SICHERHEITS-

In dieser Ausgabe erfahren Sie, wie Hacker Lücken im Telefonprotokoll ausnutzen, wie In-the-cloud-Virenschutz funktioniert und wie gut deutsche Nutzer ihre PCs schützen.

Foto: Getty

Foto: Getty Images

BÖSER TELEFONMANN

Gespräche abhören, unter falscher Nummer anrufen und gratis telefonieren – für gewiefte Telefonnutzer mit krimineller Energie kein Problem. Sie nutzen dazu SICHERHEITSLÜCKEN IM TELEFONPROTOKOLL.

Sie haben mit einem Kunden ein Telefongespräch vereinbart und rufen ihn an. Während Sie noch das Freizeichen hören, gehen Sie mit einem Kollegen noch schnell die Taktik fürs Gespräch durch. Das Ziel: Sie wollen dem Kunden überteuerte Ware verkaufen. Doch Pech gehabt, denn der Kunde ist bereits im Bilde. Denn während Sie noch das Freizeichen hörten, hat er alles mitbekommen, was Sie und Ihr Kollege am anderen Ende der Leitung besprochen haben. Eklatante Sicherheitslücken im veralteten Telefonprotokoll und bei nahezu allen Telefonen und Handys ermöglichen solche Abhöraktionen – und andere Angriffe mit gravierenden Folgen.

ÜBERTRAGUNGSPROTOKOLL UND TELEFONE MIT SCHWACHSTELLEN

Teil des Telefonprotokolls ist der sogenannte Early Mediastream, mit dem sich besonders viel Schindluder treiben lässt. Eigentlich dient er zur Übermittlung von Frei- und Besetztzeichen sowie für Ansagen wie „Kein Anschluss unter dieser Nummer“ oder „Der Teilnehmer ist zur Zeit nicht erreichbar“.

Zum Sicherheitsrisiko wird der Early Mediastream, weil die Mikrofone aller Telefone und Handys bereits dann aktiv sind, wenn in der Leitung das Freizeichen ertönt. Wer das weiß, kann die Schwachstellen des Telefonprotokolls und der Geräte gezielt ausnutzen: Mit der richtigen Ausstattung kann der Angerufene den Anrufer bereits hören, bevor er das Gespräch überhaupt angenommen hat. Die Schwächen des Telefonprotokolls lassen aber noch ganz andere Missbrauchsmöglichkeiten zu, bei denen wesentlich größere Gefahren drohen.

GRATIS & UNERKANNT TELEFONIEREN

So lässt sich der Early Mediastream für kostenlose Telefonate weltweit missbrauchen – selbst im Mobilfunknetz. Denn der Anrufer muss ja nur dann Ge-

Mit der kostenlosen App SpoofCard für iPhone und Android können Anrufer ihre wahre Identität verschleiern. Der Nutzer tippt eine beliebige Nummer in ein Fenster der App, der Angerufene sieht dann nur diese Nummer.

CENTER
12.3.–26.3.2011

sprächsgebühren zahlen, wenn der Angerufene entsprechend den Vorgaben des Telefonprotokolls das Gespräch tatsächlich annimmt. Doch das ist gar nicht notwendig, ein Gespräch ist auch ohne eine reguläre Telefonverbindung möglich: Die Gesprächspartner lassen es einfach klingeln und können sich dennoch unterhalten. Damit der Leistungsbetrug funktioniert, müssen allerdings einige technische Voraussetzungen erfüllt sein:

■ **Internet-Telefonie:** Zur Basisausstattung gehört ein Konto bei einem Internet-Telefonanbieter, der das SIP-Protokoll (**S**ession **I**nitiation **P**rotocol) nutzt, zum Beispiel Skype oder Sipgate. Darüber wird eine Internet-Telefonverbindung ins öffentliche Telefonnetz aufgebaut.

■ **Telefonie-Software:** Nur mit dem Einsatz einer Software lässt sich das störende Freizeichen entfernen. Hacker nutzen dafür das Gratis-Telefonprogramm Asterisk. Die nötigen Manipulationen am Programmcode erfordern dann etwas Fachwissen. Weil es diese Ausrüstung kostenlos im Internet gibt, erfreut sie sich bei skrupellosen Vieltelefonierern großer Beliebtheit.

