Von Europas größtem IT- und Tech-Magazin

c't magazin für computer technik

Mit Tipps fürs Home-office

Security-Checklisten kompakt

In fünf Minuten absichern: Windows, Smartphone, Router, E-Mail, WhatsApp, Browser, Social Media, Online-Banking, Server, Passwörter, Backups …

So bleiben Ihre Daten im Netz sicher und privat

NEU

Auch als Heft + PDF erhältlich mit 22 % Rabatt

c't Daten schützen

Halten Sie Schnüffler fern und Ihre privaten Daten sicher mit dem neuen c't-Sonderheft Daten schützen 2020!

shop.heise.de/ct-datenschutz20

Einzelheft für nur **12,90 € ›**

Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten. Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

heise shop

shop.heise.de ›

Liebe Leserinnen und Leser,

haben Sie mal fünf Minuten? Mit diesem kleinen Heft machen Sie Hackern das Leben so richtig schwer. Wir haben die wichtigsten Handgriffe zur Absicherung von Smartphone, Rechner, WLAN-Router und vielem mehr für Sie zusammengestellt, Sie müssen diese nur noch umsetzen. Und das dauert in aller Regel nicht länger als fünf Minuten. Zudem erfahren Sie, wie Sie sicher chatten und mailen, was ein gutes Passwort ausmacht und vieles mehr.

Die Checklisten wurden umfassend überarbeitet: So gibt es unter anderem eine neue Homeoffice-Checkliste, mit deren Hilfe Sie auch zu Hause sicher arbeiten können. Damit tun Sie nicht nur sich einen Gefallen, sondern auch Ihrem Arbeitgeber.

Inhalt

Doch nur gemeinsam sind wir stark: Geben Sie dieses Heftchen gern an Familie, Freunde, Kollegen und Mitarbeiter weiter. Wenn Sie das Heft lieber selbst behalten, finden Sie unter **ct.de/check2021** ein kostenloses PDF sowie eine Möglichkeit zum Nachbestellen. Ausführliche Fassungen der Checklisten mit weiteren Tipps finden Sie in c't 20/2020.

Und jetzt frisch ans Werk!

Homeoffice

Zu Hause und sicher arbeiten

Rechner schützen

Sichern Sie Ihren Homeoffice-PC nach dem Stand der Technik – etwa mit den Tipps in diesem Heft. Dazu zählen regelmäßige Betriebssystem-Updates und ein Virenscanner. Ein Virenbefall kann die gesamte Firma lahmlegen.

Daten trennen

Wenn Sie Ihren Homeoffice-Rechner auch privat nutzen, dann verwenden Sie hierfür ein eigenes Nutzerkonto. So bleibt Privates privat. Umgekehrt gilt: Firmendaten haben im Privatkonto nichts verloren.

Verschlüsseln

Achten Sie gut auf die Daten Ihres Arbeitgebers: Geben Sie nichts unbedacht weiter, löschen Sie nicht länger benötigte Dateien und verschlüsseln Sie Ihre Datenträger. Schützen Sie den Rechner mit Sperrbildschirm und Passwort.

Intranetzugriff

Greifen Sie aus dem Homeoffice ausschließlich über eine verschlüsselte VPN-Verbindung auf das Firmennetz zu. Geben Sie den Zugang keinesfalls weiter.

Videochat & Co.

Im Homeoffice stehen Ihnen Ihre Gesprächspartner selten gegenüber. Das wissen auch Cyber-Kriminelle. Seien Sie deshalb skeptisch: Ist der Videochat-Teilnehmer ohne Kamera tatsächlich Ihr Kollege? Stammt die Mail wirklich vom Chef? Rufen Sie im Zweifel lieber an.

Windows

5 Handgriffe für Windows 10

Immer up to date

Stellen Sie regelmäßig sicher, dass alle Updates installiert sind, indem Sie die Einstellungen über das Startmenü aufrufen und auf „Update und Sicherheit“ klicken. Halten Sie auch Apps wie Office, Browser und PDF-Viewer aktuell.

Virenscanner

Ein Virenscanner mit Echtzeitschutz ist unter Windows ratsam. Der Defender reicht aus. Seinen Status erfahren Sie, indem Sie „Windows-Sicherheit“ über das Startmenü aufrufen und auf „Viren- & Bedrohungsschutz“ klicken.

