Halt, Stopp! Virenpolizei!

Die c’t-Security-Checklisten 2023

Bild: Andreas Martini

Ein Moment der Unaufmerksamkeit, fehlende Schutzmaßnahmen oder ein schlecht konfiguriertes Betriebssystem, all das hilft Hackern, in Ihr System einzubrechen. Mit unseren Checklisten sichern Sie Ihre Geräte in wenigen Minuten ab und verhindern Schlimmeres im Falle einer Infiltration.

Von Wilhelm Drehling

Künstliche Intelligenz (KI) überrollt förmlich das Netz und schleicht sich immer mehr in den Alltag hinein. Die neuen KI-Helferlein unterstützen beim Schreiben, beantworten Fragen, retuschieren Bilder, geben aber zum Teil krude, wenn auch glaubhafte Antworten. Deshalb ist es wichtig, kritisch gegenüber den neuen Tools zu bleiben. Auch wenn sie sinnvolle Einsatzmöglichkeiten bieten, empfehlen wir einen vorsichtigen Umgang mit den KI-Werkzeugen. Nicht selten steht in den AGBs, dass die Anbieter sich die von Nutzern gestellten Fragen und hochgeladenes Material einverleiben dürfen, um ihre Tools weiterzuentwickeln. Das ist zwar kein typischer Angriff in Form eines Trojaners oder Hackerangriffs, betrifft aber trotzdem Ihre persönlichen Daten. Mehr dazu lesen Sie auf Seite 8.

Aufgepasst!

Es genügen ein paar Handgriffe, um Ihr Netzwerk, Ihr Smartphone und Ihren Rechner gegen die gröbsten Angriffe zu rüsten. Klar, das ist kein allumfassender Schutz, der Hightech-Viren fernhält. Da aber die meisten Angriffe einfach zu schließende Lücken ausnutzen, sind Sie mit unseren Empfehlungen erstklassig dagegen gewappnet. Außerdem sind die meisten in wenigen Minuten erledigt, so viel Zeit muss sein. Aus diesem Grund haben wir die Security-Checklisten der vergangenen Jahren auf den neuesten Stand gebracht.

Wie Sie es vielleicht schon kennen, sind unsere Empfehlungen thematisch sortiert: Los geht es mit Tipps zum Homeoffice (S. 3). Der Arbeitsplatz zu Hause ist gekommen, um zu bleiben, und sollte aufgrund der direkten Verbindungen ins Netzwerk des Unternehmens besonders geschützt werden. Da geschäftliche Mailkonten nicht selten ein bevorzugtes Ziel von Phishing-Versuchen sind, finden Sie auf Seite 7 Ratschläge, um Betrügermails zu enttarnen. Tipps und Tricks zu Windows (S. 4), Smartphone (S. 5) und WLAN-Router (S. 6) runden das Paket ab.

Seien Sie auf der Hut bei SMS-Nachrichten, die zum Kontakt mit anderen Nummern auffordern und kontaktieren Sie zur Sicherheit über Zweitkanäle Familie und Verwandte, um die Herkunft der SMS zu bestätigen.

Auch nach Feierabend haben es Betrüger auf Ihr Geld abgesehen, seien Sie also achtsam bei Transaktionen im Browser (S. 10), vor allem wenn Sie Überweisungen via Onlinebanking (S. 12) erledigen. Nutzen Sie immer eine Zwei-Faktor-Authentifizierung. Passen Sie bei Mails auf, die angeblich von Ihrer Bank stammen und Sie dazu auffordern, Ihre Anmeldedaten zu bestätigen. Es handelt sich hierbei häufig um raffinierte Phishing-Versuche!

Ein falscher Klick und schon sind die Bilder vom letzten Urlaub weg oder schlimmer noch wichtige Dokumente wie Steuerunterlagen. Daten, die Sie schützen möchten, sollten Sie absichern und zusätzlich in Form eines Backups aufbewahren (S. 13) – ein USB-Stick reicht aus. Sollten Sie zudem einen eigenen Server (S. 14) betreiben, müssen Sie sichergehen, dass dieser immer auf dem aktuellen Stand ist. Loggen Sie sich stets via SSH ein und verwenden Sie anstatt eines Passworts lieber das Public-Key-Verfahren.

Auch wenn mit Passkeys [1, 2] Passwörter obsolet werden dürften, sollten Sie nach wie vor schwierige Passwörter wählen oder einen vertrauenswürdigen Passwortmanager benutzen (siehe S. 15). Und noch ein guter Rat: Bewegen Sie sich vorsichtig auf den üblichen Messengerdiensten (S. 9) sowie diversen Social-Media-Plattformen (S. 11) und glauben Sie nicht jeder eintrudelnden Nachricht. Betrüger denken sich immerzu neue perfidere Maschen aus (siehe Screenshot links).

Weitergeben

Damit sich unsere Tipps möglichst weit herumsprechen, haben wir sie in einem kostenfreien PDF-Booklet zusammengefasst. Dieses können Sie über ct.de/ytrq herunterladen und dann nach Belieben an Freunde, Familie und Bekannte verteilen. Und nun ran ans Werk! *(wid@ct.de)* c't

Literatur

[1] Kathrin Stoll, Tschüss Passwort?, So funktionieren Passkeys, c't 26/2022, S. 126
[2] Ronald Eikenberg, Zukunft ohne Passwort, Bestandsaufnahme: Passwort-Nachfolger Passkeys, c't 13/2023, S. 12

PDF-Booklet kostenfrei herunterladen:
ct.de/ytrq

Home und Office

Security-Checkliste Mobiles Arbeiten

Bild: Andreas Martini

Das Homeoffice ist gekommen, um zu bleiben. Viele arbeiten zu Hause oder im Zug – und manche gleich dort, wo andere Urlaub machen. Auch Angreifern gefällt das, denn die externen Arbeitsplätze sind eine potenzielle Schwachstelle im Unternehmensnetz.

Von Andrea Trinkwalder

Arbeitsplatz abschirmen

Sichern Sie Ihren Homeoffice-Rechner und alle mobilen Arbeitsgeräte nach dem Stand der Technik. Dazu zählen regelmäßige Betriebssystemupdates und ein Virenscanner (siehe S. 5). Denn ein eingefangener Virus kann die gesamte Firma lahmlegen. Greifen Sie aus dem Homeoffice und unterwegs über eine verschlüsselte VPN-Verbindung auf das Firmennetz zu. Meiden Sie öffentliche WLAN-Hotspots, nutzen Sie stattdessen eine mobile Datenverbindung (4G/5G).

Schützen Sie Ihre Geräte und Daten auch vor direkten, physischen Zugriffen von Unbefugten. Ein Dieb, der Ihr Notebook geklaut hat, darf nicht auch noch Ihre Daten erbeuten. Bei mobilen Rechnern sollte der Massenspeicher daher verschlüsselt sein, zum Beispiel mit BitLocker oder VeraCrypt. Das gilt auch für USB-Sticks und andere externe Datenträger. Defekte Speichermedien entsorgen Sie nicht selbst, sondern über die Firma. Nur dann ist gewährleistet, dass sensible Informationen sicher gelöscht werden.

Aktivieren Sie Ortungs- und Fernlöschfunktionen. Suchen Sie sich unterwegs zum Arbeiten einen Platz, der vor neugierigen Blicken schützt. Richten Sie eine passwortgeschützte Bildschirmsperre ein und nutzen Sie diese konsequent, auch wenn Sie den Rechner nur kurz aus den Augen lassen (unter Windows mit Windows+L). Am besten ist ein passwortgeschützter Bildschirmschoner, der sich nach kurzer Inaktivität automatisch einschaltet.

Daten trennen

Wenn Sie Ihren privaten Rechner für die Arbeit im Homeoffice nutzen, dann richten Sie hierfür ein eigenes Nutzerkonto ein. So bleibt Privates privat. Umgekehrt gilt: Firmendaten haben im Privatkonto nichts verloren. Greifen Sie auch auf Ihre privat genutzten Cloudkonten wie Dropbox, OneDrive oder Google Drive nicht vom Arbeitskonto aus zu.

Um auf dem Smartphone berufliche von privaten Kontakten zu separieren, arbeiten Sie ebenfalls mit zusätzlichen Nutzerkonten, sofern möglich.

Verlust vermeiden

Speichern Sie wichtige, beruflich genutzte Dokumente und Daten nicht lokal auf Ihrem Rechner, Notebook oder Tablet, sondern möglichst auf dem Firmenserver. Das ist nicht nur sicherer, sondern vor allem beim hybriden Arbeiten deutlich komfortabler. Denn dort werden automatisch Backups angelegt und Sie haben gleich alles parat, wenn Sie vom Home- ins Firmen-Office wechseln. Falls Daten doch mal lokal gespeichert werden müssen, richten Sie zumindest eine automatische Synchronisierung per Backupsoftware ein. Verzichten Sie möglichst darauf, Dokumente auf USB-Sticks und externen Platten hin- und herzutragen.

Konferenzen kontrollieren

Virenschutz hin, Firewall her: Die größte Schwachstelle in der Firmen-IT ist immer noch der Mensch. Im Homeoffice stehen Ihnen Ihre Gesprächspartner selten gegenüber. Videochat-Teilnehmer ohne Kamera können Kollegen sein, aber auch Angreifer, die mitlauschen wollen. Fordern Sie die Kollegen zunächst auf, die Kamera zu aktivieren und starten Sie das Meeting neu, wenn die Geisterbilder nicht verschwinden.

