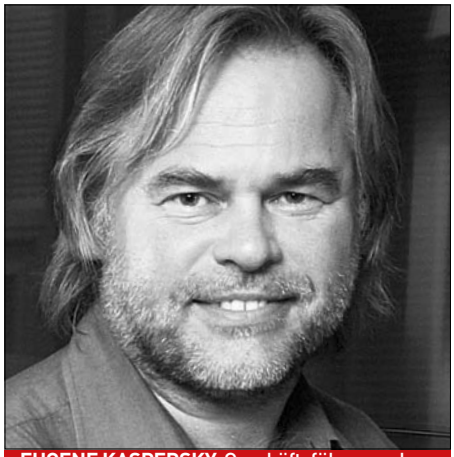


EUGENE KASPERSKY, Geschäftsführer und Gründer des Virenschutzherstellers Kaspersky

„Ich überlege mir zweimal, was ich in sozialen Netzen veröffentliche“

PROF. DR. THORSTEN HOLZ, Forscher (Systemsicherheit) an der Ruhr-Universität Bochum

„Facebook und Google nutze ich nur per TAN-Authentifizierung übers Handy“

MIKKO HYPPONEN, Chef der Forschungsabteilung beim Virenschutzhersteller F-Secure

„Ich benutze keine Software, die auch Millionen andere User verwenden“

Sicherheitstipps der EXPERTEN

Aus Fehlern wird man klug – vor allem aus denen der Profis. Ein exklusiver Blick hinter die Kulissen der IT-Security

VON FELIX KNOKE

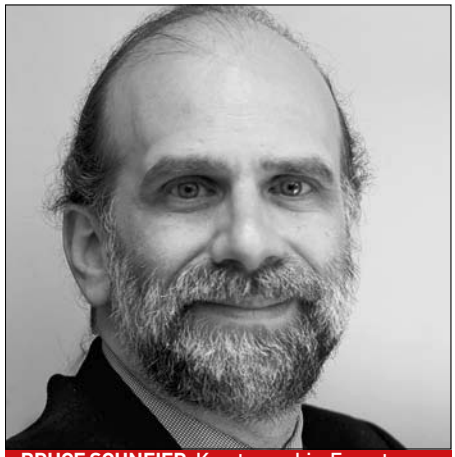
Selbst IT-Profis sind nicht vor den Tricks der Cyberkriminellen gefeit. Aber sie ziehen Lehren daraus, die allen Computernutzern helfen können. Wir haben einige der namhaftesten Sicherheitsexperten gefragt: Auf welche Masche sind Sie schon einmal hereingefallen? Und was haben Sie daraus gelernt? Wir hätten nicht mit so vielen ehrlichen, teils offenherzigen Antworten gerechnet: Eugene Kaspersky etwa berichtet uns, wie er die Entführung seines Sohnes Iwan hätte verhindern können, Grünen-Netzpolitiker Konstantin von Notz, warum verschlüsselte Kommunikation wichtig ist, und Open-Source-Ikone Richard Stallman, warum Windows einfach nur falsch ist.

Jeder kann die Faustregeln der Profis umsetzen, man braucht kein Expertenwissen, um von den Experten zu profitieren. Wer sich an diese Tipps hält, steigert sein persönliches Sicherheitsniveau ohne großen Aufwand und hält die Cyberkriminellen fern. Tipps, die auch unsere Experten immer hätten beherzigen sollen.

Eugene Kaspersky: Entführter Sohn

Als ein russisches Rentnerehepaar im April 2011 seinen zwanzigjährigen Sohn Iwan entführte, beschloss Eugene Kaspersky zusammen mit den Behörden eine List. Über die Medien verbreiteten sie, Kaspersky hätte drei Millionen Euro Lösegeld bezahlt – ein Ablenkungsmanöver, das die Entführer in Sicherheit wiegen sollte. Es funktionierte, kurz darauf griffen die Polizisten zu, Iwan entkam unverletzt.

