

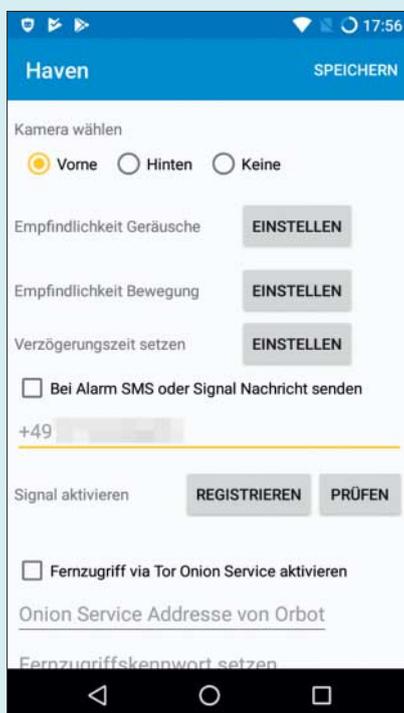
Haven zu Hause?

Edward Snowdens Überwachungs-App Haven soll vor Spionen schützen, c't 3/2018, S. 24

Wie ist die rechtliche Situation, wenn ich das Smartphone zur Wohnraumüberwachung einsetze? Ich glaube kaum, dass ich Eindringlinge vorher fragen muss, ob sie mit einer Überwachung einverstanden sind. ;o) Oder muss im Eingangsbereich ein Hinweis für unberechtigt Eindringende sein, dass die Wohnung videoüberwacht wird?

zirbelkieferr

Die Nutzung zur Wohnraumüberwachung dürfte dann unproblematisch sein, wenn man sicherstellt, dass Personen, die sich dort berechtigterweise aufhalten (Familie, Reinigungspersonal, Handwerker), nicht erfasst werden oder in die Überwachung einwilligen. Tonaufnahmen sind dabei besonders problematisch, da das gesprochene Wort einen speziellen Schutz genießt.



In Edward Snowdens Haven-App kann man zwar die Empfindlichkeit für Geräusche kalibrieren, aber das Mikrophon nicht komplett deaktivieren. Nicht nur das ist in Deutschland problematisch.

Ungleiches Maß

Smartwatches für jeden Anlass, c't 3/2018, S. 84

Der Apple Watch wird als Nachteil gewertet, dass sie nur mit iPhones läuft. Ich vermisste bei den anderen Uhren den Nachteil, dass sie nur mit Android laufen.

Die Uhren mit Tizen und Android Wear funktionieren auch mit iPhones. Im Vergleich zu Android-Smartphones ist der Funktionsumfang unter iOS zwar eingeschränkt, der umgekehrte Weg funktioniert hingegen gar nicht. Grundsätzlich sind für Android-Nutzer die Android-Uhren die erste Wahl und bei iPhone-Besitzern die Apple Watch.

USVs mit besserer Ausstattung

Blackout-Versicherung, Günstige USVs für den Büro-PC, c't 3/2018, S. 110

Schade, dass Sie nicht auch ein teureres Gerät mitgetestet haben, zum Beispiel aus der Serie APC Back-UPS Pro. Ich hätte es schon interessant gefunden, ob man für den Mehrpreis nur ein nettes Display bekommt, unter anderem mit Spannungs- und Leistungsanzeige, oder auch bessere technische Werte.

Jürgen Kamm

Bei der APC Back-UPS Pro gibt es außer einem Display auch größere Akkus, einen höherwertigen Überspannungsschutz und einen schnellen Batteriewechsel per Serviceklappe.

USVs für NAS

Für mein Synology-NAS und eine KNX-Stromversorgung im Keller suche ich eine USV mit USB-Anschluss. Ich habe ab und an Stromausfälle für wenige Sekunden, gerne auch mehrere hintereinander, was für die Platten des NAS natürlich alles andere als optimal ist. Die Leistung der USV ist sekundär. Wichtig ist mir aber der zusätzliche Stromverbrauch: Bei einer angenommenen Nutzungsdauer von fünf Jahren ist da schnell der Anschaffungspreis sekundär, zumindest bei einem Gerätepreis von 40 bis 80 Euro. Ist in der Tabelle unter Leerlaufleistung die erste Zahl die relevante?

Thomas Kern

Wir freuen uns über Post

✉ redaktion@ct.de

💬 c't Forum

📱 c't magazin

🐦 @ctmagazin

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

In der Tabelle haben wir die Leerlaufleistung als Wirk- und Scheinleistung angegeben. Die Wirkleistung in Watt ist für Ihre Stromrechnung die relevante Angabe.