Übrigens: Die beliebten Screenshots von Videokonferenzen können wertvolle Informationen für Angreifer enthalten, um sich entweder direkt ins nächste Meeting einzuklinken oder Phishing-Attacken vorzubereiten. Wenn Sie unbedingt Fotos vom letzten Meeting veröffentlichen müssen, machen Sie vorher sensible Daten wie URLs, Meeting-IDs sowie die Gesichter der Teilnehmer unkenntlich.

Anrufe & Mails hinterfragen

Nicht alles läuft auf Anhieb perfekt. Bleiben Sie auch aus der Ferne in Kontakt mit den Admins Ihrer Firma und erstellen Sie beizeiten eine Liste mit wichtigen Ansprechpartnern für den Notfall.

Anrufen und Mails sollten Sie grundsätzlich skeptisch gegenüberstehen, denn Caller-IDs und Absendernamen können gefälscht sein. Meldet sich etwa vermeintlich Ihr Lieblings-Admin oder ein Geschäftspartner telefonisch bei Ihnen, sollten Sie keine sensiblen Daten preisgeben und sich schon gar nicht auf eine Fernwartung einlassen. Selbst den vertrauten Stimmen müssen Sie zunehmend mit Skepsis begegnen, denn sie lassen sich immer besser synthetisch nachahmen. Rufen Sie bei geringstem Zweifel lieber unter der Ihnen bekannten Rufnummer zurück. *(atr@ct.de)* c't

Fenster abschließen

Security-Checkliste Windows

Bild: Andreas Martini

Auf Windows haben es Hacker besonders häufig abgesehen – schlicht, weil es so verbreitet ist. Die gute Nachricht ist, dass Sie sich mit Bordmitteln vor den meisten Angriffen schützen können.

Von Ronald Eikenberg

Updates installieren

Microsoft liefert regelmäßig Updates, die Sicherheitslücken in Windows schließen. Stellen Sie sicher, dass alle verfügbaren Updates installiert sind und die Update-Installation nicht pausiert wurde. Rufen Sie hierzu „Nach Updates suchen“ über das Suchfeld auf. Klicken Sie anschließend auf den Knopf „Nach Updates suchen“. Falls es neue Aktualisierungen gibt, starten Sie die Installation abschließend mit „Jetzt installieren“.

Erscheint oben im Fenster der Hinweis „Updates wurden bis [Datum] ausgesetzt“, klicken Sie auf „Updates fortsetzen“, damit Windows nach frischen Aktualisierungen sucht. Sorgen Sie dafür, dass Windows auch andere Microsoft-Programme wie Office auf dem aktuellen Stand hält, indem Sie unter „Erweiterte Optionen“ den Schiebeschalter „Updates für andere Microsoft-Produkte erhalten“ aktivieren.

Alte Windows-Versionen versorgt Microsoft nicht mehr mit Sicherheits-Patches, wodurch das Angriffsrisiko steigt. Nutzen Sie daher Windows 10 oder 11 mit dem derzeit aktuellen Funktions-Upgrade. Halten Sie auch Anwendungen wie Browser, Mail-Client, PDF-Viewer und Videoplayer aktuell.

Daten-GAU vorbeugen

Ihre Daten sind auf der Systemplatte oder -SSD allein auf Dauer nicht gut aufgehoben, da diese jederzeit ausfallen kann. Zudem besteht die Gefahr, dass die Daten von einem Krypto-Trojaner verschlüsselt werden. Sorgen Sie vor und legen Sie Backups aller wichtigen Daten an. Im einfachsten Fall reicht es, die Daten auf einen USB-Datenträger zu kopieren (siehe S. 13).

Virenschutz überprüfen

Ein Virenschutzprogramm kann Sie zwar nicht vor allen Gefahren schützen, doch vor vielen. Bei aktuellen Windows-Versionen ist der Windows Defender vorinstalliert, der einen ausreichenden Schutz bietet. Etwaige Testversionen anderer Virenschutzprodukte sollten Sie entfernen. Stellen Sie sicher, dass der Defender aktiv und mit aktuellen Signaturen versorgt ist. Um die Signaturen zu checken, rufen Sie den „Viren- und Bedrohungsschutz“ über das Suchfeld auf. Anschließend klicken Sie unter „Updates für Viren- und Bedrohungsschutz“ auf „Schutzupdates“ und im nächsten Dialog auf „Nach Updates suchen“.

Noch mehr Schutz bietet die Windows-11-Funktion „Smart App Control“ [1]. Ist sie aktiv, führt Windows nur noch Programme aus, die Microsoft für unbedenklich hält. Auch diese Funktion erreichen Sie über das Suchfeld.

Zugriffsschutz aktivieren

Ihr Rechner muss nicht nur vor Angriffen aus dem Internet geschützt werden, sondern auch vor physischen Zugriffen, also vor Personen, die sich dem Rechner nähern. Im besten Fall verschlüsseln Sie die Systemplatte oder -SSD mit BitLocker oder VeraCrypt [2]. So sind Ihre Daten – oder die Ihres Arbeitgebers – auch dann noch geschützt, wenn jemand an der Windows-Anmeldung vorbei direkt auf den Datenträger zugreift.

Schützen Sie Ihr Windows-Konto mit einem mindestens zehn Zeichen langen Passwort. Sie müssen es nur selten eingeben, wenn Sie als Anmeldemethode zusätzlich eine mindestens vierstellige, besser längere PIN setzen. Eine solche PIN ist ausreichend sicher, weil Windows nur sehr wenige Fehleingaben zulässt, ehe es die Eingabe verzögert.

Sperren Sie Ihren Rechner, wenn Sie ihn außer Augen lassen. Das klappt ganz fix mit der Tastenkombination Windows+L.

Datenschutz verbessern

Sorgen Sie dafür, dass nicht mehr Daten fließen als nötig: Suchen Sie im Startmenü nach „Einstellungen für Diagnose und Feedback“ und stellen Sie alles aus, was möglich ist. Windows drängt Ihnen bei der Einrichtung das Microsoft-Konto auf, das eng mit der Cloud vernetzt ist. Nutzen Sie besser ein lokales Konto. Das klappt etwa, wenn Sie vor der Einrichtung die Netzwerkverbindung kappen [3]. *(rei@ct.de)* c't

Literatur

[1] Ronald Eikenberg, Schloss ohne Schlüssel, Die neue Windows-Schutzfunktion Smart App Control, c't 24/2022, S. 28

[2] Jan Schüßler, Dicht und frei, Windows-Partition mit VeraCrypt verschlüsseln, c't 17/2020, S. 162

[3] Axel Vahldiek, Zurück in die Kiste!, Windows ohne Microsoft-Konto nutzen, c't 13/2021, S. 28

Mobil und sicher

Security-Checkliste Smartphone

Bild: Andreas Martini

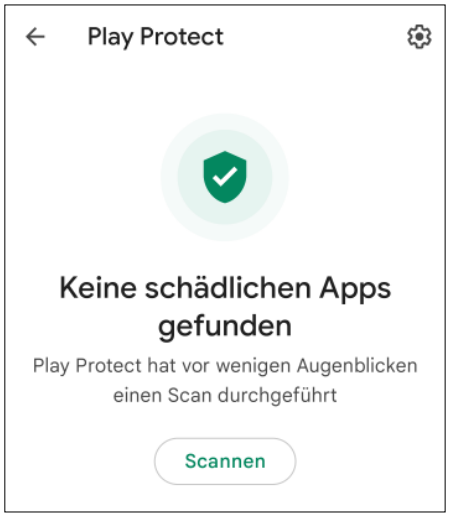
Android-Smartphones und iPhones beherbergen allerlei wichtige Daten, die nur Sie etwas angehen. Mit ein paar Handgriffen schützen Sie Ihre mobilen Begleiter vor Malware und neugierigen Mitmenschen. Die meisten Tipps gelten auch für Tablets und weitere Mobilgeräte.

Von Ronald Eikenberg

Firmware-Updates

Ganz gleich, ob Sie Android oder iOS nutzen: Achten Sie darauf, dass ein möglichst aktuelles Betriebssystem auf dem Gerät installiert ist. Betriebssystemupdates schließen meist Sicherheitslücken, und wer nicht auf dem Laufenden ist, macht es Hackern leichter als nötig. Apple versorgt seine iPhones vorbildlich mit Updates: iOS 17 erscheint sogar noch für die 2018er-iPhones XR und XS. Bei Android ist die Lage durchwachsen, insbesondere bei preiswerten Smartphones versiegt der Update-Fluss oft nach kurzer Zeit.

Ob es ein Update gibt, können Sie in den Einstellungen überprüfen. Suchen Sie dort einfach nach „Update“ oder „Softwareaktualisierung“. Dort können Sie auch die Installation anstoßen. Android-Nutzer erfahren in den Einstellungen auch das von der Android-Version unabhängige Sicherheitspatch-Level, das besagt, von welchem Datum die installierten Sicherheitspatches sind. Falls Sie ein Smartphone einsetzen, um das sich der Hersteller nicht mehr kümmert, sollten Sie mittelfristig über eine Neuanschaffung nachdenken.



Virenschutz frei Haus: Der unter Android meist vorinstallierte Play Store bringt einen einfachen Virenschutz mit.

Zugriffsschutz aktivieren

Stellen Sie sicher, dass der Sperrbildschirm eingerichtet ist und ein Passcode zum Entsperren des Smartphones festgelegt ist. Andernfalls kann jeder, dem das Gerät in die Hände fällt, auf Ihre persönlichen Daten zugreifen oder eine Trojaner-App installieren. Der Passcode sollte mindestens sechs Zeichen lang und nicht zu leicht zu erraten sein: 1234, 0815 oder Ihr Geburtsdatum sind also tabu.

