchte, surft in seinem Browser am besten im «Privaten Modus». Dadurch werden das Abspeichern von Cookies, Verlauf etc. verhindert; das Surftempo sinkt jedoch leicht. Ein anderer kleiner Nachteil: Einige Webseiten funktionieren womöglich nicht korrekt, weil sie zwingend Cookies erfordern.

Im Internet Explorer finden Sie den «Privaten Modus» unter SICHERHEIT/INPRIVATE-BROWSEN, **Screen 2**. Firefox-Nutzer klicken auf das Menü EXTRAS/PRIVATEN MODUS STARTEN.

Surfen Sie nicht im «Privaten Modus», können Sie die Cookies und weitere Surfspuren auch manuell löschen: Klicken Sie dazu im Internet Explorer aufs Menü SICHERHEIT/BROWSERVERLAUF LÖSCHEN, **SCREEN 3**. In Firefox steckt diese Option unter EXTRAS/NEUSTE CHRONIK LÖSCHEN.



Webseitenbetreiber können anhand von Cookies detaillierte Besucherstatistiken erstellen



Im «Privaten Modus» legt der Internet Explorer keinerlei Cookies auf der Festplatte ab

Schritt 2: Verschlüsselung

Bereits in der zweiten Phase des Experiments decken wir einen unerwarteten Missstand auf: Auf zahlreichen Webseiten werden beim Einloggen die Passwörter der Nutzer unverschlüsselt übertragen. Sie sind damit in einem öffentlichen WLAN problemlos von Dritten einsehbar. Betroffen sind nicht nur Gratisangebote wie etwa die Ausgangsportale Tilllate, Partyguide oder die Chat-Plattform Swisstalk. Auch die kostenpflichtigen Partnervermittlungsdienste FriendScout24 und das renommierte Parship übermitteln die Kennwörter unverschlüsselt.

Was bei Gratisdiensten meist wenig Schaden anrichtet, kann bei Bezahlangeboten richtig ins Geld gehen. Der Grund: Wer deren Premium-Dienste nutzen will, muss seine Kreditkartennummer hinterlegen. Wird das unverschlüsselt übertragene Passwort abgefangen, können sich die Diebe damit einloggen und im schlimmsten Fall die gespeicherten Kreditkarteninfos stehlen. ➜

Löschen Sie regelmässig sämtliche Spuren, die Ihr Webbrowser hinterlässt

Fachbegriffe

Cookie > Ein Cookie ist eine Datei mit Textinformationen, die vom Betreiber der Webseite ausgelöst und vom Webserver regelmässig an den Browser übertragen wird. Cookies enthalten unter anderem Informationen, die beim nächsten Besuch das Wiedererkennen des Nutzers erlauben.

Trojaner > Ein Trojaner ist ein Programm, das sich als etwas anderes getarnt in einen Computer schmuggelt. Manche Trojaner schnüffeln Benutzerpasswörter aus, die sie ins Internet übermitteln.

Adware > Gratisprogramm, das Werbung einblendet oder Software installiert, die Werbung anzeigt.

Backdoor > Meist Teil einer Software, der auf dem PC eine Hintertüre öffnet. Durch diese haben Dritte Zugang zum System oder zu Funktionen.

Proxyserver > Server, der als Vermittler zwischen dem lokalen PC und Webseiten dient. Er analysiert die Anfragen des lokalen Rechners, passt diese gegebenenfalls an und leitet sie weiter.

