Leserforum

Das geht besser

Editorial: Ärger mit Elster, c't 19/2019, S. 3

Dass es auch anders gehen kann, sehe ich als jemand, der sowohl in Deutschland wie auch in Österreich eine Steuererklärung abgeben muss. Ist man in Österreich das ganze Jahr über gleichzeitig nur bei einem einzigen Arbeitgeber angestellt und hat nichts zum Absetzen, braucht man schon seit jeher gar keine Steuererklärung abzugeben. Neuerdings bekommt man bei einfach gelagerten Fällen sogar die Steuergutschrift automatisch. Das nennt sich „Antragslose Arbeitnehmerveranlagung" beziehungsweise „Automatischer Steuerausgleich".

Und hat man doch mehr anzugeben oder arbeitet bei mehr als einem Arbeitgeber gleichzeitig, sodass man zur Steuererklärung verpflichtet ist, so lässt sich diese auch um vieles einfacher durchführen als in Deutschland. Einkünfte werden automatisch übernommen – nicht einfach vom Vorjahr sondern die tatsächlich aktuellen, von den Firmen ans Finanzamt für das jeweilige Jahr gemeldeten. Gleich bleibende Absetzbeträge kann man auch vom Vorjahr übernehmen. Kurz gesagt: Wirklich komfortabel gegenüber Elster.

Pentaculus

Neuland E-Mail

Das Problem fängt manchmal schon bei sehr viel einfacheren Techniken an: In München ist das Finanzamt schon länger nicht gewillt oder nicht in der Lage, trotz mehrfacher Hinweise auf die Fehlfunktion, die auf den offiziellen Schreiben und auf der Homepage als für mich zuständig benannte E-Mail-Adresse poststelle-abteilung1@famuc.bayern.de so zu betreiben, dass sie erreichbar ist.

Dr. Christoph Diesch

Lobenswert

Wie US-Militär und Unternehmen um Hacker buhlen, c't 19/2019, S. 16

Die US Air Force macht es vor und lässt Hacker an ihre Jets ran, um deren Sicherheit zu testen beziehungsweise zu verbessern. Eines der größten IT-Projekte unserer Zeit, die Telematik-Infrastruktur des Gesundheitswesens (immerhin müssen zwischen 150.000 und 200.000 Praxen, Apotheken, Krankenhäuser etc. vernetzt werden), geht dagegen ganz anders vor: Kritik an den unsicheren Strukturen wird totgeschwiegen, obwohl die Installateure der Konnektoren und Kartenlesegeräte reihenweise die Firewalls ausschalten und andere Bugs einbauen, wie Jens Ernst aus Schwerte nachgewiesen hat. Penetrationstests sind entweder gar nicht erst durchgeführt worden oder werden nicht publiziert (warum wohl?) und wurden Herrn Ernst nach dessen Aussage sogar untersagt. Praxen wurden bereits mit Malware infiziert. Sogar das Fernsehen hat schon berichtet, passiert ist nichts.

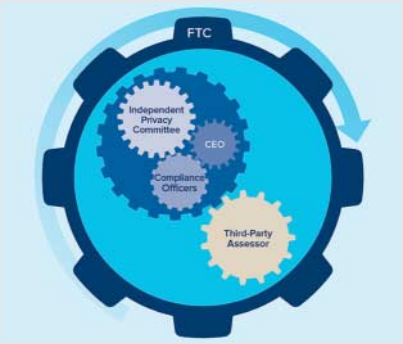
S. Schneider

Blockade

Datenschutz-Skandal kostet Facebook 5 Milliarden Dollar, c't 17/2019, S. 39

Genial – anders kann man das Bild der FTC nicht bezeichnen. Da hat sich die FTC, vermutlich durch einen übereifrigen Grafiker, selbst in den Fuß geschossen. Ein tolles Getriebe hat er da konstruiert: Ein kleines Rädchen „CEO" reicht aus, um das ganze System zu blockieren.

Christoph Schmees



Mehrere Leser haben sofort erkannt, dass beim Datenschutz der CEO das Problem ist …

Bestimmt kein Zufall

Bockige CPU-Zufallszahlen und offene Befehlssatzarchitekturen, c't 19/2019, S. 34

Auch die Intel-Implementierung hat eine Anfälligkeit für Backdoors, ist sie doch in Mikrocode geschrieben. Da kann man einen guten Algorithmus leicht durch einen schlechten tauschen, ohne dass es groß auffällt, BIOS-Update genügt. Enthält dieser Code einen Schlüssel, den nur die NSA kennt, ist das sogar eine dieser ominösen „sicheren" Backdoors.