Die meisten Smartphones lassen sich zusätzlich auch komfortabel per Gesichtsscan oder Fingerabdruck entsperren. Der Passcode muss dann nur noch selten eingegeben werden. Sie finden die entsprechenden Einstellungen auf dem iPhone unter „Face ID & Code“ (oder „Touch ID & Code“). Bei Android lauten die Stichwörter „Sicherheit“ und „Displaysperre“ sowie „Biometrie & Passwort“.

Externe Quellen meiden

Installieren Sie Apps am besten nur aus den offiziellen Stores von Apple, Google und den Geräteherstellern. Die Apps werden zumindest bei Apple und Google einem Sicherheitscheck unterzogen. Android-Nutzer, die eine App als APK-Installationspaket installieren möchten, sollten dieses nur direkt vom Entwickler der App beziehen. Stellen Sie unter Android sicher, dass der Cloud-Virenschutz Play Protect aktiv ist. Sie finden ihn im Menü des Play Store. iOS-Nutzer benötigen keinen Virenscanner.

App-Berechtigungen

Überprüfen Sie vor Installation und Nutzung einer App genau, welche Rechte sie einfordert und ob es einen nachvollziehbaren Grund für den Zugriff auf wichtige Ressourcen wie Kamera, Mikrofon und Standort gibt. Erteilen Sie den Zugriff nur Apps, denen Sie vertrauen, und nur, wenn Sie die betroffene Funktion der App auch nutzen wollen. iOS-Nutzer können unter „Einstellungen/Datenschutz“ bereits erteilte Rechte verwalten, Android-Nutzer schauen in den Einstellungen etwa unter „Datenschutz/Berechtigungsverwaltung“. Gehen Sie die Liste aufmerksam durch und entziehen Sie alle Berechtigungen, die Sie nicht für nötig halten.

Risiko Jailbreak

Durch „Rooting“ (Android) und „Jailbreaking“ (iOS) kann man sich höhere Rechte auf dem Smartphone verschaffen und tiefgreifende Modifikationen am System vornehmen. Dadurch hebelt man jedoch auch essenzielle Schutzfunktionen aus. Hinzu kommt, dass zahlreiche Apps den Start verweigern. *(rei@ct.de)* c't

Netzabsicherung

Security-Checkliste WLAN-Router

Bild: Andreas Martini

Mit Einrichtungsassistenten konfigurieren Sie WLAN-Router schnell, aber bei Sicherheitsfunktionen für das Heimnetz braucht es noch Feintuning, darunter auch die sicherheitskritische WLAN-Verschlüsselung, selbst wenn Ihr Router das aktuelle WPA3 beherrscht.

Von Dušan Živadinović

Webinterface abdichten

Fast alle modernen Router lassen sich mittels Assistenten konfigurieren; sie fragen die wichtigsten Einstellungen ab und tragen diese an passender Stelle ein. Sie lassen aber Lücken. Ändern Sie zunächst das ab Werk eingestellte Konfigurationspasswort. Denn wenn es am Gehäuseboden angebracht ist, können Unbefugte es ablesen oder fotografieren und dann Ihren Router missbrauchen.

Falls vorhanden, aktivieren Sie das automatische Firmware-Update, damit sich der Router auch dann Sicherheits-Updates zieht, wenn Sie Dringenderes zu tun haben oder verreist sind.

WLAN richtig verschlüsseln

Für die WLAN-Verschlüsselung empfiehlt sich der Mixed-Mode WPA2/WPA3. Andernfalls aktivieren Sie wenigstens den Schutz der Steuerpakete (PMF). Ändern Sie den Funknetznamen und das Passwort Ihres WLANs, besonders dann, wenn diese Einstellungen am Router angebracht sind. Aber auch generische WLAN-Zugangsdaten sind ein Einfallstor, weil sie in Bedienungsanleitungen stehen, die für jedermann zugänglich sind.

Beim veralteten WPA2 können spezielle Knackprogramme Passwörter mit Durchprobieren aufspüren (Brute-Force-Attacke). Dafür zeichnen Angreifer Ihren WLAN-Verkehr auf und füttern damit im geheimen Kämmerlein einen sehr leistungsfähigen PC. Ob er dann das Passwort schnell findet oder der Angreifer das Herumprobieren nach Tagen wegen Aussichtslosigkeit abbricht, hängt von der Länge Ihres WLAN-Passworts ab. Nutzen Sie 20 bis 30 Zeichen, wenn Sie wegen älterer Geräte auf WPA2 nicht verzichten können.

Gastnetz einsetzen

Schützen Sie Ihr Netz, indem Sie Besuchern, Smart-Home- und IoT-Geräten das Gast-WLAN zuweisen. Nutzen Sie auch für das Gastnetz ein langes Passwort und ändern Sie es gelegentlich, denn manche Besucher geben WLAN-Passwörter ohne Rückfrage weiter. Schränken Sie das Gast-WLAN auf bestimmte Dienste ein, beispielsweise Surfen und Mailen, um unerwünschtes Filesharing zu unterbinden.

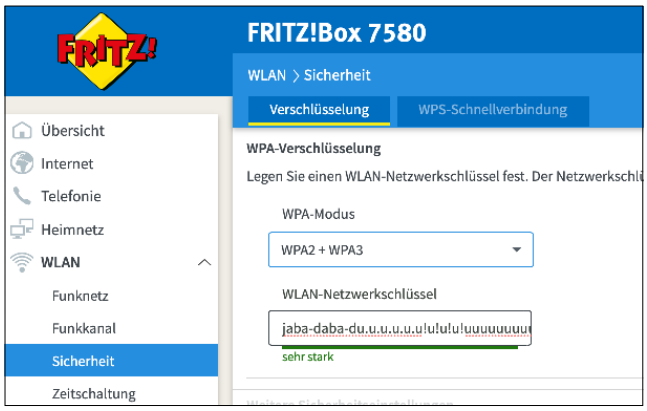
Wenn das Webinterface des Routers aus dem Internet erreichbar ist, sollte dieser Verkehr per HTTPS verschlüsselt werden. Falls Sie einen Server betreiben, auf den Sie von außen zugreifen wollen, richten Sie eine VPN-Verbindung ins Heimnetz ein; Port-Weiterleitungen funktionieren zwar ebenfalls, erfordern aber eine gute serverseitige Absicherung. Als VPN-Server eignen sich viele Router. Weitere Hinweise zum sicheren Betrieb von Servern finden Sie auf Seite 14.

WPS nur bedarfsweise

Per WPS-Funktion lassen sich WLAN-Geräte über je einen Tastendruck am Router und am Client ins WLAN bringen. Das erleichtert es aber auch Unbefugten, Zugang zu Ihrem WLAN zu erlangen. Schalten Sie diese Funktion daher nur vorübergehend bei Bedarf ein.

Manche Hersteller nutzen die UPnP-Funktion von Routern, damit sich ihre Geräte selbsttätig eine Port-Weiterleitung im Router einrichten. Das spart zwar Zeit, aber wenn UPnP anhaltend aktiv ist, kann auch eingeschleppte Malware es nutzen, um die Firewall Ihres Routers von innen zu öffnen. Deaktivieren Sie diese Funktion nach Möglichkeit oder beschränken Sie sie auf einzelne Hosts, falls Ihr Router das ermöglicht.

Wenn alle Punkte abgehakt sind, exportieren Sie die Router-Konfiguration auf Ihren PC, damit Sie bei einem Router-Ausfall ein Ersatzgerät einfach durch Konfigurationsimport in Betrieb nehmen können. *(dz@ct.de)* c't



Falls für die WLAN-Verschlüsselung nur das veraltete WPA2 verfügbar ist, gilt für die Sicherheit des WLAN-Passworts: Länge ist wichtiger als irgendwelche Sonderzeichenregeln.

Brief ohne Siegel

Security-Checkliste E-Mail

Auch wenn sich immer mehr Kommunikation auf andere Kanäle verlagert: Ganz ohne E-Mails kommt kaum jemand aus, weshalb Kriminelle sehr gerne dieses alte Medium nutzen. Umso wichtiger ist es, die Gefahren zu kennen.

Bild: Andreas Martini

Von Sylvester Tremmel

Holzauge, sei wachsam

Plumpe, leicht erkennbare Spam-Mails gibt es nach wie vor. Aber auch die Mail vom langjährigen Kunden, die mit passender Anrede fehlerfrei formuliert ist und Bezug auf Nachrichten von letzter Woche nimmt, kann gefälscht sein. Angreifer konnten solche gut gemachten Fälschungen auch schon vor der Verbreitung von Sprach-KI-Systemen (siehe Seite 8) weitgehend automatisch erstellen und verschicken. Man muss also keineswegs einer gezielten Attacke ausgesetzt sein und die Annahme „uns kleine Fische wird es schon nicht treffen“, ist eine ganz schlechte Idee.

Misstrauen Sie daher *jeder* E-Mail. Nicht nur, aber besonders dann, wenn Anhänge oder Geld im Spiel sind und die Mail scheinbar vom Chef oder der Bank kommt und ganz dringend und wichtig ist. Statt auf Links in einer Mail zu klicken, rufen Sie Websites besser über Ihre eigenen Bookmarks auf. Schlagen Sie Telefonnummern nach, statt den Angaben in einer Mail blind zu vertrauen. Ignorieren Sie niemals Sicherheitswarnungen beim Öffnen von Anhängen, ganz egal was die Mail behauptet, und fragen Sie über einen anderen Kanal beim Absender nach, wenn ein Anhang unerwartet oder untypisch ist.

Mailclient absichern

Ihren Mailclient können Sie so einstellen, dass er zumindest ein paar Risiken eliminiert: Das Nachladen externer Inhalte sollten Sie verbieten, was viele Mailprogramme zum Glück standardmäßig tun. Newsletter und so manch andere Mail sieht dadurch weniger schön aus, aber externe Inhalte werden gerne für (Werbe-)Tracking genutzt und sind auch immer wieder an Sicherheitslücken beteiligt.