Kriminelle und Terroristen wiederum nutzen die Lücken des Telefonprotokolls zur heimlichen Kommunikation. Denn Telefonate, bei denen keine abrechenbaren Kosten entstehen, können die Netzbetreiber in der Regel weder erfassen noch speichern. Und damit stehen sie auch Strafverfolgern nicht für Ermittlungen zur Verfügung.

„Gegen die Lücken im veralteten Telefonprotokoll sind die Telefonnetz-Anbieter machtlos."
Marco Di Filippo
Sicherheitsexperte Compass Security

FALSCHE IDENTITÄTEN

Die Lücken des Telefonprotokolls lassen sich auch mit deutlich weniger Aufwand ausnutzen. Über spezielle Handy-Apps, wie SpoofCard (siehe Bild Seite 28) und entsprechende Internetdienste können Angreifer falsche Identitäten vortäuschen. Was erst mal wie ein alberner Lausbubenstreich erscheint, ist für die Abzocker der Telefonmafia ein sehr interessantes Werkzeug. Denn so können sie ihre nervigen und mittlerweile strafbaren Werbeanrufe tarnen – ihre Opfer finden nur schwer heraus, woher der Anruf kam.

TELEFONNETZ-ANBIETER MACHTLOS?

Gegen den Missbrauch der Lücken des Übertragungsprotokolls sind einzelne Telefonnetz-Anbieter machtlos. Um grundlegende Sicherheit zu erreichen, müssten sie gemeinsam weltweit einen neuen Standard etablieren. Doch der ist nicht in Sicht, und so geht den Anbietern viel Geld durch die Lappen, und der Schutz ihrer Kunden bleibt auf der Strecke.

Die Lösung des Abhörproblems liegt dagegen in den Händen der Gerätehersteller. Sie müssten sicherstellen, dass die Telefonmikrofone erst aktiviert werden, wenn der Angerufene ein Gespräch auch wirklich angenommen hat. Bei einigen Modellen der Hersteller SonyEricsson und RIM Blackberry ist das bereits der Fall. Die anderen Hersteller von Telefonen und Handys sollten schnell mit einer entsprechenden Software-Aktualisierung nachziehen. *[nm/opu]*

SO WERDEN LÜCKEN IM TELEFONPROTOKOLL MISSBRAUCHT

Mit etwas technischem Know-how und kostenlosen Telefon-Programmen aus dem Internet können Kriminelle die Lücken des veralteten Telefonprotokolls problemlos ausnutzen. Dafür missbrauchen sie den Standard zur Weiterleitung von Tonsignalen („Early Mediastream"), der beispielsweise zur Übermittlung des Freizeichens dient. Die Grafiken zeigen, welche Angriffe sich so durchführen lassen.

ABHÖREN: Bereits vor der Annahme eines Gesprächs können Angerufene hören, was am anderen Ende gesprochen wird.

GRATIS-GESPRÄCHE: Telefonieren ohne zu bezahlen ist gängige Praxis bei Straftätern und Terroristen.

FALSCHE IDENTITÄT: Um unerkannt eine Person ans Telefon zu kriegen, können Angreifer falsche Rufnummern einblenden.

SCHÄDLING DER WOCHE

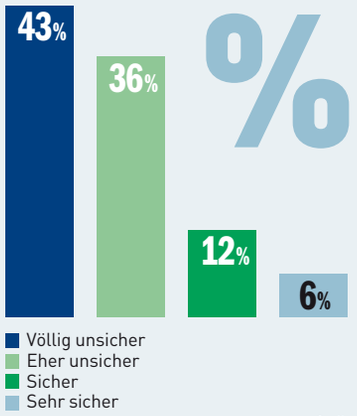
TROJAN-SPY.WINCE.BOT

Der Trojaner ZeuS, der vor einiger Zeit schon auf Windows-PCs sein Unwesen trieb, hat ein neues Ziel ausgemacht: Computerhandys mit den Betriebssystemen Windows Mobile oder Symbian. ZeuS lockt über den Computer mit einer Aktualisierungs-Software fürs Handy. Wird das angebliche Update per SMS aufgespielt, kann der Angreifer eingehende SMS-Nachrichten abfangen.