Doch damit war das Thema für Eugene Kaspersky nicht beendet. Bei den Untersuchungen stellte sich heraus, dass die Kidnapper in sozialen Netzwerken persönliche Informationen von möglichen Opfern sammelten und deren tägliche Abläufe durchleuchteten. Mit



BRUCE SCHNEIER, Kryptographie-Experte, Autor des Newsletters „Crypto-Gram"

„Alle paar Tage lege ich Backups meiner persönlichen Daten an"

KONSTANTIN VON NOTZ, MDB, Netzpolitiker der Partei Bündnis 90/Die Grünen

„Ich verschlüssele immer meine E-Mail-Kommunikation"

JACQUELINE BEAUCHERE, Microsoft Director für Schutz vor Cybermobbing und Identitätsklau

„Ich prüfe regelmäßig, mit wem ich noch in sozialen Netzwerken befreundet sein will"

den erhaltenen Informationen planten sie auch dieses Verbrechen. „Niemand weiß genau, warum sie gerade Iwan als Opfer auswählten", erklärt Kaspersky im CHIP-Gespräch. „Aber ich glaube, es lag daran, dass er exzessiv viele persönliche Informationen bei Vkontakte, dem russischen Facebook, veröffentlichte." Mit diesen Auskünften konnten die Entführer seine Bewegungen nachvollziehen, ihn überwachen und sein persönliches Sicherheitsniveau einschätzen – und das war nicht hoch genug!

Noch heute wirft sich der Vater vor, seinen Sohn nicht über Gefahren in solchen Netzwerken aufgeklärt und ihm keine Tipps für die Veröffentlichung persönlicher Daten gegeben zu haben. „Machen Sie nicht denselben Fehler," warnt Kaspersky, „und handeln Sie jetzt, um Ihre Kinder zu schützen."

Thorsten Holz: Gehackte Hacker

Auch Cyberkriminelle können Datenschlamper sein. Als Thorsten Holz sich zu Forschungszwecken den Kontrollserver eines Botnetzes genauer anschaute, traute er seinen Augen nicht. Die Botnetz-Betreiber hatten das Standardpasswort des Servers nicht geändert. So konnten die Forscher die digitale Beute der Verbrecher gigabyteweise kopieren und auswerten. „Mit einer Zwei-Faktoren-Authentifizierung wären die Gauner auf jeden Fall sicherer (vor uns) gewesen", schmunzelt Holz. Zwei Faktoren bedeutet, dass der User neben dem Passwort noch eine TAN eingeben muss, die er per SMS oder TAN-App auf dem Handy empfängt. Wer sich nur per Nutzername und Passwort einloggt, macht es Angreifern zu einfach: Sie können das Passwort per Keylogger-Trojaner einfach mitlesen. Google und Facebook bieten das Zwei-Faktoren-Log-in bereits heute an.

Mikko Hypponen: Geschröpftes Konto

Die Antivirus-Karriere des blonden Finnen begann ausgerechnet als Virenautor: Noch als Teenager programmierte Hypponen den – ihm zufolge – völlig harmlosen Omega-Virus. Die schiefe Bahn verließ er jedoch schnell und wurde oberster Virenjäger bei F-Secure und Berater internationaler Sicherheitsbehörden. Damit ist Hypponen Zeitzeuge eines dramatischen Wandels: Seit den Neunzigerjahren hat sich viel getan: Cyberkriminalität ist längst ein Milliardengeschäft, und Virenautoren haben es auf die Masse abgesehen. Hypponens Lehre daraus: Wer wenig verbreitete Programme verwendet, gerät seltener ins Fadenkreuz von Cybergaunern. „Benutzt also andere Programme", rät Hypponen. Alternativen gibt es genug: Linux statt Windows 7, den Foxit Reader statt des Acrobat Readers, Opera statt Internet Explorer. Und Java – das braucht eh kein Mensch mehr.

Einen hundertprozentigen Schutz genießen aber selbst IT-Profis nicht. Ein Kollege Hypponens hatte alle Sicherheitsvorkehrungen getroffen – und trotzdem stahlen Internetbetrüger seine Kreditkartendaten. Ein Finanzdienstleister im Hintergrund hatte ein Sicherheitsloch, über das die Betrüger Kreditkartendaten abschöpfen konnten. Da half keine Antivirus-Software. Wer so einen Diebstahl bemerkt, muss schnell handeln: Nur wer früh seine Kreditkarte sperrt, bekommt von der Bank sein Geld zurück.