Zugriffsschutz

Vor unbefugten Zugriffen schützen Sie Ihren Rechner am besten, indem Sie seine Festplatte/SSD mit BitLocker oder VeraCrypt verschlüsseln. Sichern Sie Ihren Benutzeraccount mit einem mindestens 10 Zeichen langen Passwort.

Daten schützen

Verhindern Sie, dass mehr Daten an Microsoft fließen als nötig: Suchen Sie im Startmenü nach „Einstellungen für Diagnose und Feedback“ und stellen Sie die Option „Diagnosedaten“ auf „Erforderliche Diagnosedaten“. Nutzen Sie ein lokales Nutzerkonto für Windows.

Daten sichern

Datenträger wie Festplatten und USB-Sticks können jederzeit ausfallen. Erstellen Sie regelmäßig Backups Ihrer wichtigsten Dateien (siehe S. 15).

Smartphone

Android-Smartphones und iPhones absichern

Firmware-Updates

Halten Sie Ihr Smartphone stets auf dem aktuellen Stand, indem Sie verfügbare Firmware-Updates zeitnah installieren. Diese schließen häufig Sicherheitslücken. Bekommt Ihr Gerät keine Updates mehr, sollten Sie über eine Neuanschaffung nachdenken.

Zugriffsschutz

Nutzen Sie die Bildschirmsperre, damit Unbefugte Ihr Smartphone nicht entsperren können. Zum schnellen Entsperren können Sie Passcode, Fingerabdruck oder Gesichtsscan einrichten (je nach Gerät).

Stores nutzen

Installieren Sie am besten nur Apps aus den offiziellen Stores (insbesondere App Store und Google Play), da die Apps hier einem Sicherheits-Check unterzogen wurden.

Berechtigungen

Überprüfen Sie vor der Installation einer App, welche Berechtigungen sie einfordert. Erteilen Sie nur Apps, denen Sie vertrauen, Zugriff auf Kamera, Mikrofon, Standort & Co.

Nicht rooten

Durch „Rooting“ (Android) oder „Jailbreaking“ (iOS) manipulieren Sie essentielle Schutzfunktionen Ihres Smartphones, zudem lassen sich sicherheitsrelevante Apps (etwa Banking-Apps) häufig nicht mehr starten. In den meisten Fällen ist es daher ratsam, das Gerät im Ursprungszustand zu belassen.

WLAN-Router

Schutzmaßnahmen für Fritzbox und andere

Gute Passwörter

Nutzen Sie für alle Gerätedienste wie Dateifreigaben gute Passwörter (siehe S. 16). Das gilt auch für die Konfigurationsoberfläche des Routers, da diese für Angreifer erreichbar sein kann.

Aktuelle Firmware

Router sind beliebte Angriffsziele. Nutzen Sie daher stets die aktuelle und somit sicherste Geräte-Firmware. Schalten Sie automatische Updates ein, wenn möglich.

Dienste schützen

Machen Sie möglichst keine lokalen Dienste über das Internet zugänglich – und wenn doch, dann nur mit Passwortschutz und verschlüsselt. Greifen Sie unterwegs am besten über VPN auf Dienste im Heimnetz zu.

Sicheres WLAN

Stellen Sie als Verschlüsselung mindestens WPA2, besser WPA3 ein. Nutzen Sie ein zufälliges WLAN-Passwort mit mindestens 16 Zeichen. Öffnen Sie für Gäste und Smarthome-Geräte ein Gastnetz mit separatem Passwort. Aktivieren Sie wenn möglich den Schutz für Steuerpakete (PMF).

WPS und UPnP aus

WPS und UPnP sind Komfortfunktionen, die in der Vergangenheit immer wieder von Angreifern missbraucht wurden, um Router zu kapern. Schalten Sie beide über das Webinterface des Routers aus, wenn möglich.

E-Mail

Mailen ohne Mitleser

Gesundes Misstrauen

Manchmal kommen Mails nicht vom vorgeblichen Absender: Für Phishing-Attacken fälschen Angreifer die Absender und kopieren etwa das Layout von Bank-Mails perfekt. In einigen Fällen knüpfen Angreifer sogar an bestehende Konversationen an. Werden Sie besonders misstrauisch, wenn Links, Anhänge oder Geld im Spiel sind.

Mail-Client absichern

Lassen Sie Ihren Mailclient keine externen Inhalte nachladen und nutzen Sie die HTML-Ansicht nicht als Standard. Stellen Sie außerdem sicher, dass Ihr Mailclient nur transportverschlüsselt mit dem Mailserver spricht.