Das gleiche Problem hat AMD mit seiner PSP: Auch hier haben wir Code, der den Zufall weiterreicht (produziert wird er ja erst mal in irgendeiner Hardware), und dieser Code kann natürlich kaputt sein. Äh, ne, er kann nicht nur kaputt sein, er ist sogar definitiv erkennbar kaputt. Das ist ja das Problem von AMD!

Völlig unklar ist auch, warum der Code so ranzig ist, dass man ihn nicht fixen kann. Das einzige, was ich mir ernsthaft vorstellen kann, ist, dass AMD einen NSL [National Security Letter, Anm. der Red.] hat, der sie verpflichtet, diesen Random-Generator ranzig zu machen, und dass sie das nicht wirklich besser machen dürfen.

Bernd Paysan

Ahnungslose Kunden

Neue Bezahlregeln im E-Commerce greifen später, c't 19/2019, S. 48

Dank Ihrer Artikelserie zur PSD2-Einführung in den letzten c't-Ausgaben fühle ich mich mittlerweile gut informiert. Von Seiten der Banken scheint allerdings ein deutliches Kundeninformationsdefizit zu bestehen. Außer den bei solchen Änderungen üblicherweise abzunickenden AGB-Anpassungen im üblichen Juristen-

Wir freuen uns über Post

redaktion@ct.de

c't Forum

c't magazin

@ctmagazin

Ausgewählte Zuschriften drucken wir ab. Bei Bedarf kürzen wir sinnwahrend.
Antworten sind kursiv gesetzt.

Anonyme Hinweise
https://heise.de/investigativ

deutsch habe ich noch keinerlei Informationen von meinem kontoführenden Institut gesehen, was sich so auch im Bekanntenkreis für andere Banken bestätigt.

Einzig mein Vater hat über das Onlinebanking-Portal der Deutschen Bank schon unfreiwillig PSD2-Kontakt gehabt: Dort wird beim Anmelden angeboten, den ab 14. 9. vorgeschriebenen 2-Faktor-Login schon jetzt freiwillig zu aktivieren. Da auch von der DB vorher sonst keine weiteren Informationen gekommen waren, und man vorher jahrelang immer wieder davor gewarnt wurde, TANs in fremden oder unbekannten Kontexten und Situationen einzugeben, wähnte mein Vater einen wie auch immer gearteten Angriff und stellte jegliche Aktivität an dem Rechner bis zu meinem Besuch ein …

Vor diesem Hintergrund scheint der 14. 9. eine riesige Studienmöglichkeit zur Effektivität bisheriger Aufklärungskampagnen: Variante 1 (IMHO die wahrscheinlichste): Die Onlinebanking-Nutzer haben bislang nichts von den PSD2-Änderungen gehört, stören sich aber auch nicht weiter an der zusätzlichen TAN-Abfrage und geben stumpf eine TAN ein, weil sie halt abgefragt wird. Ableitbares Ergebnis: Das Sicherheitsverständnis ist allen vorherigen Kampagnen zum Trotz gering und wegen der weiterhin geringen Haftungsrisiken wird sich daran auch vermutlich nichts ändern. Der zusätzliche Supportaufwand für Banken beschränkt sich auf einige alte Homebanking-Programme, die nicht mehr funktionieren.

Variante 2: Die Onlinebanking-Nutzer haben bislang nichts von den PSD2-Änderungen gehört, stören sich aber an der ungewöhnlichen TAN-Abfrage beim Login und brechen ab, da sie Phishing oder ähnliches vermuten. Ableitbares Ergebnis: Die vorherigen Kampagnen zur TAN- und Onlinebanking-Sicherheit haben doch zu einem verstärkten Sicherheitsbewusstsein der Anwender geführt, der zusätzliche Supportaufwand für die Banken ist erheblich, aber das ist selbstverschuldet.

Variante 3: Alles läuft glatt. Dann war meine Stichprobe wohl völlig falsch, und es gab außerhalb meines Umfeldes auch für Nicht-c't-Leser doch umfangreiche verständliche Informationen.