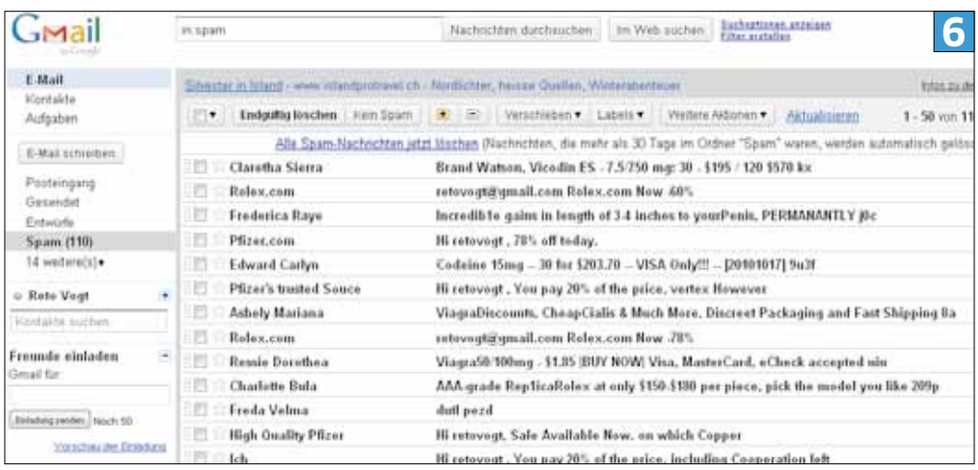
Die Passwörter auf der Plattform Parship wurden bis vor Kurzem unverschlüsselt übertragen

Parship antwortete auf die PCtipp-Anfrage, dass man daran sei, einen höheren Sicherheitsstandard fürs Login einzuführen. Mittlerweile ist dieser umgesetzt und die Logins sind alle verschlüsselt, **Screen 4**. Von FriendScout24 erhielten wir bis Redaktionsschluss keine Antwort.

So schützen Sie sich: Wie unser Experiment zeigt, werden Passwörter bei vielen Webdiensten unverschlüsselt übermittelt. Sie können so problemlos abgefangen werden. Deshalb ist es enorm wichtig, dass Sie für jeden Webdienst unterschiedliche Passwörter verwenden. Ansonsten können sich Diebe mit einem gestohlenen Passwort gleich in mehrere von Ihren Webdiensten einloggen.

Verwenden Sie für Ihre Passwörter nie bekannte Informationen wie Namen der Kinder, Geburtsdaten oder Ähnliches. Sehr gut geeignet ist eine Zeichenfolge aus Klein- und Grossbuchstaben, Zahlen und Sonderzeichen. Gut merken kann man sich etwa die Anfangsbuchstaben eines Satzes wie «Der Eiger ist ein Berg in den Alpen und 3970 Meter hoch». Hängen Sie an diesen noch einen Strichpunkt oder ein Komma, zum Beispiel: *DEieBidAu3970Mh;*

Besuchen Anwender Webseiten mit Facebook-Schnittstelle, weiss dies das soziale Netzwerk



Die zahlreichen Spammails nerven mittlerweile jeden Computeranwender

Ob eine Webseite Daten verschlüsselt übermittelt, lässt sich im Webbrowser oft erkennen. Lesen Sie dazu die Tipps von Schritt 6 auf S. 26.

Beim Verwalten vieler Passwörter hilft eine Software wie MyKeePass. Diese stellen wir in diesem Heft auf S. 57 genauer vor.

Schritt 3: Facebook überlisten

Nutzer des sozialen Netzwerks Facebook verraten bereits von sich aus viel Privates im Web. Ausserdem übergeben sie dem Betreiber des Netzwerks die Rechte an hochgeladenen Bildern, veröffentlichten Adressen sowie Telefonnummern und zeigen ihre Interessen sowie Hobbys, indem sie fleissig auf den «Gefällt mir»-Link klicken. Damit kann Facebook Profile von den Anwendern erstellen und passende Werbung einblenden.

Erstaunlich: Selbst als wir in unserem Experiment Facebook verliessen und auf eine andere Webseite wechselten, liess der Wissensdurst der Plattform nicht nach. Mithilfe von Cookies weiss Facebook, welche Seiten Anwender im Anschluss besuchen. Dazu muss nicht einmal ein Link innerhalb von Facebook angeklickt werden. Sogar wenn Anwender eine Webseite in einem neuen Browserfenster öffnen, wird dies der Plattform mitgeteilt. Immerhin beschränkt sich dies auf Webseiten, die eine Schnittstelle zu Facebook eingebaut haben – zum Beispiel die verbreiteten «Empfehlen»-Links, **Screen 5**. Das Ausloggen bei Facebook genügt übrigens nicht, um das Weiterverfolgen zu verhindern.