Zusatzschutz

Nutzen Sie eine Zwei-Faktor-Authentifizierung (2FA), wenn möglich. Manche Anbieter erlauben auch, Mails bei Eingang automatisch zu verschlüsseln oder nur zu versenden, wenn eine transportverschlüsselte Verbindung zum Zielserver aufgebaut werden kann.

Überlegt nutzen

„Allen antworten“? wird schnell zum Problem: Entfernen Sie überflüssige Empfänger und Informationen aus zitierten Nachrichten. Ausführbare Dateien und Dokumente mit Makros sollten weder verschickt noch empfangen werden und manch heikle Information ist in einem Telefonat besser aufgehoben.

WhatsApp & Co.

Sicher chatten

Verschlüsselt chatten

Nutzen Sie Messenger, die Ende-zu-Ende-verschlüsseln (wie Signal oder WhatsApp) oder das zumindest als Option bieten (wie Telegram oder Facebook Messenger). Letzteres wird oft „geheimer Chat“ genannt und muss explizit gestartet werden.

Wer hört mit?

Viele Messenger bieten Web- oder Desktop-Clients als Zusatz zur App. Einmal eingerichtet lassen sich darüber sämtliche Chats mitlesen. Prüfen Sie also regelmäßig, ob andere Geräte mit der Messenger-App verknüpft sind.

Backup kontrollieren

Backups sind wichtig, aber auch ein mögliches Datenleck: Überprüfen Sie, ob es wirklich in die Cloud erfolgen muss und wie die Daten abgelegt werden.

PIN setzen

Viele Messenger sind an eine Handynummer gebunden. Die wird per SMS bestätigt, aber SMS lassen sich umleiten. Messenger wie WhatsApp, Telegram oder Signal bieten daher an, den Prozess mit einer zusätzlichen PIN abzusichern. Nutzen Sie dieses Feature und bewahren Sie die PIN gut auf.

Betrug erkennen

Betrüger und Kettenbriefe gibt es auch bei Messengern. Seien Sie skeptisch, öffnen Sie keine unerwarteten Links und leiten Sie nur weiter, was Sie überprüft haben.

Browser

Die wichtigsten Handgriffe für Chrome, Firefox, Edge und weitere

Aktuell bleiben

Nutzen Sie stets die neueste Browserversion, da in alten Versionen meist Sicherheitslücken klaffen. Stellen Sie sicher, dass sich der Browser automatisch mit Updates versorgt.

Add-ons checken

Viele Erweiterungen haben Zugriff auf alle Inhalte sämtlicher besuchter Webseiten, auch auf das Online-Banking. Werfen Sie ungenutzte Erweiterungen aus dem Browser.

Tracker blockieren

Firefox, Microsoft Edge und Safari bringen Trackingblocker mit. Schalten Sie sie scharf. Bei Chrome können Sie Tracker mit der Erweiterung uBlock Origin blockieren.

Berechtigungen

Websites können Berechtigungen einfordern, um etwa auf die Kamera, das Mikrofon und den Standort zuzugreifen. Gestatten Sie dies nur, wenn es unbedingt nötig ist. Die erteilten Berechtigungen können Sie in den Datenschutzoptionen der Browser einsehen und löschen.

Adressen checken

Geben Sie persönliche Daten nur auf Websites ein, die verschlüsselt ausgeliefert werden (Adresse beginnt mit https:// beziehungsweise der Browser zeigt ein geschlossenes Schlosssymbol neben der Adresse an). Überprüfen Sie die Domain der Website genau.

Social Media

Facebook, Twitter, Instagram & Co.

Zwei Faktoren nutzen

Nutzen Sie eine Zwei-Faktor-Authentifizierung (2FA), wenn möglich. 2FA per App wie Google Authenticator ist sicherer als via SMS.

Zugriffe checken

Bei vielen sozialen Netzen können Sie Diensten und Apps den Zugriff auf Ihren Account gewähren. Kontrollieren Sie diese Liste regelmäßig und entfernen Sie alle Drittanbieterdienste, die Sie nicht länger nutzen.

Gezielt teilen

Bei Facebook, aber auch bei anderen Anbietern kann man festlegen, mit wem man Inhalte teilen möchte – etwa mit individuellen Freundeslisten. Nutzen Sie dies, um Inhalte nur mit Personen zu teilen, die sie auch sehen dürfen.