Ähnliches gilt für HTML-Mails. Schalten Sie die HTML-Ansicht am besten ganz aus und lassen Sie Ihren Client nur die Textansicht anzeigen. Eine Option dafür bietet fast jeder Client, wenn auch mitunter gut versteckt. Im verbreiteten Client Thunderbird klicken Sie im Menü auf „Ansicht/Nachrichteninhalt/Reiner Text“. Nur wenn diese Ansicht absolut unleserlich (oder leer) ist, sollten Sie auf die HTML-Darstellung ausweichen und eine Extraportion Skepsis walten lassen. Viele Mailclients erlauben, HTML-Inhalte temporär und direkt aus der Mailansicht zu aktivieren, sodass der Komfortverlust gering ist. In Thunderbird rüstet das Add-on „Allow HTML Temp“ diese Option nach.

Verschlüsselung

Die Verschlüsselung von E-Mails ist ein Trauerspiel, das sich nur sehr langsam bessert. Sofern Sie keinen Mailclient im Browser nutzen, sollten Sie zunächst in den Programmeinstellungen sicherstellen, dass zum Versand und Empfang TLS oder STARTTLS genutzt werden. So wandern Ihre Mails und Passwörter zumindest nicht im Klartext durch das Hotel-WLAN.

Manche Mail-Provider erlauben, Mails nur dann zu versenden, wenn so eine Transportverschlüsselung bis zum Zielserver aufgebaut werden kann. Dann können immerhin nur noch die beteiligten Mailserver mitlesen. Sofern Ihr Anbieter diese empfehlenswerte Option anbietet, finden Sie sie in den Account-Einstellungen des Providers.

Alle Lauscher aussperren können Sie nur mit Ende-zu-Ende-Verschlüsselung. Die ist leider in der Handhabung eher kompliziert und die einschlägigen Standards S/MIME und OpenPGP kämpfen mit diversen Problemen und einer geringen Verbreitung. Wenn Sie sich mit Ihren Korrespondenten auf ein Verfahren einigen können, sollten Sie es aber nutzen: Besser als nichts sind beide Verfahren allemal. Zum Einstieg bietet sich der erwähnte Mailclient Thunderbird an. Er hat seit Version 78 eine relativ einsteigerfreundliche OpenPGP-Unterstützung integriert.

Als Notlösung bieten manche Provider an, Mails automatisch per OpenPGP oder S/MIME zu verschlüsseln, wenn sie bei ihnen eingehen. Die Nachrichten sind dann immerhin vor fremden Augen sicher, sobald sie Ihren Account erreicht haben. Um selbigen abzusichern, sollten Sie Zwei-Faktor-Authentifizierung (2FA, siehe Seite 15) nutzen, was die meisten Mailprovider mittlerweile anbieten.

Bedachtes Mailen

Hinterfragen Sie auch beim Versand, wie und wofür Sie E-Mails nutzen. Reine Textmails zu verschicken verhindert zwar schicke Formatierungen, erspart aber den Empfängern die Risiken von HTML-Mails. Mehr noch gilt das für ausführbare Dateien oder Office-Dokumente mit Makros. Solche verdächtigen Inhalte wollen Sie nicht per Mail empfangen, also versenden Sie auch nichts Derartiges. *(syt@ct.de)* c't

Thunderbird-Add-on und -OpenPGP-Doku: ***ct.de/yguz***

Heißes Eisen

Security-Checkliste KI-Sprachmodelle

Bild: Andreas Martini

Große Sprachmodelle sind allerorten, fassen Texte zusammen, geben Stichpunkte, beantworten Fragen und vieles mehr. Aber Sie sollten den Systemen weder zu sehr trauen noch ihnen zu viel anvertrauen.

Von Sylvester Tremmel

Große Sprachmodelle (Large Language Models, LLMs), wie sie zum Beispiel in ChatGPT zum Einsatz kommen, sind der Auslöser für den aktuellen KI-Hype. Oftmals wird an einer Anwendung aber nicht LLM dranstehen, wenn ein Sprachmodell drinsteckt, sondern allgemein „KI“. Wann immer eine Anwendung Texte schreibt, umschreibt oder mit Ihnen chattet, können Sie davon ausgehen, dass Sie es mit einem LLM zu tun haben.

Datenschutz beachten

Das Feld der LLMs befindet sich in rasanter Entwicklung. Um mit der Konkurrenz mitzuhalten, gestatten sich viele Hersteller in den Nutzungsbedingungen, die von Ihnen eingegebenen Texte für das weitere Training ihrer Systeme zu verwenden. Prüfen Sie die Nutzungsbedingungen also genau und vertrauen Sie einem LLM im Zweifelsfall lieber keine privaten Informationen oder Geschäftsgeheimnisse an.

Das gilt auch dann, wenn Sie dem Hersteller vertrauen, denn Sie teilen die Daten nicht nur mit ihm: Einmal ins Training eingeflossen, kann es durchaus passieren, dass *andere Nutzer* dem LLM Ihre Daten wieder entlocken. Das ist ein grundsätzliches Problem von LLMs: Mitunter generieren sie keinen neuen Text auf Basis ihrer immensen Trainingsdatensammlung, sondern geben Schnipsel aus diesem Heuhaufen wortwörtlich wieder. Die Hersteller wissen um das Problem, haben es aber selbst nicht im Griff. Beispielsweise weist Google die eigenen Mitarbeiter an, keinen Code oder vertrauliche Informationen mit dem eigenen KI-Chatbot Bard zu teilen.

Ausgaben hinterfragen

Vorsicht müssen Sie auch bei Informationen walten lassen, die aus dem System wieder herauskommen: Im Grunde versuchen LLMs, Texte sprachlich möglichst plausibel zu vervollständigen, nicht faktisch möglichst korrekt. Die Hersteller arbeiten zwar fleißig an der Faktentreue ihrer Schöpfungen, haben aber noch einen weiten Weg zu gehen: Sogenannte Halluzinationen, also falsche, haltlose Behauptungen, produzieren auch die fortgeschrittensten LLMs immer und immer wieder. Ob sie sich je komplett ausschließen lassen, ist ungewiss.

Wenn Sie sich solche Fehler nicht als eigene anrechnen lassen wollen, müssen Sie die Informationen gründlich überprüfen, durch eigene Recherche. Denn mitunter bringt man zwar LLMs durch kritische Rück- und Nachfragen dazu, das Behauptete zu korrigieren, doch das passiert beileibe nicht immer. Häufig stützen die Systeme auf Nachfrage stattdessen ihre Lüge mit sinnlosen Referenzen auf ebenso halluzinierte Quellen. Hauptsache, der Text bleibt plausibel.

Systemen misstrauen

Neben solchen Unzulänglichkeiten sehen sich LLMs auch gezielten Angriffen ausgesetzt. Man forscht beispielsweise daran, ob sich LLMs „vergiften“ lassen, indem man – vom Hersteller unbemerkt – manipulierte Trainingsdaten einschleust, die ein LLM in bestimmten Situationen zu unerwünschtem Verhalten verleiten.

Nicht nur erforscht, sondern schon in der Praxis demonstriert werden indirekte Prompt Injections [1]. Dabei nutzen Angreifer aus, dass LLMs häufig externe Daten einlesen sollen, beispielsweise, um ein Paper zusammenzufassen oder eine Website zu übersetzen. Geschickte Phrasen in diesen Daten können einem Angreifer Kontrolle über das LLM verschaffen, sodass es fortan seine Anweisungen ausführt. Gerade in Kombination mit anderen Systemen erwachsen daraus enorme Risiken: Der hilfsbereite Firmen-Chatbot mutiert so zum Verräter, der die letzten E-Mails vom Chef abruft und über das Internet an den Angreifer ausleitet. Geschickte Angreifer schreiben die Prompt Injection weiß-auf-weiß oder anderweitig versteckt in die Daten und weisen den Bot an, neben dem Angriff auch seine ursprüngliche Aufgabe zu erledigen – dann bekommen Sie die Attacke eventuell nicht einmal mit.

Sofern Sie LLMs nicht komplett meiden, können Sie sich nur bedingt vor solchen unterwanderten KIs schützen, denn ein zuverlässiges Gegenmittel ist noch nicht gefunden. Es hilft, LLMs grundsätzlich als kompromittiert zu betrachten, ähnlich einer E-Mail mit Anhang: Erlauben Sie keine vollautomatischen Zugriffe auf andere Systeme, nicken Sie keine Aktionen blind ab und klicken Sie nicht reflexhaft auf jeden Link, den Ihnen das System präsentiert. Inhaltlich prüfen sollten Sie jede Ausgabe ohnehin, schon aufgrund der erwähnten Halluzinationen. *(syt@ct.de)* c't

Literatur

[1] Sylvester Tremmel, Fremdgesteuert, Wie Prompt Injections KI-Suchmaschinen korrumpieren können, c't 10/2023, S. 26

WhatsSecure?

Security-Checkliste Messenger

Bild: Andreas Martini

WhatsApp, Signal, Telegram, Matrix, Facebook-Messenger, XMPP und so weiter: Die Liste populärer Messengerdienste ist lang. „Sicher" sollen sie alle sein, doch es gibt wichtige Unterschiede im Detail. Vor allem aber bedarf Sicherheit der Kontrolle – durch Sie.