GRAFIK DER WOCHE

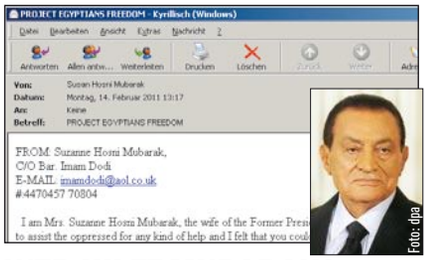
MEHRHEIT SIEHT DATEN-SICHERHEIT SKEPTISCH

Die Mehrzahl der deutschen Internetnutzer hält ihre persönlichen Daten im Internet, etwa in sozialen Netzwerken, für unsicher.



Quelle: Bitkom

SPAM DER WOCHE



WER HILFT MUBARAK?

Hosni Mubarak, ehemaliger Staatschef von Ägypten, will sein Vermögen in Sicherheit bringen. Dazu braucht er Ihre Hilfe, die ihm 3 Millionen US-Dollar wert ist. Die Mail-Empfänger sollen paar Tausender Vorschuss leisten, nach der Übermittlung der Kontaktdaten soll der Rubel rollen. Wie immer bei solchen „Scam-Mails" gilt: Ab in den Papierkorb!

TOP 5
DER BEDROHUNGEN

1 LECKS IN SOZIALEN NETZWERKEN
Sicherheitslücken in sozialen Netzwerken wie Facebook, Lokalisten oder Friendscout 24 nehmen immer mehr zu. Die neue Internetseite **socialnetworksecurity.org** will nun verstärkt auf die Gefahren der sozialen Netzwerke aufmerksam machen.

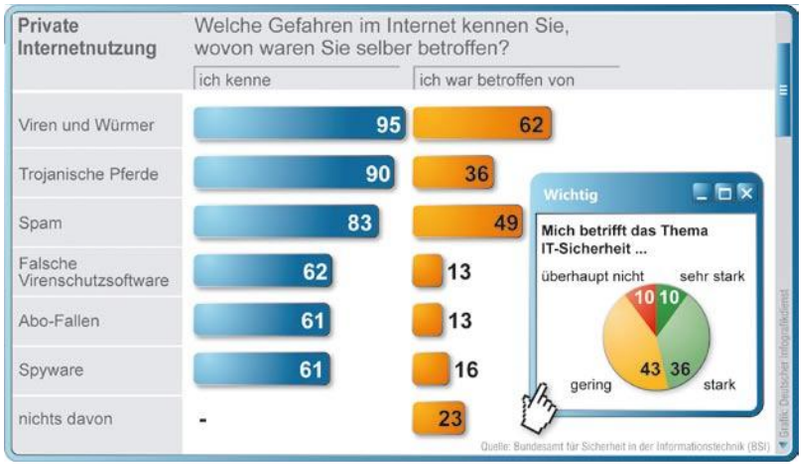
2 SOFTWARE-LECKS
In Microsoft Windows, Office und Internet Explorer sowie in diversen Adobe-Produkten klaffen weiterhin Sicherheitslecks, über die Schädlinge auf PCs geschleust werden können.

3 VIREN
In den vergangenen Wochen gab's einen deutlichen Anstieg neuer Schadprogramme.

4 ONLINE-KRIMINELLE
In Baden-Württemberg ist die Anzahl der Internet-Straftaten 2010 um 4,6 Prozent gestiegen.

5 iPHONE-PASSWÖRTER
Fraunhofer-Mitarbeitern ist es gelungen, gespeicherte Passwörter aus einem gesperrten iPhone auszulesen.

Quelle: Herstellerinformationen



▲ **Viele Nutzer verzichten auf Virenscanner und eine Firewall.**

◀ **Die meisten Deutschen unterschätzen Internetgefahren.**

SCHLECHT GESCHÜTZT

Die Deutschen gehen zu sorglos mit dem Thema PC-Sicherheit um, warnt das Bundesamt für Sicherheit in der Informationstechnik.

Die Zahl von fiesen Schädlingen, Hacker-Angriffen, Werbe-E-Mails und Betrugsversuchen im Internet nimmt ständig zu. Das wissen auch deutsche Internetnutzer. Doch statt PC und persönliche Daten vor der Gefahrenflut abzuschirmen, werden deutsche Surfer immer leichtsinniger. Das zeigt eine aktuelle Studie des Bundesamts für Sicherheit in der Informationstechnik (BSI).