Anfragen checken

Oft steckt hinter Freundschaftsanfragen der Versuch, persönliche Daten abzugreifen. Checken Sie jede Anfrage sorgfältig. Ist das Mitglied frisch dabei und hat viele neue Kontakte, kann das auf einen Betrug hindeuten.

Private Nachrichten

Selbst von Nachrichten Ihrer Kontakte kann Gefahr ausgehen: Hacker übernehmen Accounts und verschicken in fremdem Namen gefährliche Links oder fragen nach Geld. Seien Sie skeptisch und fragen Sie Ihren Kontakt im Zweifel über einen anderen Kanal, was es damit auf sich hat.

Online-Banking

Bankgeschäfte ohne Kummer

Transaktion checken

Checken Sie bei Online-Überweisungen das Zielkonto und die Summe auf dem TAN-Generator, in der App Ihrer Bank oder auf dem Kartenleser und vergleichen Sie sie wenn möglich mit der Rechnung.

Banking virenfrei

Banking mit dem PC oder Smartphone ist nur sicher, wenn das System virenfrei ist. Sorgen Sie dafür, dass auf Ihrem PC ein Virenscanner mit aktuellen Updates aktiv ist (siehe Seite 5).

Phishing erkennen

Online-Betrüger verschicken massenhaft Mails im Namen von Bankinstituten, um Trojaner einzuschleusen oder Zugangsdaten abzugreifen (Phishing). Geben Sie Ihre Zugangsdaten nur auf der Webseite der Bank (Adresse selbst eintippen oder per Bookmark ansteuern) oder in Ihrer Online-Banking-Software ein.

Belege überprüfen

Insbesondere Kreditkartennutzer sollten jede Abrechnung kontrollieren und unbefugte Abbuchungen umgehend an ihre Bank melden. Auch Ihre Kontoauszüge sollten Sie regelmäßig prüfen.

Handy nicht rooten

Rooten oder jailbreaken Sie Ihr Smartphone oder Tablet nicht, da Sie damit wichtige Schutzfunktionen lahmlegen. Viele Banken-Apps starten auf modifizierten Geräten aus diesem Grund gar nicht erst.

Backups

Daten sicher sichern

Machen!

Das Wichtigste am Backup ist, es auch wirklich zu machen – der richtige Zeitpunkt, um damit anzufangen, ist: jetzt!

Alles besser als nichts

Schutz vor Datenverlusten bietet so ziemlich jede Kopie, die getrennt vom Original abgelegt ist. Selbst ein Ausdruck auf Papier ist besser als nichts.

Trojanersicher

Verschlüsselungstrojaner greifen alles an, was sie erreichen können. Daher ist ein Backup nur dann zuverlässig, wenn es sich auf keinem Weg von Ihrem PC aus erreichen lässt.

Feuerfest

Damit im Ernstfall Original und Kopie nicht gemeinsam durch Feuer oder Löschwasser vernichtet werden, lagern Sie mindestens eine Kopie außer Haus.

Diebstahlsicher

Wenn ein Dieb Zugriff auf das Backup-Medium erlangt, kann er die Daten darauf lesen. Lagern Sie es also am besten in einem feuerfesten Tresor.

Wiederherstellen

Solange Sie Ihr Backup nicht testweise wiederhergestellt haben, darf es nicht als zuverlässig gelten.

Wiederholen

Backups veralten, weil die seitdem hinzugekommenen Daten naturgemäß nicht enthalten sind. Sichern Sie Ihre Daten also regelmäßig.

Passwörter & Accounts

Was wirklich zählt

Kein Recycling

Nutzen Sie für jede Website und jede Anwendung ein individuelles Passwort. Wer für mehrere Websites das gleiche Passwort nutzt, ist leichte Beute: Wird eine Site gehackt, kann sich der Angreifer auch in alle anderen einloggen.

Lang statt komplex

Nutzen Sie lieber möglichst lange Kennwörter statt möglichst viele Sonderzeichen. Die Länge ist die effektivste Stellschraube, um das Knacken des Kennworts hinauszuzögern.

Passwortmanager

Speichern Sie Ihre Passwörter auf keinen Fall unverschlüsselt auf dem Rechner. Nutzen Sie einen Passwortmanager wie KeePass oder LastPass, um Zugangsdaten sicher verschlüsselt aufzubewahren. Wenn Sie Passwörter im Browser speichern, sollten Sie dafür ein Master-Passwort setzen, wenn möglich.

Zettel und Stift

Der einfachste Passwortspeicher ist ein Zettel, den Sie an einem sicheren Ort aufbewahren. Auf Geldbörse oder Tresor hat kein Trojaner Zugriff.