Von Sylvester Tremmel

Auf die Verschlüsselung achten

Grundsätzlich sollten Sie Daten nur Ende-zu-Ende-verschlüsselt austauschen (end-to-end encryption, E2EE), sodass niemand mitlesen kann, nicht einmal der Server, der die Nachrichten vermittelt. Auch wenn es seitens der EU Bestrebungen gibt, hier Löcher zu bohren: Noch ist eine lückenlose Ende-zu-Ende-Verschlüsselung legal und bei Messengern erfreulich weit verbreitet. Die meisten Apps nutzen sie standardmäßig oder bieten sie zumindest als Option an. Viele Messenger bauen auf das von Signal eingeführte Double-Ratchet-Verfahren, das einige Vorzüge hat [1]. Aber auch Apps mit anderen Verfahren bieten in aller Regel ausreichend Schutz.

Viel wichtiger als die technische Umsetzung ist, dass E2EE auch tatsächlich zum Einsatz kommt. Einige Apps, beispielsweise Telegram, nutzen E2EE nämlich nur, wenn Sie als Nutzer eine spezielle Art von Chat eröffnen, oft „geheime Unterhaltung" oder ähnlich genannt. Auch beim Facebook-Messenger ist das so, wenngleich Meta seit einer Weile mehr und mehr Unterhaltungen standardmäßig per E2EE schützt. Achten Sie also gut darauf, ob und wann Ihr Messenger verschlüsselt!

Eine Ausnahme von der Regel stellen übrigens sehr große Gruppen oder „Kanäle" dar, wie es sie seit Langem bei Telegram und neuerdings auch bei WhatsApp gibt. Diese sind in aller Regel nicht Ende-zu-Ende-verschlüsselt, weil das technisch schwierig und von zweifelhaftem Nutzen ist: Bei Tausenden oder sogar Hunderttausenden Chatteilnehmern sind Geheimnisse ohnehin kaum zu wahren.

Wer hört mit?

Viele Messenger bieten Web- oder Desktop-Clients zusätzlich zur App. Gerade am Arbeitsplatz ist das praktisch, dann muss man nicht ständig zum Handy greifen, wenn ein Kollege etwas schreibt. Bei den meisten Messengern lassen sich – einmal eingerichtet – dann sämtliche Konversationen bis auf Weiteres am Computer mitlesen. Die Messenger-Apps auf dem Smartphone zeigen daher (meist in den Einstellungen), welche Geräte verknüpft sind. Prüfen Sie diese Liste regelmäßig und löschen Sie, was Sie nicht mehr brauchen.

Backups richtig einstellen

Backups können essenziell sein, aber sie sind auch eine mögliche Schwachstelle. Überlegen Sie sich, von welchen Messengern und Chats Sie Backups brauchen und wofür. Manche Apps wie zum Beispiel Signal und WhatsApp legen automatisch oder auf Wunsch verschlüsselte Backups auf dem Smartphone an. Das ist gut, hilft aber nicht, falls das Smartphone selbst kaputtgeht; Sie müssen solche Backups regelmäßig auf ein anderes Gerät laden. Bei Backups in die Cloud, die manche Messenger anbieten, sollten Sie skeptisch sein: Prüfen Sie, ob die Daten dort so verschlüsselt sind, dass nur Sie Zugriff haben.

Viele Messenger erlauben es, Nachrichten nach einer einstellbaren Zeit automatisch zu löschen. „Selbstzerstörende", „selbstlöschende" oder „verschwindende" Nachrichten nennen die Apps das. Vorsicht: Das Feature kann nicht verhindern, dass der Gesprächspartner die Nachricht dauerhaft speichert. Aber es eignet sich gut, um Chatverläufe kurz und Messenger-Backups klein zu halten.

Vor Account-Übernahmen schützen

Viele Messenger binden Accounts an eine Handynummer. Das ist nicht unproblematisch, auch wenn es dafür gute Gründe gibt, die wir in [2] erklärt haben. Anders handhabt das beispielsweise der Messenger Threema, der auch ohne Telefonnummer auskommt. Bei Apps, die eine Nummer verlangen, wird sie per SMS bestätigt, was sich manipulieren lässt. Schlimmstenfalls können Dritte dadurch Accounts übernehmen. Die meisten solcher Messenger erlauben daher, den Registrierungsprozess mit einer zusätzlichen PIN abzusichern. Das Feature sollten Sie nutzen, bewahren Sie aber die PIN gut auf. Sonst werden Sie selber Probleme bekommen, wenn Sie eines Tages Ihr Handy austauschen wollen.

Achten Sie außerdem darauf, Ihre Accounts bei einem Nummernwechsel umzuziehen und nicht unter der alten Nummer weiterzubetreiben. Die kann nämlich wieder vergeben werden. Falls der neue Besitzer denselben Messenger nutzen will und die Nummer registriert, werden Sie dadurch aus Ihrem Account ausgesperrt.

(syt@ct.de) **ct**

Literatur

[1] Sylvester Tremmel, Für immer unlesbar, Wie moderne Kommunikationsverschlüsselung funktioniert, c't 3/2021, S. 60

[2] Sylvester Tremmel, Zeigt her Eure Kontakte, Warum Messenger nach Ihrer Telefonnummer fragen, c't 6/2021, S. 118

Sicher surfen

Security-Checkliste Browser

Browser sind ein beliebtes Ziel für Angreifer, weil jeder sie nutzt. Deshalb sollten Sie Ihren Browser maximal sicher einstellen.

Bild: Andreas Martini

Von Jo Bager

Aktuell halten

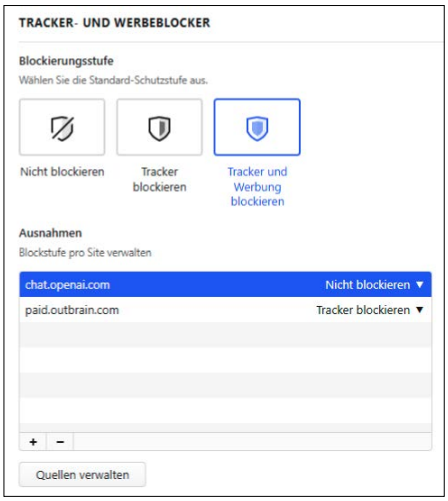
Um sicher zu surfen, sollte der Browser Ihrer Wahl immer auf dem neuesten Stand sein. Die Hersteller geben laufend Updates heraus, mit denen sie bekannte Sicherheitslücken schließen. Alle gängigen Browser lassen sich so einstellen, dass sie sich automatisch aktualisieren. Es kann aber vorkommen, dass die Update-Versorgung klemmt oder dass Sie den Browser zur Installation neu starten müssen. Überprüfen Sie gelegentlich über das Menü, ob ein Neustart notwendig ist. Die betreffende Option findet sich häufig im Hilfe-Menü, unter „Über <Browsername>“ oder „Nach Updates suchen“.

Add-ons aufräumen

Onlinebanking, vertrauliche Mails: Browser-Erweiterungen, auch Add-ons oder Extensions genannt, haben Zugriff auf alles, was innerhalb des Browsers geschieht. Prüfen Sie vor der Installation also genau, worauf Sie sich einlassen. Installieren Sie nur Erweiterungen aus den offiziellen Verzeichnissen der Hersteller und achten Sie auf Downloadzahlen und Nutzerbewertungen. Verzichten Sie im Zweifel lieber zugunsten der Sicherheit. Prüfen Sie auch gelegentlich die installierten Erweiterungen und misten Sie gründlich aus. Bei Chrome und Edge finden Sie die Erweiterungen im Hauptmenü, bei Firefox klicken Sie auf „Add-ons und Themes“. Deaktivieren Sie Add-ons, die Sie nur selten nutzen, und schalten Sie sie bei Bedarf vorübergehend ein.

Schnüffler aussperren

Blockieren Sie Tracker, die Ihr Surfverhalten überwachen und Ihre Interessen ausspionieren. Einige Browser wie Firefox, Edge, Vivaldi und Brave können das bereits von Haus aus, Sie müssen den Tracking-Blocker nur noch in den Einstellungen scharf schalten. Probieren Sie zunächst die strengste Einstellung. Falls es anschließend Probleme bei Ihren Lieblingswebsites gibt, können Sie den milderen Standardmodus wählen. Nutzer anderer Browser wie Chrome können sich mit Add-ons wie Privacy Badger oder uBlock Origin behelfen (siehe ct.de/yc3u). Letzteres beseitigt zudem aufdringliche und mitunter verseuchte Werbung.



Datenschutz inklusive: Viele Browser wie hier Vivaldi enthalten einen Tracking-Blocker, den Sie aktivieren und so streng wie möglich schalten sollten.

Berechtigungen prüfen

Websites können Berechtigungen einfordern, um etwa auf Kamera, Mikrofon und Standort zuzugreifen: Ein Videochat-Dienst benötigt den Zugriff auf Kamera und Mikrofon, Google Maps kann Ihren aktuellen Standort nur mit Ihrer Zustimmung ermitteln. Stimmen Sie nur zu, wenn es einen triftigen Grund gibt und Sie dem Dienst vertrauen. Kontrollieren Sie die bereits erteilten Berechtigungen und sieben Sie gründlich aus. In den Chrome-Einstellungen finden Sie die Berechtigungen unter „Datenschutz und Sicherheit/Website-Einstellungen“, in den Firefox-Einstellungen unter „Datenschutz & Sicherheit/Berechtigungen“. Edge-Nutzer schauen in den Einstellungen unter „Cookies und Websiteberechtigungen“.

