Leserforum

Brauche kein Bargeld

Editorial: Bargold lacht!, c't 24/16, S. 3

Ich bin ein großer Freund von der Tatsache, das Bargeld – nicht ganz, aber – teilweise abzuschaffen.

Wer nutzt den 500-Euro-Schein wirklich für den Einkauf? Neues TV im Doof-Markt? Mit Karte bezahlt. Möbelkauf? Mit Karte oder auf Rechnung.

Ich gehe noch weiter und würde die 1-, 2- und 5-Cent-Münzen gleich mit abschaffen, da sie völlig überflüssig sind: auf-/abrunden, fertig. Der Rest gleicht sich aus.

Es ist aber sicher nicht richtig, vom Wegfall des 500-Euro-Scheins gleich so panikartig auf die Abschaffung des Bargelds insgesamt zu schließen.

Obwohl ... Außer für den Bäcker und den Parkautomaten brauche ich persönlich heute schon kein Bargeld mehr.

Axel Schwenke

Erpresstes Geld verschwindet elektronisch

Durch Ransomware und andere Methoden der Erpressung von PC-Besitzern verschwindet erpresstes Geld elektronisch auf Nimmerwiedersehen. Die Zwischenkontobesitzer sind ahnungslos. Der erpresste PC-Besitzer bleibt der Dumme.

Auch andere elektronische Betrügereien, bei denen Konten und damit Nutzer manchmal gleich in Millionenanzahl geschädigt werden, sind aus der Presse zur Genüge bekannt.

Wie Politiker, Banken, Behörden und andere Schlauberger da von sicherer als Bargeld reden können, ist mir völlig unverständlich.

Weg vom elektronischen Zahlungsverkehr und zurück zum Bargeld pur sollte mal ein Wirtschaftswissenschaftler fair durchrechnen.

Gandalf22

Facebook nicht nutzen

Was Facebook mit Ihren Daten macht, c't 24/16, S. 72

Auf insgesamt 14 Seiten wird dargelegt, wie und welche Daten Facebook erhebt und verwendet, und wie machtlos man dagegen ist. Im Grunde genommen ein sehr interessanter Artikel, aber überraschen wird das keinen mehr.

Schlimm ist, dass die deutsche, europäische und globale Politik nichts gegen derartige Firmen unternimmt und man sich lieber in Details verliert und den Firmeninteressen unterwirft.

Noch viel schlimmer ist aber, dass zwar im Artikel ausführlich erklärt wird, wie man sein Facebook-Profil absichert. Die einzige wirkliche Lösung wird aber nicht genannt: Facebook & Co. einfach nicht nutzen!

Heiko Hennig

Gläserne Menschen bei Facebook

Jeder, der Facebook nutzt, muss sich bewusst sein, dass er nicht der Kunde, sondern das Produkt ist. Aber dann macht man sich bewusst zum gläsernen Menschen. Viel schlimmer ist die Datensammelwut und -verknüpfung bei Nicht-Mitgliedern, die nicht mal mitbekommen, was Facebook alles über sie weiß und die dem Ganzen völlig hilflos gegenüberstehen.

Das sind Zustände, die Orwells Visionen noch bei Weitem in den Schatten stellen. Und aufgrund der Filterblase und des Echokammer-Effekts wird Facebooks Macht über die Meinungen auch immer größer. Und die Politik sieht dem Ganzen eher hilflos zu oder ahnt noch nicht so ganz die Tragweite.

Dies kann durchaus auch als Lackmustest für Demokratie verstanden werden. Handelt die Politik noch im Interesse des Bürgers oder ist die Politik nur noch Marionette der Wirtschaft und es entscheiden längst ganz andere, wie es weitergeht?!

Julian Hansen

In den Fängen von Facebook, Titel-Geschichte in c't 24/16

Wir freuen uns über Post

redaktion@ct.de

c't Forum

c't magazin

@ctmagazin

Ausgewählte Zuschriften drucken wir ab und kürzen sie wenn nötig sinnwahrend.

Antworten sind kursiv gesetzt.

