Von Europas größtem IT- und Tech-Magazin

c't magazin für computer technik

Neu: Tipps für mobiles Arbeiten

Security-Checklisten kompakt

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

Liebe Leserinnen und Leser,

unser digitaler Alltag ist im Wandel – mehr denn je. Viele Firmen bieten weiterhin eine gewisse Flexibilität bei der Wahl des Arbeitsortes. Doch wer zu Hause, im Stadtpark oder im ICE produktiv sein möchte, muss die Sicherheit seiner technischen Begleiter im Griff haben, denn überall lauern unterschiedliche Gefahren.

Um der neuen Situation gerecht zu werden, finden Sie in der diesjährigen Ausgabe unserer Security-Checklisten eine Zusammenfassung der wichtigsten Handgriffe, um überall sicher zu arbeiten. Auch bei der Absicherung Ihrer privat genutzten Smartphones, Rechner, Router, Online-Dienste & Co. lassen wir Sie natürlich nicht im Stich. Zu jeder Checkliste finden Sie eine ausführliche Fassung mit weiteren Tipps in der c't-Ausgabe 20/2021.

Inhalt

Es sind nur wenige Handgriffe nötig, um vor den häufigsten Cyber-Gefahren geschützt zu sein. Diese Zeit sollten Sie sich nehmen! Geben Sie dieses Booklet gern an Freunde, Verwandte, Kollegen weiter oder die PDF-Variante, die Sie unter **ct.de/check2022** finden. Dort ist auch eine begrenzte Stückzahl gedruckter Exemplare nachbestellbar.

Mobiles Arbeiten

Sicher hybrid arbeiten zwischen Homeoffice und Firma

Rechner schützen

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

Daten trennen

Wenn Sie Ihre Geräte auch privat nutzen, dann verwenden Sie hierfür eigene Nutzerkonten. 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 Rechner, Notebooks, Smartphones und Tablets mit Sperrbildschirm und Passwort.

Intranetzugriff

Greifen Sie außerhalb des Büros ausschließlich über eine verschlüsselte VPN-Verbindung auf das Firmennetz zu. Geben Sie den Zugang keinesfalls weiter. Meiden Sie öffentliche WLANs (Hotspots).

Videochat & Co.

Im Homeoffice stehen Ihnen Ihre Gesprächspartner selten gegenüber. 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

Grundschutz für Windows

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. Gibt es neue Updates, klicken Sie einfach auf „Jetzt installieren“. Halten Sie auch Programme wie Office, Browser und PDF-Viewer aktuell.

Daten sichern

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

Virenscanner

Ein Virenscanner mit Echtzeitschutz ist unter Windows ratsam. Der vorinstallierte 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 den internen Datenträger mit BitLocker oder VeraCrypt verschlüsseln. Sichern Sie Ihren Account mit einem Passwort und sperren Sie den Rechner, wenn Sie ihn verlassen.

Daten schützen

Suchen Sie im Startmenü nach „Einstellungen für Diagnose und Feedback“ und stellen Sie die Option „Diagnosedaten“ auf „Erforderliche Diagnosedaten“. Verwenden Sie ein lokales Konto für Windows, wenn möglich.

Smartphone

Android-Smartphones und iPhones absichern

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 einfach benutzen können. Zum schnellen Entsperren können Sie Passcode, Fingerabdruck oder Gesichtsscan einrichten.

Stores nutzen

Wer nicht genau weiß, was er tut, sollte nur Apps aus den offiziellen Stores (insbesondere App Store und Google Play) installieren. Die Apps werden dort einem Sicherheits-Check unterzogen.

Berechtigungen

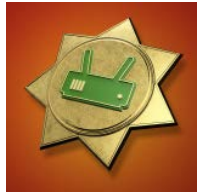
Überprüfen Sie vor der Installation einer App, welche Berechtigungen sie einfordert. Erteilen Sie Zugriff auf Kamera, Mikrofon, Standort & Co nur, wenn die App das nachvollziehbar benötigt und Sie ihr vertrauen.

Nicht rooten

Durch „Rooting“ (Android) oder „Jailbreaking“ (iOS) manipulieren Sie essenzielle 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 – 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 für Ihr WLAN 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 bei Fritzboxen die „geschützte Anmeldungen von WLAN-Geräten (PMF)“, wenn möglich.

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

E-Mails lassen sich leicht manipulieren. Angreifer können Absender fälschen, das Layout (etwa von einer Bankmail) perfekt kopieren und sogar fehlerfrei an bestehende Konversationen anknüpfen. Seien Sie also misstrauisch, besonders wenn Links, Anhänge oder Geld im Spiel sind oder der Mailinhalt bedrohlich wirkt.

Mail-Client absichern

Lassen Sie Ihren Mailclient keine externen Inhalte nachladen und nutzen Sie möglichst keine HTML-Ansicht. Stellen Sie außerdem sicher, dass Ihr Mailclient nur verschlüsselt per TLS/STARTTLS 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 Transportverschlüsselung zum Zielserver aufgebaut werden kann – aktivieren Sie solche Optionen Ihres Anbieters.

Überlegt nutzen

Entfernen Sie überflüssige Empfänger und Informationen aus zitierten Nachrichten. Ausführbare Dateien und Dokumente mit Makros sollten weder verschickt noch empfangen werden und heikle Informationen sind oft besser in einem Telefonat aufgehoben.