So schützen Sie sich: Facebook setzt beim Ausloggen ein Cookie, um aufzuzeichnen, welche Webseiten danach besucht werden. Möchten Sie nicht dauernd die Cookies löschen, um das zu verhindern? Dann hilft ein zweiter Browser. Surfen Sie Facebook beispielsweise nur mit dem Internet Explorer an. Andere Webseiten besuchen Sie hingegen mit dem Firefox-Browser. Dadurch kann das soziale Netzwerk zu den anderen besuchten Webseiten keine Informationen mehr sammeln.

Schritt 4: Spam dämmen

Wir machen die Probe aufs Exempel und prüfen, welche Gefahr von unerwünschten Werbemails (Spam) ausgeht. Wir klicken auf die Werbelinks von Luxusuhren- und Arzneimittelanbietern sowie für Penisvergrösserungen, **Screen 6**.

Eines ist klar: Dadurch bestätigen wir den Spam-Versendern die Echtheit unserer Mailadresse. Das wird die Menge an Werbemails beträchtlich erhöhen. Ansonsten stellen wir punkto Sicherheit keine Probleme fest: Auf den von uns besuchten Spam-Webseiten verstecken sich keine Schädlinge. Das heisst aber überhaupt nicht, dass dies bei allen Spam-Webseiten so ist.

Überraschend: Auf allen besuchten Werbewebseiten wurden verschlüsselte Bezahlmöglichkeiten (für Kreditkarte) angeboten. Allerdings sind die Einkäufe rechtlich problematisch: Ohne den Anbietern Böses zu unterstellen, dürfte es sich bei der Ware – insbesondere bei Luxusartikeln – um Fälschungen handeln. Ein weiteres Problem dabei: Seit rund zwei Jahren dürfen Zollbeamte offensichtlich oder mit hoher Wahr-

scheinlichkeit gefälschte Waren beschlagnahmen. Auch beim Kauf von Medikamenten im Internet, besonders im Ausland, gilt: Hände weg!

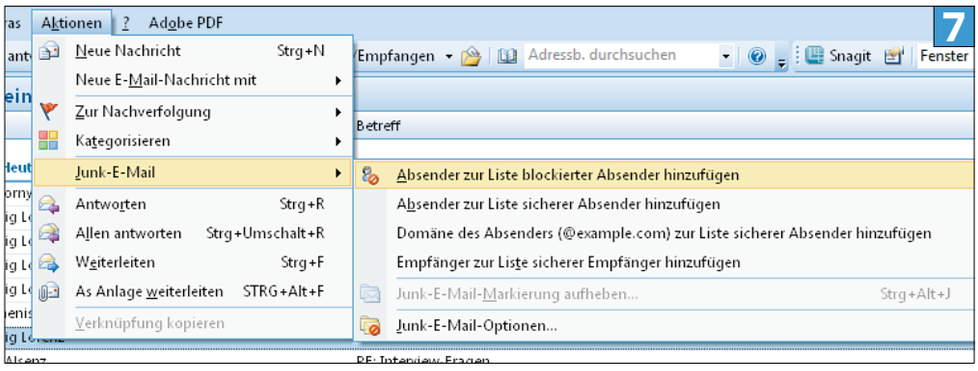
So schützen Sie sich: Obwohl wir in unserem Experiment keinen Schädling via Spam einfingen, kann dies passieren. Öffnen Sie deshalb in Mails aus unbekannter Quelle niemals die Anhänge, sondern löschen Sie diese umgehend. Klicken Sie auch nie auf Weblinks in Mails von Fremden.