Auf Adressen achten

Geben Sie persönliche Daten, Passwörter und Finanzdaten nur auf Websites ein, die Daten verschlüsselt übertragen. Die Webadresse beginnt mit dann mit https:// und der Browser zeigt ein geschlossenes Vorhängeschloss neben der Adresse an. Darüber hinaus sollten Sie die Adressen genau auf Ungereimtheiten untersuchen: Ein falscher Buchstabe oder ein seltsames Zeichen reichen aus, um Sie nicht zu Ihrer Bank, sondern auf eine perfekt kopierte Phishing-Seite zu lenken. Steuern Sie kritische Websites nicht über Links an, die Sie per Mail erhalten haben, sondern nutzen Sie Lesezeichen oder tippen Sie die Adresse von Hand ein. *(jo@ct.de)* c't

Tracking-Blocker für Chrome und andere: ***ct.de/yc3u***

Soziale Sicherheit

Security-Checkliste Social Media

Bild: Andreas Martini

Social-Media-Konten stellen de facto die digitale Identität vieler Nutzer dar. Die Plattformen bieten deshalb Schutzfunktionen, die Sie anwenden sollten. Und: Schalten Sie gerade bei auffällig attraktiven sozialen Kontakten nicht den gesunden Menschenverstand aus.

Von Holger Bleich

Zwei Faktoren nutzen

Werden Ihre Konten bei Facebook, Instagram oder LinkedIn gekapert, kann das nicht nur für Sie, sondern auch für Freunde und Kollegen katastrophale Folgen haben. Der Schutz solcher Accounts ist deshalb besonders wichtig. Nutzen Sie dazu alle Möglichkeiten, die die Plattformen bieten. Was in einigen anderen Checklisten bereits erwähnt ist (siehe auch Seite 15), gilt in besonderem Maße für soziale Plattformen: Sie sollten, wo immer möglich, weitere Zugangsbarrieren neben dem Passwort aufbauen, also auf eine Zwei-Faktor-Authentifizierung (2FA) setzen.

Auf der Facebook-Website gelangen Sie über einen Klick auf Ihr Profilbild oben rechts in die „Einstellungen“, wo der Menüpunkt „Privacy Center“ über „Sicherheit“ zur „zweistufigen Authentifizierung“ führt. Dort veranlassen Sie, dass bei jedem Zugriffsversuch von einem unbekannten Gerät oder Browser der zweite Faktor abgefragt wird, also etwa eine via SMS verschickte PIN oder der Anmeldecode einer zuvor mit dem Konto verbundenen Authentifizierungs-App. Ähnliche Einstellungen bieten inzwischen alle großen sozialen Netzwerke, also etwa Instagram, Twitter, Google (YouTube) und LinkedIn. Auch auf der Kurzvideo-Plattform TikTok lässt sich 2FA einrichten, allerdings nur in der mobilen App, dort in den Einstellungen unter „Sicherheit“.

Damit die Abfrage nicht jedes Mal nervt, merken sich die Plattformen Geräte-IDs oder setzen Cookies und bleiben auf dem Gerät angemeldet. Dies kann zum Sicherheitsproblem werden, wenn sich mehrere Menschen einen Rechner oder ein Tablet teilen und ist definitiv gefährlich, wenn der Kontenzugriff von öffentlichen Terminals erfolgt. Sie sollten von Zeit zu Zeit prüfen, welche Geräte derzeit autorisierten Zugriff aufs Konto haben und deshalb von der 2FA ausgenommen sind. Bei Meta finden Sie diese Liste für Facebook und Instagram über die „Kontenübersicht“ im Privacy Center unter „Hier bist Du aktuell angemeldet“. Dort lässt sich der Zugriff selektiv unterbinden.

Zugriffe prüfen

Bei vielen sozialen Netzen können Sie externen Diensten und Fremd-Apps Zugriff auf Ihren Account gewähren, beispielsweise für Single-Sign-on-Logins auf verbundenen Websites. Bisweilen räumen sich Apps viel mehr Rechte als nötig ein. Sie sollten die Aktivitäten und Berechtigungen der Apps im Auge behalten. Facebook etwa gewährt Ihnen Kontrollmöglichkeiten in den Einstellungen unter „Apps und Websites“. Besonders beliebt sind Apps bei Instagram-Nutzern. Unter „Apps und Websites“ in den Profileinstellungen listet der Dienst die aktiven Apps auf. Kontrollieren Sie diese Liste ab und an und entfernen Sie nicht mehr benötigte Apps.

Gezielt teilen

Bei Facebook, aber auch bei anderen Anbietern wie LinkedIn kann man festlegen, mit wem man Inhalte teilen möchte. Behalten Sie Ihre Zielgruppen-Voreinstellung im Blick, um nicht versehentlich einen größeren Adressatenkreis anzusprechen als gewünscht.

So sollten Sie beispielsweise nicht öffentlich posten, dass Sie zwei Wochen im Urlaub sind, denn das legt nahe, dass Ihr Haus leersteht. Die Voreinstellung sollte eher defensiv sein. Sie lässt sich etwa bei Facebook in den Privatsphäre-Einstellungen unter „Deine Aktivität“ ändern.

Anfragen checken

Freundschaft und Vertrauen sind auch auf Facebook, Instagram, LinkedIn oder TikTok ein begehrter Status. Befreundete Kontakte sehen je nach Profileinstellungen viel mehr Privates. Oft stecken daher hinter Freundschaftsanfragen Versuche, persönliche Daten abzugreifen, die Person zu stalken oder gar Geld zu ergaunern. Prüfen Sie jede Anfrage sorgfältig. Ist das Mitglied frisch dabei und hat viele neue Kontakte, kann das auf einen Betrug hindeuten – selbst wenn das Profil vermeintlich von einer Person stammt, die Sie persönlich kennen. Fake-Accounts haben oft Profilfotos von attraktiven Menschen.

Private Nachrichten

Lassen Sie Vorsicht walten, wenn jemand Sie anschreibt, es sehr dringend wirkt, und wenn er um Geld oder andere Gefallen bittet: Vielleicht wurde der Facebook-Account gehackt und übernommen, und nun versuchen Fremde, Ihr Vertrauen zu missbrauchen. Überweisen Sie keinesfalls Geld und rücken Sie nicht unbedacht Ihre Handynummer heraus, bevor Sie sich von der Identität überzeugen konnten – zum Beispiel mit einer Frage, die *garantiert* nur die befreundete Person beantworten kann. *(hob@ct.de)* c't

Geldwerter Schutz

Security-Checkliste Onlinebanking

Auf Ihrem Bankkonto liegt Ihr Geld – logisch, dass Betrüger und Cyberkriminelle scharf darauf sind. Absolute Sicherheit gibt es beim Onlinebanking nicht, aber Sie können es Kriminellen ziemlich schwer machen.

Bild: Andreas Martini

Von Markus Montz

Transaktionen checken

Viele Aktionen erfordern eine Zwei-Faktor-Authentifizierung (2FA), zum Beispiel durch eine PIN beim Login, gefolgt von einer TAN oder Push-Bestätigung bei einer Transaktion. Ähnliches gilt, wenn Sie ein neues Gerät für die 2FA freischalten. Checken Sie daher stets den Zweck dieser Bestätigung und brechen Sie ab, wenn er nicht stimmt. Bei Online-Überweisungen prüfen Sie außerdem, ob Empfänger-IBAN und Betrag korrekt sind – sie müssen auf sämtlichen beteiligten Geräten (PC, Smartphone, TAN-Generator) übereinstimmen.

Banking virenfrei

Für Banking auf dem PC oder Smartphone muss das System frei von Schadsoftware sein. Sorgen Sie auf einem Windows-PC dafür, dass ein Virenscanner mit aktuellen Updates mitläuft. Der bei Windows 10 und 11 mitgelieferte Defender bietet hinreichenden Schutz (siehe auch S. 13). Laden Sie Anwendungen nur von seriösen Websites herunter. Installieren Sie auf dem Smartphone allgemein nur Apps aus vertrauenswürdigen Quellen. Im Zweifel ist das Google Play für Android und der App Store für iOS.

Phishing erkennen

Bei vielen Betrugsversuchen verschicken Betrüger manipulativ gestaltete Mails oder Textnachrichten. Ein Beispiel sind Mails, die angeblich von einer Bank stammen. Diese enthalten in der Regel schädliche Anhänge oder Links auf Fake-Websites. Darüber schleusen die Täter Schadcode ein oder greifen Zugangsdaten ab (Phishing).

Prüfen Sie alle Mailanhänge sorgfältig, selbst wenn sie von bekannten Absendern stammen. Eine Bank schickt Ihnen wichtige Dokumente postalisch oder stellt sie in Ihr Onlinebanking-Postfach. Mails oder Textnachrichten mit Links, um Ihr Konto mit PIN und TAN zu „bestätigen", sind fast immer Betrugsversuche. Prüfen Sie bei allen Links zuerst die Ziel-URL. Schöpfen Sie Verdacht, wenn eine persönliche Anrede fehlt, Rechtschreibfehler enthalten sind oder Sie zur Eile getrieben werden. Geben Sie Ihre Zugangsdaten im Browser nur auf der Webseite der Bank ein, nachdem Sie die Adresse selbst eingetippt oder per Lesezeichen angesteuert haben. Sicher sind auch die App der Bank oder eine seriöse Onlinebanking-Anwendung.

Mitunter rufen Betrüger auch mit gefälschten Absender-Rufnummern an und geben sich als Bankberater oder Polizist aus. Eine Masche besteht darin, Sie vor einer angeblich drohenden Gefahr zu warnen, um Sie zu unüberlegten Handlungen zu provozieren (Social Engineering) [1]. Beenden Sie das Gespräch und rufen Sie die Bank über die Telefonnummer in Ihren Unterlagen (!) zurück.