Kapiteltasten fehlen

Der passende E-Book-Reader für (fast) jede Gelegenheit, c't 2/2018, S. 60

Ich besitze selbst einen Reader (Kindle 4 mit Steuerkreuz) und wundere mich etwas, ob ich der einzige bin, der seinen Kindle zum Lesen einer Zeitung (in meinem Fall: Die Zeit) nutzt. Mit meinem Kindle 4 kann ich nämlich wunderbar eine ganze Zeitung lesen, indem ich bequem via Steuerkreuz von Artikel zu Artikel durch die Zeitung springe und auf Bedarf mit den Blätter-Tasten je Artikel einzelne Seiten nach vorne blättern kann.

Leider scheinen Knöpfe aus der Mode gekommen zu sein, da kein mir bekanntes Gerät jene „Kapitel-Blätter-Tasten“ mehr anbietet und ich stattdessen mühsam (via Kontextmenüs) von Kapitel zu Kapitel springen muss. Dies führt nicht zuletzt dazu, dass ich meinen Kindle 4 nach zweimaligem Verlust immer auf eBay durch Gebrauchtgeräte des gleichen Modells ersetzen musste. Jedoch wird jene „Quelle“ ja irgendwann auch versiegen. Haben Sie die gleiche Erfahrung gemacht oder übersehe ich hier etwas? Oder ist vielleicht einfach mein Nutzungsprofil so exotisch?

Stefan Hermes

Geräte mit Steuerkreuz sind uns schon lange nicht mehr untergekommen. Beim Kindle

Anzeige

lässt sich das Springen mit einer Wischgeste von unten und dann über Bildschirmstasten realisieren, aber ist natürlich längst nicht so einfach und schnell. Immerhin kommen Blättertasten wieder etwas häufiger vor, nachdem Touch eine Zeit lang als einzige Eingabemethode übrig zu bleiben schien.

Nicht als root-User

Heimserver hinter DS-Lite oder CG-NAT erreichbar machen, c't 2/2018, S. 138

Ich halte es für ein großes Sicherheitsrisiko, den Tunnel vom privaten Netz auf dem Server im Internet dort als User root aufzubauen, auch wenn er keine Shell hat. Ich würde einen unprivilegierten User auf dem Server vorschlagen, der dann hohe Ports verwendet. Die Umleitung von 80/443 auf die hohen Ports könnte dann in der Firewall (z. B. in PREROUTING) erfolgen.

Gebhard Zocher

Keine Panik

FAQ SSH - Secure Shell, Das richtige Schlüssel-format, c't 3/2018, S. 158

Ich habe mir den Vortrag „Resilient Kryptographie“ angesehen und die Stelle, wo auf die 1000 US-Dollar hingewiesen wird. Der Vortragende bezieht sich dabei auf folgenden Artikel: <https://acmccs.github.io/papers/p1631-nemecA.pdf>. Auf Seite 1640 steht ganz klar, dass für 2048-Bit-RSA-Schlüssel auf einem Amazon Cluster mit 2 Intel E5-2666-CPU's mit @2,9 GHz dann doch 45,98 Jahre Rechenzeit für 40.305 US-Dollar notwendig sind. In der letzten Spalte stehen dann die reinen Energiekosten von 944 US-Dollar.

Das Gemeine an solchen Meldungen ist die Verunsicherung „normaler“ Benutzer. Denn was hängen bleibt ist, dass alle 2048-Bit-RSA-Schlüssel unsicher sind und ein Hack für 1000 US-Dollar zu bekommen ist. Das stimmt so nicht.

R. Zeller

Router für ISDN-Anlagen

ISDN-Abschied rechtzeitig planen, Reserven einbauen, c't 2/2018, S. 120

Wir nutzen einen „Business Complete Premium“-Anschluss mit einer guten alten Eumex 800 als Telefonanlage und warten seit Jahren darauf, in Berlin-Mitte mehr Bandbreite mit einem Anlagenanschluss nutzen zu können. Wir wollen sowohl die SIP als auch unseren Nummernkreis behalten, sind also darauf angewiesen, bei der T-Com zu bleiben. Meine Frage bezieht sich darauf, welche Router mit dem „DeutschlandLAN Sip-Trunk“ kompatibel sind? Im Artikel stehen einige, aber verstehen die sich alle auf Anlagenanschlüsse am SO?

Die Telekom nennt selbst nur zwei Router (von Zyxel) und bei AVM finde ich nur einen sehr vagen Hinweis.