Markieren Sie eintreffende Werbemails als Spam, damit das Mailprogramm diese beim nächsten Mal erkennt und automatisch in den entsprechenden Ordner aussortiert. In Microsoft Outlook finden Sie den Befehl unter Aktionen/Junk-E-Mail/Absender zur Liste blockierter Absender hinzufügen, **Screen 7**. Thunderbird-Nutzer klicken die entsprechende Nachricht an und drücken die Taste *J*.

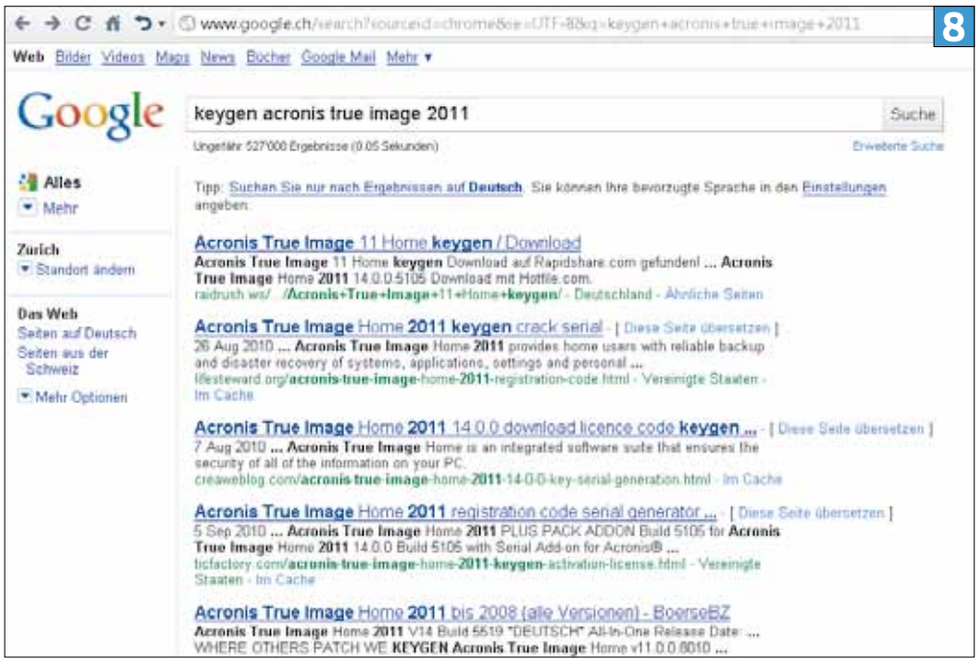
Schritt 5: nur gute Downloads

Musik-Downloads sind in der Schweiz legal. Egal, aus welcher Quelle sie stammen. In unserem Experiment laden wir jedoch keine Musik aus zwielichtigen Quellen herunter. Der Grund: Der Zufall spielt eine grosse Rolle, ob man sich einen Schädling einfängt, der als Musik-File getarnt ist.

Noch risikoreicher ist das Herunterladen von sogenannten Key-Generatoren oder Produktschlüsseln, um den Kauf von Software zu umgehen, **Screen 8**. Das ist nicht nur illegal. Zudem weiss man nie, ob ein Schlüsselgenerator wirklich nur das tut, was er sollte. Für die Programmierer ist es ein Leichtes, in das Tool Schadcode einzupflanzen. Was auf Download-Seiten für Key-Generatoren auch vorherrscht, ist Werbung für Pornoseiten mit teils sehr unappetitlichen ➜



Blockieren Sie Absender von Spam-Nachrichten, um diese künftig automatisch zu filtern



Es ist verboten, Key-Generatoren aus dem Internet herunterzuladen

Interview

«Den Unterschied macht Windows Defender»

***PCtipp:* Ihre Firma OneConsult hat unser Surfexperiment professionell ausgewertet. Ist Ihnen dabei vielleicht etwas Ungewöhnliches oder Unerwartetes aufgefallen?**
J. Alsenz/Chr. Baumgartner: Nein, eigentlich nicht. Die Möglichkeiten zum Tracking von Benutzerinformationen sind bekannt, die Wege der Malware auch. Nur dass Facebook beim Logout nochmals ein neues Cookie setzt, hat etwas erstaunt. Es ist möglich, dass dies andere grosse Seiten ebenfalls tun.