GEFAHR ERKANNT – ABER NICHT GEBANNT

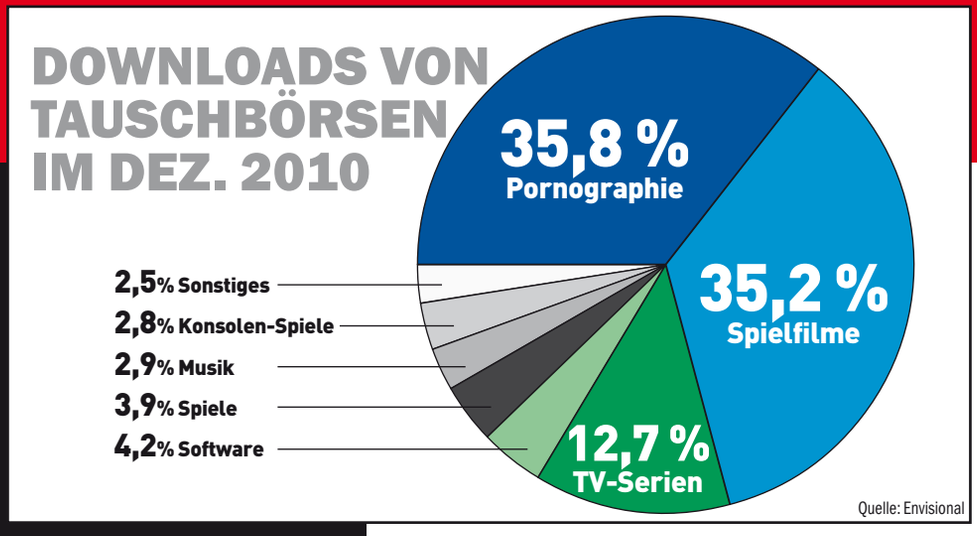
Eines der erschreckendsten Ergebnisse der Studie: Der Einsatz von Viren-Schutzprogrammen ist rückläufig! Nur noch 87 Prozent der Bundesbürger nutzen ein Schutzprogramm. Bei der BSI-Umfrage aus dem Jahr 2008 waren's noch 92 Prozent. Und nur 60 Prozent geben an, dass sie eine Firewall* verwenden – wobei die meisten wohl einfach nicht wissen, dass ein solche Schutzmauer ihren PC schützt: Schließlich haben Windows und alle Schutzpakete eine Firewall.

Laut BSI-Studie hat mehr als ein Viertel der Befragten noch nie eine Sicherheitsaktualisierung für Windows oder andere Programme aufgespielt. Und nur 42 Prozent nutzen dafür bewusst die automatische Update-Funktion, die Windows und fast jede Software bietet. Allerdings ist diese Funktion standardmäßig aktiviert, und die BSI-Studie erfasst nicht, wie viele der Befragten von der Aktualisierung gar nichts merken.

90 Prozent der Befragten gaben an, ihnen sei Internetsicherheit wichtig oder sogar sehr wichtig. 60 bis 90 Prozent wissen um Gefahren wie Schadprogramme und Abo-Fallen. Dennoch schätzen 75 Prozent ihre Sicherheitskenntnisse in Schulnoten bestenfalls zwischen 3 und 6 ein. „Unsere Bürgerbefragung offenbart erstaunliche Gegensätze", so Matthias Gärtner vom BSI. „Unsere Studie zeigt, dass viele Bürgerinnen und Bürger zwar um die Risiken beim Internetsurfen wissen, die notwendigen Schutzmaßnahmen jedoch ergreifen noch zu wenige". *[nm/opu]*

EIN VIERTEL DES DATENVERKEHRS IST ILLEGAL

23,76 Prozent des gesamten Internetverkehrs beanspruchen die Nutzer von Daten-Tauschbörsen – fast ausschließlich zum illegalen Download urheberrechtlich geschützter Daten.



1-2-3-Klicks
„Privat-Modus" im IE9

Wer den „inPrivate-Modus" des Internet Explorers ständig nutzt, um keine Spuren auf dem PC zu hinterlassen, sollte so vorgehen:

1 Klicken Sie mit der *rechten* Maustaste auf die Arbeitsoberfläche sowie auf Neu und Verknüpfung. Tippen Sie danach "C:\Program Files\Internet Explorer\iexplore.exe" -private ein, und klicken Sie auf Weiter.