Bruce Schneier: Gehirn-Backup

Bruce Schneier hat zwei Gehirne: Das zerbrechlichere ist ein Reiselaptop mit allen E-Mails, Kontakten und Terminen. „Mein Gehirn-Backup", witzelt Schneier. Ein Datenverlust wäre für den Sicherheitsexperten eine Katastrophe. Deshalb braucht sein Gehirn-Backup selbst eine Datensicherung. „Je mehr unser Leben am Computer stattfindet, desto schlimmer ist ein Datenleck", erklärt Schneier. Mit einem verteilten Backup im Web und auf verschiedenen Datenträgern erhöhen Sie Ihr Sicherheitsniveau signifikant. „Leute", predigt Schneier deshalb schon seit Jahrzehnten, „legt Backups an!"

Konstantin von Notz: Unlesbare Mails

Über das Internet- und Computerwissen deutscher Politiker wurde in den vergangenen Monaten viel gespottet. Konstantin von Notz, →

BRIAN KREBS, Sicherheitsexperte für Hacker- und Schwarzmarktforen

„Ich installiere nur bekannte Software und lösche sie so bald wie möglich“

JOANNA RUTKOWSKA, Sicherheitsforscherin und Entwicklerin von QubesOS

„Ich nehme einen Rechner zum Surfen und einen zum Arbeiten“

RICHARD STALLMAN, Gründer des GNU-Projekts, erster Präsident der Free Software Foundation

„Ich rühre nichts an, was nicht Freie Software ist“

Bundestagsabgeordneter der Grünen aus Schleswig-Holstein, hält dem miesen Image Technikwissen entgegen – und will mehr Datensicherheit im Bundestag durchsetzen. Denn bislang können Bürger zwar verschlüsselte Mails an ihre Abgeordneten schicken, diese können die Nachrichten aber nicht öffnen. „Ich habe die Bundestags-IT gebeten, Bürgerinnen und Bürgern die vertrauliche, verschlüsselte Kommunikation mit Abgeordneten zu ermöglichen und die entsprechende freie Software bereitzustellen.“ Nach Auskunft der IT-Verwaltung soll das „in Kürze“ möglich sein.

Jetzt müssen sich nur noch die Vorteile verschlüsselter E-Mails in der Bevölkerung herumsprechen. Denn unverschlüsselte Kommunikation ist nicht mit Datenschutz vereinbar: Eine solche Mail kann jeder im Netzwerk mitlesen. „Dabei ist es viel einfacher geworden, einen effektiven Selbstdatenschutz zu betreiben“, so von Notz. Die dafür benötigten Tools und Anleitungen gibt es kostenlos im Netz und sind auch für Laien verständlich.

Jacqueline Beauchere: Falsche Freunde

Kinder sind beliebte Ziele von Identitätsdieben. Immer wieder stößt Jacqueline Beauchere, Sicherheitsexpertin bei Microsoft, auf Fälle, bei denen Identitätsdiebe im Namen von Kindern Schuldenberge anhäufen. Mit deren Sozialversicherungsnummer ergaunern sich die Kriminellen Kredite und gehen auf Einkaufstour. Den Schaden tragen die Eltern. In ihrem Freundeskreis warnt Beauchere deswegen junge Eltern und rät: „Macht Onlinesicherheit zu einem Familienthema, klärt eure Kinder auf und setzt vernünftige Grenzen.“ Dazu gehört auch, regelmäßig die Freundeslisten der Kinder, etwa auf Facebook, zu checken. Denn bei Kindern ist es häufig so: Der beste Freund von heute ist der Erzfeind von morgen.