Nach Beendigung des Experiments waren beide Computer so stark verseucht, dass sie unbrauchbar wurden. Was können Anwender tun, die sich einen Schädling eingefangen haben?
Die Anwender müssen eine Recovery-Boot-CD oder einen USB-Stick mit einer solchen Funktion verwenden. Anschliessend lässt sich ein Backup des sauberen Systems einspielen. Falls dieses nicht vorhanden ist, lohnt es sich, den PC mit einer Antiviren-CD zu desinfizieren.

Unter Windows XP gab es doppelt so viele Trojaner wie auf dem Windows-7-PC. Lag das am Betriebssystem oder am veralteten Browser?
Weder – noch. Teilweise war die Schad-Software unter Windows XP nicht einmal mehr lauffähig. Den eigentlichen Unterschied hat die Software Windows Defender gemacht, die in Windows Vista/7 enthalten und aktiviert ist. Dieses Programm erkennt vor allem Adware und Spyware.

Bei unserem Experiment landeten sämtliche Schädlinge nur durch bewusste Benutzerinteraktionen auf dem Computersystem. Hätte Virenschutz-Software überhaupt etwas genützt?
Ja! Ein Virenscanner verhindert die Ausführung von gefährlichen Dateien und gibt eine Warnung aus. Wer nach einer Meldung des Virenscanners eine heruntergeladene Datei immer noch ausführt, ist selbst schuld.

Heute konkurrieren Gratis-Antivirenlösungen wie Avira AntiVir oder Microsoft Security Essentials mit kostenpflichtigen Antivirenprogrammen. Wo liegen genau die Unterschiede? Genügen die kostenlosen Anwendungen?
Das lässt sich nicht generell sagen, weil es sowohl bei den kostenpflichtigen als auch den Gratisscannern sehr grosse Unterschiede gibt. Gratisangebote lassen sich nur im privaten Umfeld nutzen, für den kommerziellen Einsatz muss man in jedem Fall zahlen. Wir empfehlen, für Kauf-Software professionelle Testergebnisse zu konsultieren *(z.B. unter www.pctipp.ch mit Webcode **pdf110164**; Anmerkung der Redaktion).*

Jan Alsenz arbeitet als Teamleiter Security Audits bei der Firma OneConsult in Thalwil

Christoph Baumgartner ist CEO des Unternehmens OneConsult

Auf Webseiten mit dem Kürzel *https://* werden Kreditkartendaten sicher und verschlüsselt übermittelt

Fotos. Ausserdem kann man sich auf Webseiten für illegale Downloads auch schnell Adware einfangen. Bei uns passierte dies, als wir ein aufdringliches Werbebanner anklickten, das uns die Installation einer Software empfahl.

So schützen Sie sich: In der Schweiz ist der Download von urheberrechtlich geschützten Songs, Filmen und TV-Serien erlaubt. Verboten ist hingegen das Anbieten. Das Problem dabei: Viele Tauschbörsendienste laden die Dateien nicht nur herunter, sondern bieten diese gleichzeitig an. Diese Funktion müssen Sie ausschalten. Ist das nicht möglich, könnten Sie belangt werden. Ganz verboten ist das Herunterladen von Software, Produktschlüsseln und Key-Generatoren. Unser Rat: Auf der sicheren Seite sind Sie, wenn Sie Musik und Filme von seriösen Anbietern wie etwa Ex Libris (www.exlibris.ch) oder iTunes (www.apple.com/ch/itunes) herunterladen. Dort verstecken sich keine Schädlinge und es gibt keine rechtlichen Probleme.