Dipl.-Ing. J. Lindenberg

Das können wir leider auch nicht für beliebige Geräte aus dem Stand sagen – nur ein Blick ins Datenblatt verschafft schnell Klarheit. Ferner vertreibt die Telekom selbst Bntec-, Lancom-, Zyxel- und weitere Geräte, teils unter eigener Marke (siehe ct.de/ysjj). Für die Digitalisierungsboxen sagt die Telekom die SIP-Trunk-Kompatibilität in der herunterladbaren Broschüre selbst zu. Bei den Lancom-Geräten muss man sich zu den Details durchklicken, wo das schon für das kleinste Modell R883 versprochen wird. Beim Zyxel 5501 findet sich nichts zum SIP-Trunk.

Reparaturkosten

Kompakte Notebooks mit CPUs der achten Core-i-Generation, c't 2/2018, S. 110

Außer den sowieso schon sehr hohen Kosten für das Microsoft Surface Book sollte noch die Reparaturpolitik von Microsoft erwähnt werden. Wenn nach der recht kurzen Garantiezeit (1 Jahr) etwas kaputt geht, kostet jede Reparatur: 685,44 Euro

Produkt	Preis (EUR)
Surface Pro 3	567.00
Surface 3	294.00
Surface 3 (LTE)	294.00
Surface Pro 4	450.00
Surface Book	567.00
Surface Studio	892.00
Surface Laptop	450.00
Surface Pro (latest)	450.00

Nach Ablauf der Garantie verlangt Microsoft knackige Gebühren (hier ohne Steuern) für Reparaturen an Surface-Geräten, auch wenn nur ein kleines Teil defekt ist.

(inklusive Mehrwertsteuer)! Mein etwas über ein Jahr altes Surface Book weist seit einiger Zeit einen Riss in der Strg-Taste auf. Etwas, was ich nicht sonderlich ernst genommen habe. Jetzt allerdings droht der Totalausfall der Taste, was mir auf einmal klar macht, wie häufig sie gebraucht wird. Daraufhin habe ich bei Microsoft nachgefragt und als Kostenvoranschlag die 685,44 Euro genannt bekommen. Bezogen auf den Neupreis ist dies natürlich ein Schnäppchen, jedenfalls wenn ich das Gerät aus dem Fenster geworfen hätte – für den Austausch einer Taste halte ich es für mehr als überzogen.

Mark Kahl

Ergänzungen & Berichtigungen

Mehrwert bei Satoshi

Allzeit-Hoch bei Kurs und Gebühren: Taugt Bitcoin noch als Zahlungsmittel?, c't 3/2018, S. 30

Ein Satoshi ist zehn Mal mehr wert als im Artikel beschrieben, nämlich ein hundert-millionstel Bitcoin (1/100.000.000 BTC) und nicht ein milliardstel.

Meltdown/Spectre-Patches brauchen PowerShell 5

Meltdown & Spectre: Update-Guide für Windows, c't 3/2018, S. 66

Die abgedruckten PowerShell-Befehle funktionieren unter Windows 7 nur, wenn die PowerShell mindestens in Version 5 installiert ist. Die wiederum steckt im Windows Management Framework 5.0, zu finden via ct.de/ysjj.

Telekom-Router, PowerShell 5: ct.de/ysjj

Key size	University cluster (Intel E5-2650 v3@3GHz Q2/2014)	Rented Amazon c4 instance (2x Intel E5-2666 v3@2.90GHz, estimated)	Energy-only price (\$0.2/kWh) (Intel E5-2660 v3@2.60GHz, estimated)
512 b	1.93 CPU hours (verified)	0.63 hours, \$0.063	\$0.002
1024 b	97.1 CPU days (verified)	31.71 days, \$76	\$1.78
2048 b	140.8 CPU years	45.98 years, \$40,305	\$944
3072 b	2.84 * 10 ²⁵ years	9.28 * 10 ²⁴ years, \$8.13 * 10 ²⁷	\$1.90 * 10 ²⁶
4096 b	1.28 * 10 ⁹ years	4.18 * 10 ⁸ years, \$3.66 * 10 ¹¹	\$8.58 * 10 ⁹

Die Kosten für das Knacken eines RSA-Schlüssels mit 2048 Bit Schlüssellänge liegen zum Glück weit über 1000 US-Dollar. Dafür bekommt man gerade mal den Strom für die 46 Jahre Rechenzeit.

Bild: Maus Nemecek et. al., Vortrag auf CCS '17