Chrome und Edge problematisch

Add-on fungiert als Datenwanze für seinen Hersteller, c't 24/16, S. 16

Wir sind uns einig, dass viele Browser-Erweiterungen unsicher programmiert sind. Vielen Dank für den Hinweis auf upalytics.com! Ihrem Rat, einen Browser von Google oder Microsoft zu verwenden und auf Erweiterungen ganz zu verzichten, können wir uns aber nicht anschließen.

Google und Microsoft sind Datenkraken, und ihre Browser sind die Datenstaubsauger, die ihnen die Daten liefern. Da würden auch die besten Add-ons nicht helfen. Daher raten wir dringend davon ab, die Browser dieser Hersteller zu nutzen.

Ohne einen guten Adblocker wie uBlock Origin sind die Nutzer.innen Trackern schutzlos ausgeliefert. Denn davor schützt die in den meisten Browsern verwendete Google Safe Browsing API nicht. Außerdem: Google hat sich zwar ein paar Gedanken um Datenschutz gemacht, aber NSA und GCHQ können Nutzer.innen über das Google-Cookie eindeutig identifizieren. Daher raten wir Personen, die nicht von Geheimdiensten ausspioniert werden möchten, Zugriffe auf diese API zu unterbinden. Noch unsicherer ist Microsofts Malware-Schutz „SmartScreen" – ein weiterer Grund, weshalb wir von Microsoft-Browsern abraten. Über eine Empfehlung für den Tor-Browser hätten wir uns hingegen sehr gefreut.

Hartmut Göbel und Christian Pietsch, Digitalcourage e.V.

Die Kurve kriegen

DNSSEC: Warum RSA-Schlüssel nur noch zweite Wahl sind, c't 24/16, S. 22

Im Artikel wird beschrieben, dass langfristig nur 15360-Bit-RSA-Schlüssel sicher sind. Das stimmt im Prinzip, gilt in der Schärfe aber nur für Anwendungen, bei denen Daten verschlüsselt und für viele Jahre (>20) geheim gehalten werden müssen.

Bei DNSSEC werden die RSA-Schlüssel jedoch zum Signieren der DNS-Daten verwendet, nicht um die Daten geheim zu halten. Die DNSSEC-Schlüssel sollten so gewählt werden, dass sie innerhalb des Schlüsselaustauschintervalls (DNSSEC Key-Rollover) nicht gebrochen werden können. Bei einem Intervall von 30 Tagen für den ZSK (Zone Signing Key) gilt auch ein 1024 Bit langer RSA-Schlüssel als sicher, 1536 oder 2048 Bit sind auf jeden Fall ausreichend. Nach heutigen Erkenntnissen ist es Geheimdiensten nicht möglich, RSA-Schlüssel in einer kurzen Zeit von 30 Tagen zu brechen. Und nach dem Tausch eines DNSSEC-Schlüssels ist der alte wertlos. Wird er nach Ablauf von 30 Tagen gebrochen, hat das keine negativen Auswirkungen auf die DNSSEC-Sicherheit, da die Signaturen nur zum Zeitpunkt der DNS-Abfrage geprüft werden.

Bei der Wahl der Länge von kryptografischen Schlüsseln sollte immer die Anwendung der Schlüssel (Verschlüsselung oder Signatur) und die Gültigkeit der Daten betrachtet werden.

Carsten Strotmann

Amazon tut nichts

Amazon bekommt Abzock-Masche seit Jahren nicht in den Griff, c't 24/16, S. 68

Als ich vor einem halben Jahr nach Fernsehern, speziell von Samsung, gesucht habe, fielen mir viele Shops auf, die gängige Modelle oft zu 50 bis 70 Prozent der anderen Preise anboten. Dort wurde, wie beschrieben, um Kontaktaufnahme per E-Mail gebeten.