Schritt 6: sicher bezahlen

Unser Abenteuer geht weiter – und wir werden leichtsinniger: Wir klicken die verschiedensten Links im Web an, um endlich einen Virus einzufangen. Denn bislang landete erst Adware auf unserer Festplatte. Aber auch auf den besuchten Pornoseiten finden sich keine richtig gefährlichen Schädlinge: Was die Seitenbetreiber von den Besuchern wollen, ist Geld. Bezahlen lässt sich jeweils nur mit Kreditkarte, aber immerhin verschlüsselt. Wir konnten jedoch nicht kontrollieren, wie sicher die Seitenbetreiber die Kreditkartendaten speichern und ob tatsächlich nur die bezogenen Dienstleistungen belastet werden.

So schützen Sie sich: Wir raten, Kreditkartendaten nur auf Webseiten einzugeben, die ein Impressum mit Kontaktadresse haben. Achten Sie auch darauf, ob die allgemeinen Geschäftsbedingungen (AGB) angegeben sind. Diese dürfen nicht fehlen. Zudem müssen Zahlungsdaten immer verschlüsselt übermittelt werden. Achten Sie darauf, ob die Internetadresse mit dem Kürzel *https://* beginnt, **Screen 9**. In diesem Fall ist eine verschlüsselte Übertragung sichergestellt. Ausserdem erscheint ein Schlosssymbol in der Adressleiste oder Statusleiste des Browsers. Wenn Sie auf dieses klicken, erhalten Sie nähere Infos zur Verschlüsselung und zum Webseitenbetreiber.

Auch nützlich ist der Bezahldienst PayPal: Wenn Sie diesen verwenden, werden keine Kreditkartendaten direkt an den Verkäufer übertragen. Das erhöht die Sicherheit. Tipps und Tricks zu PayPal finden Sie unter www.pctipp.ch mit Webcode **pdf110144**.

Schritt 7: Menschenverstand

Jetzt gehts ans Eingemachte: Wir landen während unseres Experiments auf typischen Abzockseiten wie Horoskopdiensten, Lebensprognosen, Routenplanern etc., **Screen 10**. Auch hier fangen wir uns keinen Virus ein. Dafür wollen uns die vermeintlichen Gratisdienste übers Ohr hauen und Geld abknöpfen. Denn in den AGBs verstecken sie teure Gebühren. Gibt man auf diesen Seiten seine Daten an, landet mit Garantie eine Rechnung oder Mahnung im Briefkasten.

Schliesslich hat es uns doch erwischt: Den ersten richtigen Schädling fangen wir bei der Installation einer Software ein, einem gefälschten Flash Player. Wichtig ist dabei: Es war eine bewusste Benutzerinteraktion notwendig, um unseren PC mit Schad-Software zu infizieren. Windows 7 warnte uns vor der Installation, XP nicht.

Als uns wenig später auf einer Webseite eine Virenschutz-Software vor angeblichem Befall warnt, wird es noch kritischer: Wir folgen den Empfehlungen des seriös wirkenden Programms und installieren es. Die Software ist aber eine Fälschung. Sie verankert sich in den Start-Prozess von Windows und verlangt ständig den Kauf der Vollversion. Doch der Anbieter ist mit einer einzigen Kreditkartennummer nicht zufrieden. Die Rückmeldung ist jedes Mal dieselbe: «Please use another card» («Bitte verwenden Sie eine andere Karte»), **Screen 11**. Es findet also gar keine Überprüfung der eingegebenen Daten statt. Dem Programm geht es nur darum, möglichst viele Kreditkartendaten zu sammeln.

Wir schliessen unser Selbstexperiment ab. Das Endresultat: Auf den beiden Computern finden sich insgesamt 2 Trojaner, 3 Trojaner-Installer, 3 Adware-Programme, 1 Backdoor-Tool und Tausende von Cookies. Am Ende des Experiments waren die PCs nicht mehr brauchbar. Interessant: Ausser den Cookies mussten wir alle Schädlinge bewusst installieren. Keiner konnte sich heimlich auf das System schleusen.