Belege überprüfen

Insbesondere Kreditkartennutzer sollten jede Abrechnung kontrollieren und unbefugte Abbuchungen umgehend bei ihrer Bank reklamieren. Prüfen Sie auch Ihre Kontoauszüge regelmäßig. Noch besser ist es, alle paar Tage im Onlinebanking am PC oder in der Smartphone-App die Umsätze auf Ihrem Kreditkarten- und Girokonto zu verfolgen. Je nach Bank können sich Nutzer außerdem per Mail, SMS oder Push-Nachricht über neue Transaktionen oder Ereignisse wie das Unterschreiten eines bestimmten Kontostands benachrichtigen lassen.

Handy nicht rooten

Rooten oder jailbreaken Sie Ihr Smartphone oder Tablet nicht, mit dem Sie Onlinebanking betreiben. Andernfalls legen Sie wichtige Schutzfunktionen lahm. Das ist besonders dann gefährlich, wenn Sie beim Smartphone-Banking den zweiten Faktor über eine Sicherheits-App auf dem gleichen Gerät beziehen. Viele Sicherheits-Apps von Banken, teilweise aber auch deren Banking-Apps, starten unter modifizierten Betriebssystemen deshalb gar nicht erst.

Generell ist es empfehlenswert, ein ungerootetes Smartphone mit einem Betriebssystem zu verwenden, das noch Sicherheitsupdates bekommt. Dennoch sind ältere Betriebssysteme nicht per se unsicher. Aus Haftungsgründen empfiehlt es sich, den Vorgaben Ihrer Bank zu folgen: Solange Sie ein Betriebssystem nutzen, das die App Ihrer Bank offiziell noch unterstützt, kann Ihr Kreditinstitut zumindest daraus keine grobe Verletzung der Sorgfaltspflichten ableiten. Ohne solch eine grobe Verletzung haften Sie für Schäden mit maximal 50 Euro [2].

(mon@ct.de) c't

Literatur

[1] Mirko Dölle, Bei Anruf: Geld weg! Wie Telefonbetrüger die Zwei-Faktor-Autorisierung aushebeln, c't 14/2023, S. 66

[2] Stefan Hessel, Datenfänger und Haftungsflüchtlinge, Smartphone-Banking aus rechtlicher Sicht, c't 11/2020, S. 66

Kein Backup, kein Mitleid

Security-Checkliste Backups

Die Frage ist nicht, ob Sie Daten verlieren, sondern nur, wann. Backups sind daher unverzichtbar. Hier ein paar Tipps, worauf Sie dabei achten sollten.

Bild: Andreas Martini

Von Axel Vahldiek

Jetzt!

Damit Sie im Ernstfall keine Daten verlieren, brauchen Sie ein Backup. Auf welche Art Sie das erstellen, ist an sich erst mal egal, denn jedes Backup ist besser als kein Backup. Wichtig ist, dass Sie es auch wirklich machen. Der richtige Termin dafür ist immer der gleiche: jetzt! Sichern Sie zuerst die wichtigsten Daten. Starten Sie mit Unikaten wie Steuerunterlagen, Diplomarbeit und anderen Arbeitsergebnissen. Denken Sie an Originale von Fotos, Videos und Korrespondenz. Orientieren Sie sich für die anderen Daten daran, wie aufwendig die Wiederbeschaffung oder erneute Bearbeitung sein wird.

Schutz vor „Hoppla!“

Schutz vor Datenverlusten durch Fehlbedienungen und Hardwareausfälle bietet so ziemlich jede Kopie, die getrennt vom Original abgelegt ist. Für kleine Datenmengen mögen schon USB-Sticks als Speichermedium reichen, die Dinger gibt es schon für wenige Euro im Sammelpack. Für Laien oft einfacher ist das Ausdrucken auf Papier. Diese Art von Backup ist sogar langlebig: Ein 60 Jahre altes Foto mag vergilbt sein, das Motiv ist aber noch erkennbar. Zum Vergleich: Versuchen Sie mal, eine nur halb so alte CD zu lesen.

Feuerfest

Wenn in Ihrer Wohnung Feuer ausbricht, verbrennen neben dem PC liegende USB-Datenträger gleich mit. Also muss das Sicherungsmedium woanders hin. Keller und Dachboden mögen naheliegend sein, reichen aber nicht, denn das Löschwasser fließt in den Keller und die Flammen kommen überall hin. Kurzum: Das Backup muss raus aus dem Haus. Nehmen Sie beispielsweise eines Ihrer Backupmedien aus dem Büro abends mit nach Hause oder lagern Sie es bei Verwandten. Leicht merken lässt sich das als 3-2-1-Regel: 3 Kopien auf 2 Datenträgern, davon 1 außer Haus.

Trojanersicher

Verschlüsselungstrojaner greifen heutzutage so ziemlich alles an, was sie erreichen können. Fehlende Zugriffsrechte versuchen sie sich zu verschaffen. Daher ist ein Backup nur dann zuverlässig, wenn Sie es technisch getrennt vom Original aufbewahren. Es darf vom Quellrechner aus auf keinem(!) Weg erreichbar sein. Ein USB-Laufwerk, welches nach dem Sichern abgestöpselt wird, ist technisch getrennt – doch Obacht: Wenn Sie es für die nächste Sicherung wieder anstöpseln, ist es eben wieder nicht mehr getrennt. Dagegen hilft nur, mehrere Sicherungsmedien im Wechsel oder Einmalmedien wie DVDs zu verwenden.

Diebstahlsicher

Wenn ein Dieb Zugriff auf das Backupmedium erlangt, kann er die Daten darauf lesen. Lagern Sie es also am besten in einem feuerfesten Tresor. Alternativ hilft das Verschlüsseln des Backups; dann bekommt der Dieb mangels Schlüssel nur Datenmüll zu sehen. Wichtig: Stellen Sie sicher, dass Sie das Backup im Ernstfall wieder entschlüsseln können.

Testen

Solange Sie Ihr Backup nicht testweise wiederhergestellt haben, darf es nicht als zuverlässig gelten. Verwenden Sie zum Wiederherstellen unbedingt einen anderen PC – wenn der alte verbrannt oder geklaut ist, stehen Sie vor genau der gleichen Situation.

Wiederholen

Backups veralten, weil die seitdem hinzugekommenen Daten naturgemäß nicht enthalten sind. Sichern Sie Ihre Daten also regelmäßig. Noch besser ist es, wenn Sie den Vorgang so weit automatisieren, dass er ohne aktive Mithilfe abläuft. Achten Sie dann aber unbedingt darauf, dass Fehlschläge erkannt werden und Sie davon erfahren. Dazu kann es sinnvoll sein, die Logs automatisch auf dem Schirm erscheinen zu lassen, etwa beim morgendlichen Start des Arbeitsplatz-PCs oder per regelmäßig versandter Mail.

Ruhiger schlafen

Ihr Backup erfüllt alle Anforderungen? Herzlichen Glückwunsch! Falls nicht: In c’t 10/2020 finden Sie ab Seite 16 gleich drei Artikel mit Tipps zum Einrichten von Backups für Admins sowie für ein zentrales Backup für Ihre ganze Familie, egal, wie weit verstreut die Verwandten leben. *(axv@ct.de)* c't

Sicher veröffentlichen

Security-Checkliste Server & Hosting

Bild: Andreas Martini

Sobald ein Server aus dem Internet erreichbar ist, wird er zum potenziellen Angriffsziel. Sichern Sie Ihren Heim- oder Mietserver oder das Webhosting-Paket also besser sofort ab.

Von Jan Mahn

Mit Besuch rechnen

Ein aus dem Internet erreichbarer Server ist nicht „geheim“, nur weil Sie keine Domain für die Seite eingerichtet haben. In wenigen Stunden kann ein Angreifer sämtliche IPv4-Adressen des Internets durchprobieren und wird Ihre versteckt geglaubte Seite finden. Auch wenn Sie Ihren Server nur per IPv6 zugänglich machen, wo die Wahrscheinlichkeit, zufällig entdeckt zu werden, wirklich winzig ist, gehört ein Kennwort vor Ihre Dienste. Welches Protokoll Sie auch verwenden: Transportverschlüsselung mindestens mit TLS 1.2 ist Pflicht. TLS 1.0 und 1.1 sind unsicher und gehören abgeschaltet. Sobald Sie ein Zertifikat für eine Domain bestellen, ist diese übrigens öffentlich bekannt: Durchsuchbar ist die Liste aller ausgestellten Zertifikate zum Beispiel über die Seite crt.sh.

Sich selbst angreifen

Wer einen Dienst im Internet veröffentlicht, sollte öfter mal die Perspektive wechseln. Schauen Sie sich die veröffentlichten Dienste nicht nur aus Nutzer-, sondern hin und wieder aus Angreifersicht an. Scannen Sie Ihr Netzwerk auf offene Ports oder nutzen Sie dafür am besten ein externes Monitoringwerkzeug. Viele Datenlecks, über die wir berichtet haben, hätten verhindert werden können, wenn die Betreiber Authentifizierung (Anmeldung) und Autorisierung (Berechtigungsprüfung) in Ruhe geprüft hätten. Beliebteste Fehler: Windows-Dateifreigaben (SMB) ohne Anmeldung, Webserver mit aktivem Directory Listing und Webanwendungen mit URLs, die hochzählbare Zahlen enthalten und Zugriff auf fremde Daten gestatten.

SSH, aber sicher

SSH ist ein vergleichsweise sicherer Weg auf Ihren Server, unter Linux-Admins schon lange der Standard und auch für Windows verfügbar. Um die Sicherheit zu erhöhen, sollten Sie sich per Public-Key-Verfahren anmelden und den Zugang per Kennwort abschalten. Das macht Brute-Force-Attacken nahezu unmöglich. Häufig wird empfohlen, den SSH-Server auf einem anderen Port als 22 lauschen zu lassen. Das ist aber nur ein schwacher Schutz und fällt in die Kategorie „Security by Obscurity“.