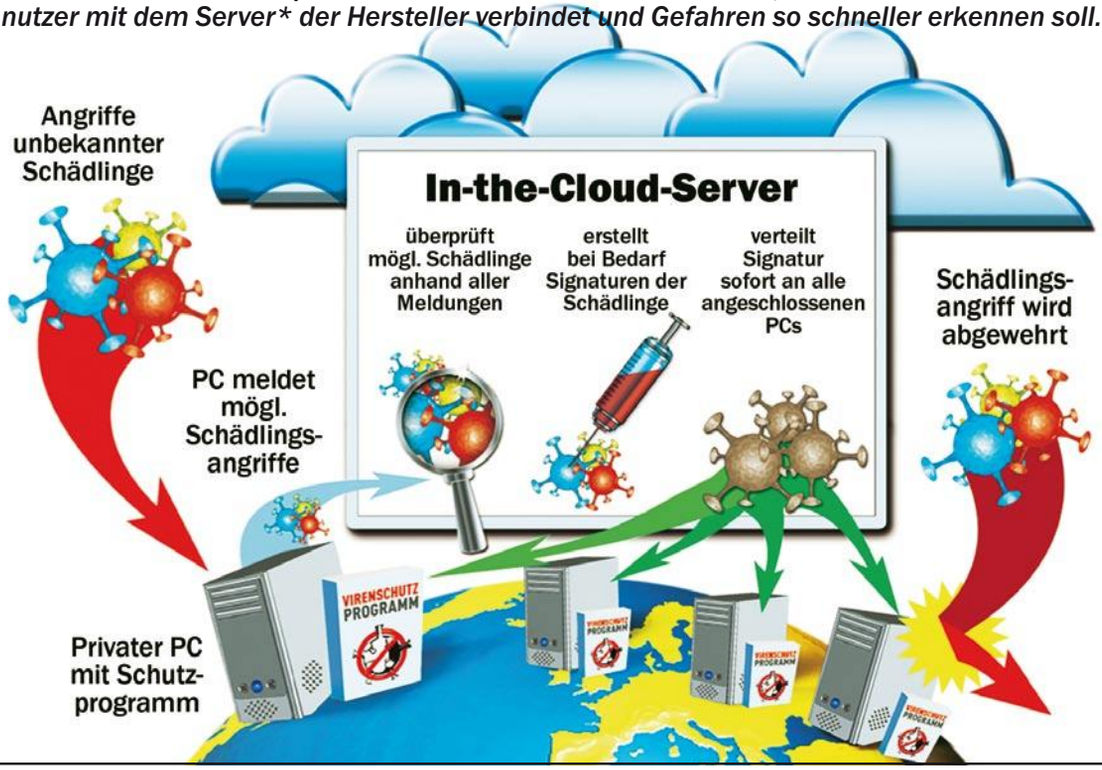
2 Geben Sie dann einen Namen für die Verknüpfung ein, etwa IE9_privat. Es folgt ein Klick auf Fertig stellen.

3 Per Doppelklick auf starten Sie künftig den Internet Explorer direkt im Privat-Modus.

*Die Erklärung dieses Fachbegriffs finden Sie auf Seite 140/141.

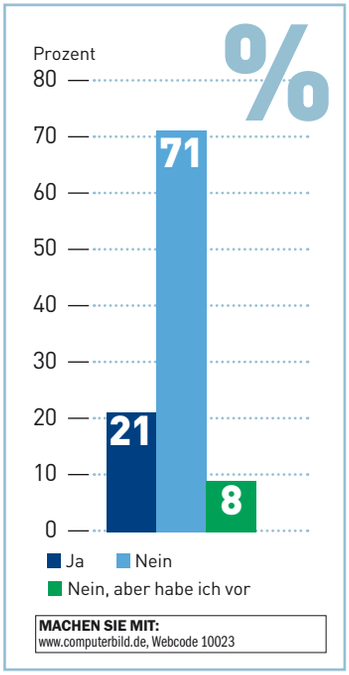
SO FUNKTIONIERT IN-THE-CLOUD-SCHUTZ

Die meisten Sicherheitspakete nutzen In-the-Cloud-Virenschutz, der die PCs der Softwarenutzer mit dem Server der Hersteller verbindet und Gefahren so schneller erkennen soll.*



UMFRAGE DER WOCHE

Verwenden Sie ein Kennworttresor-Programm?



MACHEN SIE MIT:
www.computerbild.de, Webcode 10023