Eine regelmäßige digitale Hygiene schützt vor Cybermobbing. „Zum Schuljahresende oder bei einem Schulwechsel ist eine gute Gelegenheit dafür“, sagt Beauchere. „Gehen Sie mit ihrem Kind die Freundesliste durch und räumen Sie auf.“ Derselbe Rat gilt freilich auch für die Eltern: „Man kann schnell den Überblick über seine Freunde bei Facebook & Co. verlieren, und darüber, wer welche Informationen von einem sieht.“

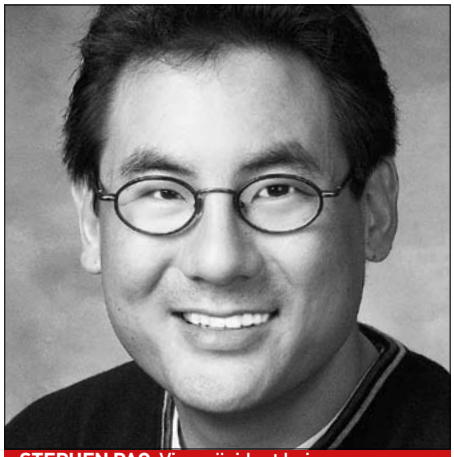
Brian Krebs: (Un)freundliche Quellen

Brian Krebs hat auf die harte Tour gelernt, dass Vertrauen im Internet zwar gut, Kontrolle aber auch nicht schlecht ist. Vor ein paar Jahren schrieb ihn ein Hacker an: „Hey, Brian, schau Dir mal diesen Link an!“ Krebs schaute nicht nur, sondern klickte – und zerstörte damit sein Betriebssystem. Er verbrachte Stunden damit, seinen Computer wieder arbeitsfähig zu machen. Seitdem trennt der Sicherheitsexperte seine Arbeitsumgebung von der Kommunikation. „Du weißt nie, was dir jemand übers Netz schickt. Selbst ‚freundliche Quellen‘ könnten dir eine Schadsoftware senden, weil sie glauben, dass du sie schon nicht einfach so ausführst.“ Inzwischen ist Krebs deutlich argwöhnischer geworden: „Ich installiere nur Programme, die ich kenne und auch wirklich installieren wollte, halte sie immer auf dem neuesten Stand und lösche sie, sobald ich sie nicht mehr brauche.“

Joanna Rutkowska: Sicheres OS

Das Übel an der Wurzel packen, das ist Joanna Rutkowskas Ansatz. Computersicherheit beginnt für sie an der Basis eines jeden Rechners, der Hardware. „Bisherige Betriebssysteme nutzen viel zu wenig neueste Hardware-Technologien aus, die die Computersicherheit stark verbessern könnten.“ Die polnische Sicherheitsforscherin arbeitet daher mit ihrem Team von Invisible Things Lab an dem besonders sicheren und quelloffenen Betriebssystem QubesOS (siehe auch CHIP 08/2011).

Rutkowska zufolge bietet keine auf dem Markt angebotene „Sicherheitslösung“ eine wirklich sinnvolle Antwort auf die Frage, wie man im Alltag das Surfen wirklich sicherer machen kann. Daher muss man sich selbst behelfen und verschiedene Geräte für verschiedene Aufgaben nutzen. „Ich nehme zum Beispiel mein iPad ➔



STEPHEN PAO, Vizepräsident beim Sicherheitsunternehmen Barracuda Networks

„Wenn's geht, schalte ich HTTPS an, besonders bei Facebook"

CANDID WÜEST, Sicherheitsanalyst beim Virenschutzhersteller Symantec

„Wenn ich bei einer Datei unsicher bin, führe ich einen Onlinescan durch"

SEBASTIAN SCHREIBER, White-Hat-Hacker und Geschäftsführer bei SySS

„Ich glaube nicht mehr an einfache Sicherheitstipps"

zum Surfen und einen abgesicherten Rechner zum Arbeiten." Aber irgendwann soll QubesOS das überflüssig machen. „Vielleicht kann ich ja in ein paar Jahren sagen: Wer einen sicheren Computer will, nimmt einfach QubesOS."