Ich machte Amazon darauf aufmerksam, dass speziell im Umfeld von Samsung-Fernsehern scheinbar jeder zweite Shop in betrügerischer Absicht aufgesetzt/bestückt wurde und sie sich das mal genauer anschauen sollten. Es kamen nur allgemein gehaltene Mails, die versicherten, dass man das Problem sehr ernst nähme. Dass auch nur ein einziger Shop entfernt oder von Amazon eingeschritten wurde, konnte ich während der circa einwöchigen Suchphase nicht feststellen. Ob der Satz Ihres Kommentars „... Amazon reagiert immer erst dann, wenn der Kunde längst reingefallen ist“ zutrifft, kann man nur hoffen. Ich konnte feststellen, dass offensichtlich betrügerische Angebote selbst dann nicht entfernt wurden, nachdem sie gemeldet wurden. Eine wirksame Kontrolle/Prävention gibt es wohl nicht oder sie wird nur sehr lasch gehandhabt.

W. Ettenhofer

Gegenmaßnahmen

Wir betreuen Hunderte Amazon-Seller und -Vendoren. Über ein Prozent unserer Kunden im Seller-Segment sind Opfer der von Ihnen beschriebenen Masche geworden. Einige beteuern, komplexe Passwörter verwendet zu haben und zwar unikale für jeden einzelnen Account. Insofern war auch unsere Vermutung, dass es sich um Phishing-Opfer handeln müsse.

Es verwundert, dass Amazon nicht längst entsprechende Gegenmaßnahmen ergriffen hat. Immerhin ist das Vorgehen immer identisch. Ein Seller, der zuvor nie Waschmaschinen und Kühlschränke angeboten hat, bietet von einem Tag auf den anderen Tausende hochpreisige Produkte an, die sich immer ähneln. Auch die Masche mit den Kontaktdaten ist, wie von Ihnen berichtet, immer dieselbe. Es müsste daher relativ einfach sein, Betrugspräventionsmaßnahmen einzurichten.

Name ist der Redaktion bekannt

Sicherheitsfassade

AVM entweicht geheimer Krypto-Schlüssel, c't 24/16, S. 32

Ein kompromittierter Schlüssel ist schlecht. Dass AVM das passiert, auch. In der heutigen Zeit ist das aber leider nichts Außergewöhnliches. Wenn aber die Provider Monate brauchen, um dies zu korrigieren, dann haben sie seit Jahren entweder nichts oder das Falsche gemacht. Von der Sicherheitsfassade durch Routerzwang bleibt ein potemkinsches Dorf.

sowosama

Vergleich mit der 1050 Ti

Kaufberatung: Grafikkarten zum Spielen, Arbeiten und Rechnen, c't 24/16, S. 102

In der Tabelle fehlt zum Vergleich die 1050Ti, die explizit erwähnt wird. Wo sollte man die einsortieren?

Stefan Krämer

Mit 4 Watt im Leerlauf und 55 Watt im 3D-Test ist die GeForce GTX 1050 Ti (siehe c't 23/16, S. 42) besonders sparsam und liegt im 3DMark Fire Strike mit 6728 Punkten leicht über der GeForce GTX 960.

pfSense-Alternative

Router-Selbstbau mit Open-Source-Software, c't 24/16, S. 122

Vielen Dank für die interessanten Artikel. Es gibt eine Router-Distribution, die Sie meiner Ansicht nach unbedingt erwähnen sollten: OPNsense (https://opnsense.org) ist ein Fork von pfSense. Es hat eine aktive deutsche Entwickler-Community, die Menüs sind in verschiedenen Sprachen wählbar. Was am wichtigsten ist: Auf etwaige Fehler reagiert die Community sehr rasch.

Jakob Strebel

Rockbox-iPod befüllen

Pimp my Pod, Den iPod mini mit Flash-Karte und neuem Akku aufrüsten, c't 24/16, S. 164

Wenn Rockbox mit Kernel Panic abstürzt, dann kann, zumindest bei den Classic iPods, die Musik mit der Original-Firmware über den Dateimodus und dem Explorer (nicht mit iTunes) geladen und unter Rockbox abgehört werden.

cdtmbu

Ergänzungen & Berichtigungen

USB 2.0 statt 3.0

Einsteiger-Fritzbox für Kabel-Anschlüsse, c't 24/16, S. 26

Anders als im Artikel erwähnt hat die Fritzbox 6490 wie das neue 6430er-Modell zwei USB-2.0-Ports, nicht zweimal USB 3.0.