So schützen Sie sich: Einen technischen Schutz gegen Abzockseiten wie Horoskopdienste, Lebensprognosen, Routenplaner etc. gibt es keinen. Das Einzige, was hilft, ist ein wachsames Auge. Wer nicht in eine Abofalle tappen will, sollte sich angewöhnen, die allgemeinen Geschäftsbedingungen von Webseiten kurz zu überfliegen. Häufig genügt auch eine schnelle Suche via *Ctrl+F* nach den Begriffen

Das geht ins Geld: angebliche Gratisdienste, die in den AGBs teure Gebühren verstecken

Euro und *Franken*. Sollten Sie dennoch einmal in eine solche Abofalle tappen, müssen Sie den geforderten Betrag nicht bezahlen. Am besten wehren Sie sich mit einem eingeschriebenen Brief beim Betreiber der Abzockseite. Mehr dazu unter www.pctipp.ch mit Webcode **44569**.

Die schlimmste Bedrohung in unserem Experiment waren Software-Fälschungen. Sie haben die PCs unbrauchbar gemacht. Um sich kein solches Programm einzufangen, sollten Sie wenn möglich nicht via Google Software suchen und herunterladen. Besuchen Sie stattdessen direkt die Hersteller-Webseite oder suchen Sie auf seriösen Download-Portalen nach dem Programm (zum Beispiel unter www.pctipp.ch/downloads).

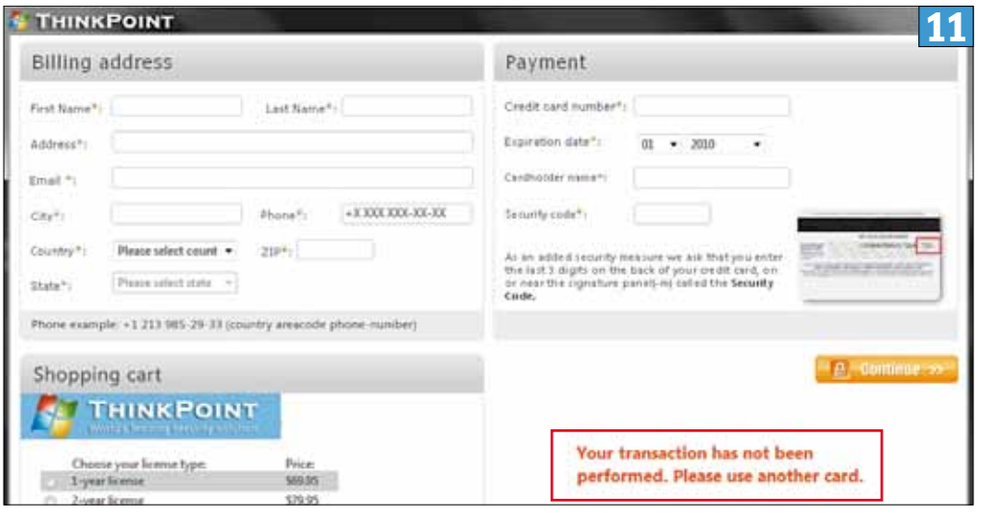
Verwenden Sie dennoch Google, werfen Sie einen genauen Blick auf die fragliche Webseite und studieren Sie Impressum sowie AGB. Weitere nützliche Tipps zu falschen Virenschutzprogrammen und zum Entfernen von diesen finden Sie mit den Webcodes **45320** sowie **45153**.