Richard Stallman: Spionierendes Windows

Er ist ein unermüdlicher Kämpfer für Freie Software, ein Begriff, den er selbst geprägt hat. Stallman bezeichnet sich zwar nicht als Sicherheitsexperte im engeren Sinne, aber er warnt unablässig vor einer ganz besonderen Computergefahr: Software, die der User nicht kontrollieren kann und Software, vor deren Schädlichkeit User zu oft ihre Augen verschließen. „Das beste Beispiel ist für mich Windows: Es hat Überwachungsfunktionen, digitale Handschellen für die Dateien der Nutzer und Hintertürchen", mahnt Stallman. Er rät daher zu Freier Software, die Sie nicht ausspioniert und mit der Sie die Kontrolle über Ihre Daten behalten.

Stephen Pao: Unbedarfte Mitarbeiter

Jedes Mal, wenn Stephen Pao einen neuen Mitarbeiter einstellt, legt sich der Mitgründer von Barracuda Networks im Firmen-WLAN auf die Lauer. Sollte der oder die Neue es wagen, sich ohne HTTPS-Schutz – also eine sichere Webverbindung – bei Facebook einzuloggen, schlägt Paos Hackersoftware Firesheep Alarm. Jetzt kann sich der Netzwerkexperte in das Facebook-Profil des Mitarbeiters einloggen und beliebig Daten einsehen und verändern. Pao belässt es freilich bei einem lustigen Hinweis – und weist den Neuling in einem ernsten Gespräch darauf hin: „Du weißt schon, dass du in einem IT-Sicherheitsunternehmen arbeitest, oder? Schalte HTTPS an!"

Ohne HTTPS werden Daten unverschlüsselt zwischen der Website und dem User-Rechner übertragen. In einem öffentlichen WLAN-Netz ist das eine Einladung für Betrüger. Bei Facebook findet man die entsprechende Option unter „Kontoeinstellungen | Sicherheit | Sicheres Durchstöbern". Wer es noch nicht getan hat, sollte hier dringend ein Häkchen setzen. Eine gleiche Funktion bieten auch viele andere Webdienste – nur leider meist nicht voreingestellt.

Candid Wüest: Unschuldiger Stick

Weil man Freunden meist traut, hat Candid Wüest die Bitte eines Freundes blind erfüllt: „Schau dir mal an, was für einen Virus ich hier auf dem USB-Stick habe." Was der Freund nicht erwähnt hatte: Dabei handelte es sich um einen aggressiven USB-Autorun-Wurm, der sofort aktiv wird, sobald man den USB-Stick einsteckt. Prompt infizierte er Wüests Testsysteme. „Ich musste alle Computer wieder neu aufsetzen!" Ein Leichtsinnsfehler, den der Symantec-Experte leicht hätte verhindern können. Da nicht alle Sicherheitsprogramme jeden Virus erkennen, lohnt sich ein Onlinescan. Der Webdienst **virustotal.com** etwa überprüft Files mit über 40 verschiedenen Scannern. Auch für Wüest gilt inzwischen: Datei auswählen, hochladen und aufs Ergebnis warten.

Sebastian Schreiber: Vergessener Code

Als sogenannter Pen-Tester bricht Sebastian Schreiber im Auftrag von Firmen in deren Netzwerke und Computersysteme ein – und hätte sich kürzlich fast selbst ausgesperrt. Als er einen schweren Tresor mit Stahlwänden und Codeschloss einrichten wollte, klingelte das Telefon, und schon hatte Schreiber den Code vergessen. „Echt doof, bei einem Tresor. Zum Glück stand die schwere Tür noch offen, dann lässt sich der Schließcode schnell zurücksetzen." Einfache Tipps hätten da wenig geholfen, aber an die glaubt er ohnehin schon lange nicht mehr, selbst für den PC nicht. „Die Gefahren, die man mit einem einfachen, knackigen Trick abwehren könnte, sind schon seit zwanzig Jahren überholt." Wer heute einen Computer schützen will, muss ihn mühevoll pflegen, ihn gegen Gefahren abhärten und vor allem Vorsicht im Internet walten lassen. „Mein Tipp: Immer wenn ein Experte eine einfache Lösung verspricht, dann seien Sie besonders skeptisch." Zumal Experten ja selbst nicht fehlerfrei sind.

FELIX KNOKE, AUTOR@CHIP.DE