Lars H. Kruse

Nano-Nebenwirkungen

Mikro- und Nanoroboter räumen auf, c't 19/2019, S. 144

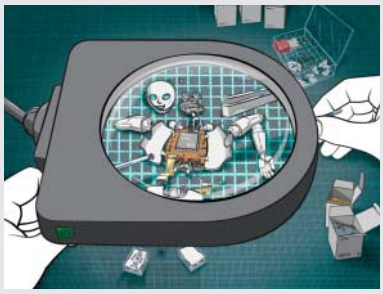


Bild: Rudolf A. Blaha

In c't 19/2019 zeigten wir, wie Nano-Roboter aufräumen. In einer c't-Story aus dem Jahr 2005 waren sie dabei etwas zu gründlich.

Als ich den Artikel „Die Mikrowelt im Griff – Mikro- und Nanoroboter räumen auf" gelesen habe, in dem es auch darum geht, derartige Nanotechnik „freifliegend" im menschlichen Körper einzusetzen, fiel mir sofort wieder ein Text über unfreiwillige Nebenwirkungen ein, die solche Technik haben könnte. Ja, ich habe lange danach suchen müssen, aber ich bin fündig geworden bei der Story aus c't 21/2005 auf Seite 238.

Dietmar Wolle

Negativer Kontrast

Dark Mode mit CSS für Webseiten umsetzen, c't 19/2019, S. 174

Bevor man über Stromsparen spricht, sollte man über die Ergonomie sprechen. Allseits bekannt ist, dass negativer Kontrast die Augen schneller ermüdet, insbesondere dann, wenn die Schrift hell-grell auf dunklem Hintergrund erscheint. Ich für meinen Teil habe, wenn ich zu negativem Kontrast genötigt werde, enorme Schwierigkeiten mit sogenannten Nachbildern. Wenn ich auch nur eine Minute (!) lang solch eine Seite lese und dann wieder normale Bilder vor mir habe, fühlt sich das an, als hätte sich der negative Kontrast in meine Netzhaut eingebrannt. Das ist ein sehr unschönes Gefühl.

van Grunz

Schweigen ist Gold

Warum Sie bei Medizin-Apps unbedingt das Kleingedruckte lesen sollten, c't 17/2019, S. 60

Sie schreiben im letzten Absatz Ihres Kommentars, dass die Patienten die Datenschutzbestimmungen der Gesundheits-Apps gründlich studieren sollen. Da frage ich mich, wie das gehen soll, denn selbst wir als Profis können kaum durchsteigen und verstehen, was tatsächlich mit den Daten passiert. Ihr Satz geht aber noch weiter, nämlich die Gesundheitsdaten im Zweifel nur dem anzuvertrauen, der gesetzlich zum Schweigen verpflichtet ist: dem Arzt.

Warum dann nicht das Problem so auch lösen, wie es das Gesetz im Verhältnis zwischen Patient und Arzt vorschreibt? Da die Gesundheits-App schließlich auch nichts anderes ist als ein virtueller Arzt, könnte das Gesetz auch diese zum Schweigen verpflichten. Das wäre eine simple, aber wirksame Methode, die Gesundheits-Apps nutzbar zu machen, ohne Angst zu haben, dass die Daten an andere weitergegeben werden.

Nikolaus Riehm

BigInt funktioniert nicht

BigInt: Rechnen mit beliebig großen ganzen Zahlen, c't 16/2019, S. 186

Ich habe bincalc-master/index.html in Opera 58 und Chrome-Canary probiert. In beiden Fällen funktioniert der simple Test 23+23 nicht. Es kommt nie ein Ergebnis und „Calculating …" pulsiert. Fehlt da noch etwas? Sollte „?" nicht help.html aufrufen? Bei mir passiert nichts.

Jürgen Bartels

Ihre Problembeschreibung legt nahe, dass Sie die Datei index.html per Doppelklick geöffnet haben. Sie brauchen aber einen Webserver, über den alle im Repository enthaltenen Dateien abrufbar sind. Das war gemeint, als wir im zweiten Absatz (offenbar zu knapp) schrieben: „Speichern Sie die Dateien einfach in ein Verzeichnis Ihrer Wahl unterhalb des Document Root Ihres Webservers – schon können Sie loslegen."

Fragen zu Artikeln

Mail-Adresse des Redakteurs am Ende des Artikels

Artikel-Hotline jeden Montag 16–17 Uhr 05 11/53 52-333