Fazit: vielfältige Bedrohungen

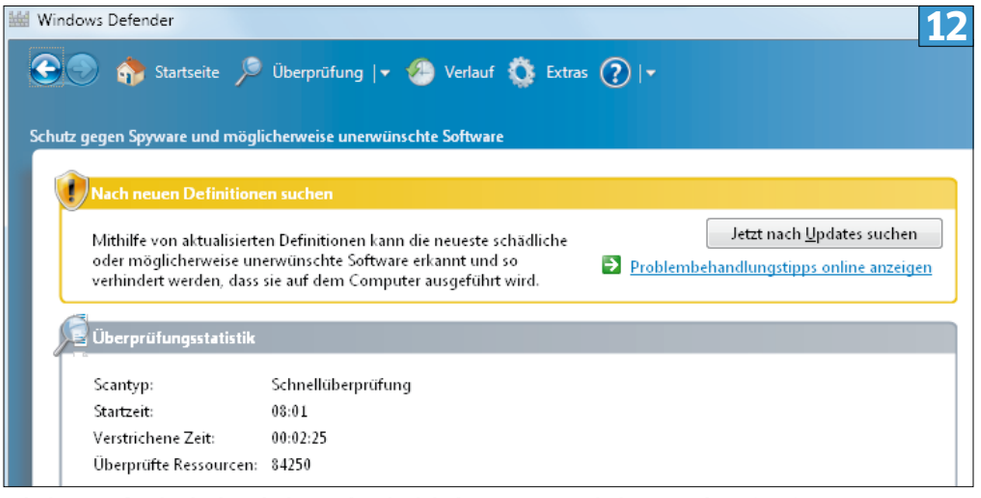
Schädlinge wie Viren und Würmer sind heute nicht mehr die vorherrschende Bedrohung im Internet: Erst in der letzten Phase unseres Experiments ist richtig gefährliche Schad-Software auf unserem System gelandet – obwohl wir beinahe einen ganzen Tag ohne Schutz im Internet unterwegs waren. Diese befand sich zudem auf unseriösen, teils kriminellen Webseiten und tarnte sich als seriöse Software. Haben wir nur Glück gehabt? Lesen Sie dazu die Meinung der Sicherheitsexperten Jan Alsenz und Christoph Baumgartner von OneConsult im Interview auf S. 25.

Fakt ist: Während des Experiments entdeckten wir keine einzige Webseite, die eine Schwachstelle des Webbrowsers ausnutzte und so einen Schädling ins System schleuste. Erst als wir selbst heruntergeladene Programme ausführten, infizierten wir unseren Computer. Deshalb ist eine Antiviren-Software weiterhin Pflicht. Sie warnt vor der Ausführung von bekannten schädlichen Programmen und blockiert diese.

Grosse Unterschiede stellten wir zwischen den beiden Betriebssystemen Windows XP und Windows 7 fest: In Ersterem fanden wir nach dem Experiment doppelt so viel Schad-Software wie in Windows 7. Grund ist vor allem das kostenlose Schutzprogramm Windows Defender, das in Windows Vista/7 intergriert ist, **Screen 12**.



Dieser aggressive Trojaner verlangt von uns immer neue Kreditkartennummern



Windows Defender ist in Windows Vista/7 dabei; XP-Nutzer erhalten es mit Webcode **29358**

Unser Experiment zeigt auch, dass Cyberkriminelle nicht mehr das primäre Ziel haben, den PC zu zerstören. Vielmehr möchten sie Geld verdienen. Das machen sie unter anderem mit Spammails, versteckten Kosten in Geschäftsbedingungen oder gefälschter Software. Dagegen bietet vor allem eines Schutz: der eigene Menschenverstand. Lesen Sie alle Hinweise immer genau durch und installieren Sie nur Programme, die Sie wirklich benötigen. Klicken Sie nicht blindlings auf Links auf unbekannten Seiten oder in E-Mails von Fremden. Verwenden Sie eine Antiviren-Software, die Sie vor der Installation von gefährlicher Software warnt.

Prekär sieht es punkto Datenschutz aus: Viele Webseiten sammeln fleissig Informationen über ihre Besucher für Statistiken und personalisierte Werbung. Ein besonders negatives Beispiel ist Facebook. Möchten Sie das verhindern, sollten Sie Cookies regelmässig löschen.