Zwei Faktoren

Nutzen Sie bei Webdiensten wann immer es geht die Zwei-Faktor-Authentifizierung, um Ihre Accounts effektiv vor Hackern zu schützen. Alternativ können Sie häufig einen USB-Sicherheitsschlüssel nutzen (U2F oder FIDO2).

Server & Hosting

Für Admins & Webmaster: So sperren Sie Hacker aus

Zwei Faktoren

Schützen Sie sämtliche Admin-Accounts durch einen zweiten Faktor (etwa U2F/FIDO2), wenn möglich. Bieten Sie auch Ihren Nutzern eine Zwei-Faktor-Authentifizierung an.

Sicherer Zugriff

FTP ist unsicher, weil es nicht verschlüsselt. Nutzen Sie SFTP oder FTPS, um Inhalte hochzuladen, und schalten Sie FTP am besten ab. Sichern Sie den SSH-Zugang, indem Sie die Anmeldung per Passwort deaktivieren, und authentifizieren Sie sich stattdessen per Public-Key-Verfahren.

Aktuell halten

Serverbetriebssystem, Dienste und Webanwendungen sind leichte Beute für Hacker, wenn nicht alle Security-Patches installiert sind. Stellen Sie regelmäßig sicher, dass alles auf dem aktuellen Stand ist.

Logfiles checken

Behalten Sie relevante Log-Dateien im Blick, um Angriffe und Infektionen zu erkennen. Fail2ban (Unix) und RdpGuard (Windows) entdecken Brute-Force-Attacken in den Logs und setzen die IP-Adressen der Angreifer automatisch auf die Blacklist.

Passwörter hashen

Speichern Sie niemals Klartextpasswörter Ihrer Nutzer. Nutzen Sie stattdessen ein modernes Hash-Verfahren wie PBKDF2. Speichern Sie darüber hinaus so wenige Daten wie möglich über Ihre Nutzer.

Impressum

Redaktion
Karl-Wiechert-Allee 10,
30625 Hannover
Telefon: 05 11/53 52-300
Telefax: 05 11/53 52-417
Internet: www.ct.de

Chefredakteur: Dr. Jürgen Rink (jr) (verantwortlich für den Textteil)

Koordination: Ronald Eikenberg (rei@ct.de)

Art Direction: Nicole Judith Hoehne

DTP-Produktion: Matthias Timm, Heise Medienwerk GmbH & Co. KG, Rostock

Verlag
Heise Medien GmbH & Co. KG
Karl-Wiechert-Allee 10,
30625 Hannover
Telefon: 05 11/53 52-0
Telefax: 05 11/53 52-129
Internet: www.heise.de

Herausgeber: Christian Heise, Ansgar Heise, Christian Persson

Geschäftsführer: Ansgar Heise, Dr. Alfons Schräder

Mitglied der Geschäftsleitung: Beate Gerold, Jörg Mühle

Verlagsleiter: Dr. Alfons Schräder

Anzeigenleiter: Michael Hanke (-167, verantwortlich für den Anzeigenteil), www.heise.de/mediadaten/ct/

Leiter Vertrieb und Marketing: André Lux (-299)

Druck: QUBUS Media, Utermöhlestraße 9, 31135 Hildesheim

// heise devSec()

Die Konferenz für sichere Software- und Webentwicklung

ONLINE – 21. UND 22. OKTOBER 2020

Frühbucherrabatt
bis zum 23. September

Sichere Software beginnt vor der ersten Zeile Code …

THEMEN SIND UNTER ANDEREM:

- Agile Threat Modeling
- OWASP Top 10 und OWASP API Security Top 10
- Jakarta EE Security und MicroProfile JWT
- Was kann C++ von Rust klauen?
- Cloud-Security auf dem Prüfstand

Nehmen Sie über Ihren Browser bequem vom Büro oder Homeoffice teil, tauschen Sie sich per Text- und Videochat mit Teilnehmern und Referenten aus, und nutzen Sie das Videoarchiv, um im Nachgang alle Vorträge anzuschauen.

www.heise-devsec.de

Goldsponsoren: WIBU SYSTEMS, ANITIZER ... because security matters

Silbersponsoren: COLOGNE INTELLIGENCE, WINGS-FERNSTUDIUM AN DER HOCHSCHULE WISMAR

Veranstalter: heise Security, heise Developer, dpunkt.verlag