Messenger

Sicher chatten mit WhatsApp, Signal & Co.

Verschlüsselung

Nutzen Sie Messenger, die automatisch Ende-zu-Ende-verschlüsseln (etwa Signal, Threema, WhatsApp oder Wire) oder Ihnen zumindest die Option bieten (wie Telegram oder der Facebook Messenger). Einzig in ohnehin öffentlichen Gruppen mag Ende-zu-Ende-Verschlüsselung verzichtbar sein.

Backup kontrollieren

Ein Backup ist wichtig, aber auch ein mögliches Datenleck: Überprüfen Sie, ob es wirklich in die Cloud erfolgen muss und ob die Daten verschlüsselt abgelegt 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.

PIN setzen

Viele Messenger sind an eine Handynummer gebunden, die per SMS verifiziert wird. Weil Nummern wechseln und SMS umgeleitet werden können, erlauben viele Messenger 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

Wichtige Handgriffe für Chrome, Firefox, Edge & Co.

Aktuell bleiben

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

Add-ons checken

Viele Erweiterungen haben Zugriff auf alle Inhalte sämtlicher besuchter Webseiten, auch beim Online-Banking. Werfen Sie ungenutzte Erweiterungen aus dem Browser und deaktivieren Sie solche, die Sie nur selten brauchen.

Tracker blockieren

Mittlerweile bringen viele Browser Trackingblocker mit. Schalten Sie sie scharf. Alternativ oder zusätzlich können Sie Erweiterungen wie uBlock Origin nutzen.

Berechtigungen

Websites können Berechtigungen einfordern, um etwa auf Kamera und Standort zuzugreifen. Gestatten Sie dies nur, wenn es wirklich nötig ist. Erteilte Berechtigungen können Sie in den Browseroptionen einsehen und löschen.

Adressen prüfen

Geben Sie sensible Daten nur auf Websites ein, die verschlüsselt ausgeliefert werden (Adresse beginnt mit „https://“ oder der Browser zeigt ein geschlossenes Schlosssymbol neben der Adresse an). Überprüfen Sie die Domain der Website genau; Ihnen bekannte Adressen öffnen Sie besser per manueller Eingabe oder über ein Bookmark als über einen zugeschickten Link.

Social Media

Facebook, Twitter, Instagram & Co.

Zwei Faktoren nutzen

Nutzen Sie eine Zwei-Faktor-Authentifizierung (2FA), wenn möglich. 2FA mit einer 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 durch individuelle 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 Betrugsabsichten 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

Prüfen 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 es wenn möglich mit der Rechnung.

Banking virenfrei

Banking mit dem PC oder Smartphone ist nur sicher, wenn das System geschützt ist. Halten Sie es mit Updates aktuell und nutzen auf dem PC einen Virenscanner (siehe Seite 5 und 6).

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 Website der Bank (Adresse selbst eintippen oder per Bookmark ansteuern) oder in Ihrer Online-Banking-App 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 ist 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 und sicher, wenn es sich von Ihrem PC aus nicht 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 darauf gespeicherten Daten lesen. Lagern Sie es am besten an einem sicheren Ort, etwa in einem feuerfesten Tresor, oder verschlüsseln Sie es.

Testen!

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

Wiederholen

Backups veralten, weil die nach ihrer Erstellung 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 dasselbe 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. Beides hilft, aber die Länge ist eine viel effektivere 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 Bitwarden, um Zugangsdaten sicher verschlüsselt aufzubewahren. Wenn Sie Passwörter im Browser speichern, sollten Sie dafür ein Master-Passwort setzen.

Leaks checken

Überprüfen Sie von Zeit zu Zeit, ob Ihre Online-Accounts gehackt wurden und im Darknet kursieren. Hierfür können Sie die kostenlosen Dienste **sec.hpi.de/ilc** und **haveibeenpwned.com** nutzen (siehe auch ct.de/check2022).

Zwei Faktoren

Nutzen Sie bei Webdiensten wann immer es geht die Zwei-Faktor-Authentifizierung, um Ihre Accounts effektiv vor Hackern zu schützen. Am besten mit einem USB-Sicherheitsschlüssel (U2F oder FIDO2).

Server & Hosting

Für Admins & Webmaster: So sperren Sie Hacker aus

Zwei Faktoren

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

Sicherer Zugriff

Nutzen Sie keine unverschlüsselten Protokolle, sondern nur solche mit Transportverschlüsselung: Setzen Sie SFTP oder FTPS ein, um Inhalte hochzuladen, und schalten Sie FTP am besten ab. Webseiten nur per HTTPS anbieten. Bei SSH die Anmeldung per Passwort abschalten und stattdessen per Public Key anmelden.

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, am besten automatisch.

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)

Koordinator: Ronald Eikenberg
(rei@ct.de)

DTP-Produktion: Astrid Seifert

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

Herausgeber: Christian Heise,
Ansgar Heise, Christian Persson

Geschäftsführer: Ansgar Heise,
Dr. Alfons Schräder

Mitglied der Geschäftsleitung:
Beate Gerold, Jörg Mühle

Verlagsleitung: Dr. Alfons Schräder

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

Leiter Vertrieb und Marketing:
Andre Lux (-299)

Druck: QUBUS media GmbH,
Beckstraße 10,
30457 Hannover