Zweiten Faktor nutzen

Die Homepage ist für Unternehmen das Schaufenster zum Kunden. Wenn Sie die bei einem Hoster betreiben, ist ein zweiter Faktor für den Admin-Zugang heute Pflicht. Ein einziges Kennwort als Schutz für die gesamten Web-Angebote eines Unternehmens ist heute nicht mehr zeitgemäß! Wer an die Verwaltungsoberfläche kommt, kann eine Menge Schaden anrichten und Sie sogar für längere Zeit aussperren; hat er Ihre Kontaktdaten geändert, müssen Sie im ungünstigen Fall erst beweisen, dass Sie der rechtmäßige Eigentümer sind. Unterstützt der Anbieter keinen zweiten Faktor, fragen Sie beim Kundenservice nach, ob die Funktion in Planung ist, oder suchen Sie sich einen neuen Hoster.

Aktuell halten

Halten Sie die Systeme aktuell. Auf dem neuesten Stand sein sollte unbedingt das Betriebssystem des Servers, ebenso der Webserver und die Interpreter der verwendeten Skriptsprachen (wie PHP, Node.js und Python). Am besten automatisieren Sie die Updates, damit sie regelmäßig ausgeführt werden.

Logfiles sollten Sie nicht erst studieren, wenn es ein Problem gibt. Werfen Sie regelmäßig einen Blick auf die Protokolle. Auch die Logs des SSH-Servers oder unter Windows für Remote Desktop sollten Sie regelmäßig auf Auffälligkeiten checken. In großen Umgebungen sollten Sie das Monitoring all Ihrer Systeme auf einer Plattform zentralisieren, visualisieren und Alarme einrichten. Nur dann fallen Angriffe zeitnah auf.

Nicht alles gehört ins Internet

Die Port-Weiterleitung ist eine Funktion, die jeder Haushaltsrouter unterstützt. Weil sie so einfach einzurichten ist, sind sich viele nicht bewusst, welche Verantwortung der Klick mitbringt: Wer ein Gerät zum Beispiel auf Port 80 ins Internet hängt, ist ab dem Moment Serverbetreiber! Die Software muss fürs Veröffentlichen im Internet ausgelegt und mit sicheren Zugangsdaten verriegelt sein. Vorsicht ist geboten, wenn Heizungsmonteur oder Elektriker die Heizung oder den PV-Wechselrichter mal „schnell im Router freigeben“ wollen. Solche Geräte sind nicht als Server fürs weltweite Internet ausgelegt. Die sichere Alternative zur Portweiterleitung ist ein VPN-Tunnel ins Heimnetz.

(jam@ct.de) c't

Passwort: sicher

Security-Checkliste Passwörter & Accounts

Passwörter sind nicht nur ein notwendiges Übel, sondern der Schlüssel zur digitalen Identität. Mit den folgenden Tipps haben Sie so wenig Passwortstress wie möglich, ohne an der Sicherheit zu sparen.

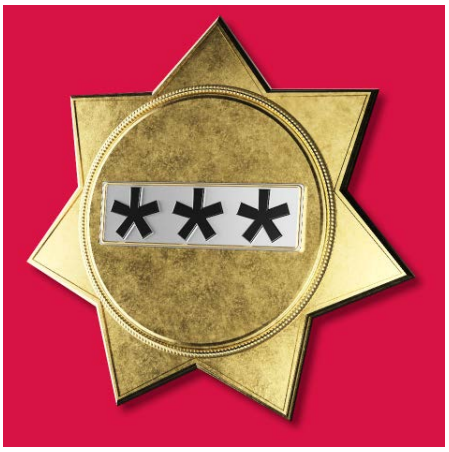


Bild: Andreas Martini

Von Ronald Eikenberg

Nicht recyceln

Nutzen Sie für jeden Dienst ein anderes Kennwort. Sollten Sie Passwörter recycelt haben, gehen Sie am besten alle wichtigen Zugänge durch und legen Sie individuelle Passwörter fest – insbesondere bei Diensten, bei denen es um persönliche Daten oder um Geld geht.

Besser lang

Um Passwörter ranken sich zahlreiche Mythen, viele davon sind inzwischen widerlegt. So gilt es als überholt, Passwörter regelmäßig zu ändern. Ändern müssen Sie ein Passwort nur, wenn es in die falschen Hände gelangt, etwa nach einem Hack.

Ein gutes Passwort muss alltagstauglich sein und sich auch am Smartphone eintippen lassen. Besser als möglichst viele Sonderzeichen ist es, möglichst lange Passwörter einzusetzen: Die Länge ist der größte Hebel, um die Sicherheit zu erhöhen. Insbesondere bei Verschlüsselung (Dateien, Festplatten, PGP & Co.) sollten Sie so viele Zeichen nutzen, wie Sie handhaben können. Ein Weg zum Ziel ist das Aneinanderreihen von Wörtern zu „Passphrasen“, absichtliche Schreibfehler sorgen für mehr Sicherheit.

Passwortmanager

Nutzen Sie am besten einen Passwortmanager wie KeePass oder Bitwarden, um Ihre Zugangsdaten zu verwalten. Die nützlichen Helfer speichern Passwörter sicher verschlüsselt auf Rechner, Smartphone und Tablet. Sie müssen sich dann nur noch das Masterpasswort merken, mit dem Sie den Passwortmanager entsperren. Einen Vergleichstest von 15 Passwortmanagern finden Sie in c't 5/2021 [1].

Darknet-Leaks checken

Cyber-Ganoven erbeuten immer wieder und im großen Stil Datenbanken mit Zugangsdaten. Überprüfen Sie von Zeit zu Zeit in öffentlichen Datenbanken, ob und für welche Ihrer Zugänge Passwörter bereits im Darknet kursieren. Das können Sie zum Beispiel mit dem „HPI Identity Leak Checker“ und „Have i been pwned?“ herausfinden (siehe ct.de/check2023). Gibt es einen Treffer, sollten Sie das betroffene Passwort als kompromittiert betrachten und ändern. Rechnen Sie außerdem mit einem Anstieg an Phishingmails an die betroffene Mailadresse, die sich möglicherweise sogar auf den gehackten Dienst beziehen.

Zwei Faktoren nutzen

Viele Onlinedienste bieten eine optionale Zwei-Faktor-Authentifizierung (2FA), die effektiv vor Hackern schützt: Ist sie aktiv, fragt der Dienst beim Einloggen nicht nur nach dem Passwort, sondern auch nach einem zweiten Faktor, etwa in Form eines Zahlencodes. Schalten Sie wann immer möglich eine 2FA-Methode ein [2]. Meiden Sie dabei aber das SMS-Verfahren, da es unsicher ist. Nutzen Sie besser das Verfahren „Time-based One-time Password“ (TOTP), bei dem Sie die Codes selbst mit einer App wie Google Authenticator, Authy oder FreeOTP generieren.

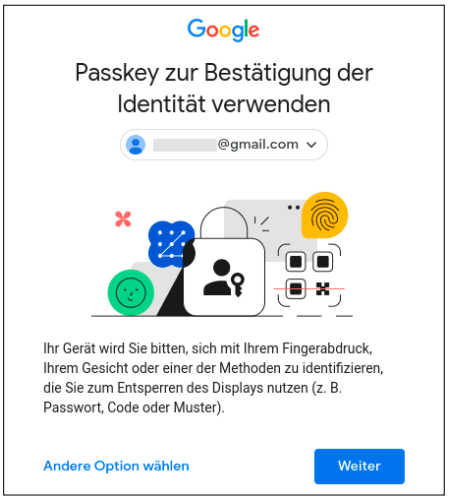
Am sichersten ist FIDO2, das jedoch noch nicht viele Webdienste als Anmeldemethode anbieten. Zukünftig werden Sie sich bei immer mehr Diensten mit einem sogenannten Passkey [3] registrieren und einloggen können. Die Eingabe eines Passworts oder 2FA-Codes ist damit nicht mehr nötig. Nutzen Sie diese Möglichkeit, wenn sie angeboten wird. Das klappt unter anderem bereits bei Google. *(rei@ct.de)* c't

Literatur

[1] Jan Schüßler, Marvin Strathmann, Ich kaufe ein ****, 25 Passwortmanager für PC und Smartphone, c't 5/2021, S. 16

[2] Kathrin Stoll, Abgedichtet, Angriffe auf den zweiten Faktor – So schützen Sie sich, c't 11/2023, S. 26

[3] Ronald Eikenberg, Zukunft ohne Passwort, Bestandsaufnahme: Passwort-Nachfolger Passkeys, c't 13/2023, S. 12



Sicher ohne Passwort: Bei manchen Diensten kann man bereits Passkeys zur Authentifizierung nutzen.

Impressum

Redaktion

Heise Medien GmbH & Co. KG, Redaktion c't
Postfach 61 04 07, 30604 Hannover
Karl-Wiechert-Allee 10, 30625 Hannover
Telefon: 05 11/53 52-300
Telefax: 05 11/53 52-417
Internet: www.ct.de, E-Mail: ct@ct.de

Chefredakteur: Torsten Beeck *(tbe@ct.de)* (verantwortlich für den Textteil)

Stellv. Chefredakteur: Axel Kossel *(ad@ct.de)*

Chef vom Dienst: Georg Schnurer *(gs@ct.de)*

Leser & Qualität

Leitung: Achim Barczok *(acb@ct.de)*

Koordination Leserkommunikation: Martin Triadan *(mat@ct.de)*

Leiter redaktionelle Entwicklung: Jobst Kehrhahn **(***keh@ct.de***)**

Ressort Internet, Datenschutz & Anwendungen

Leitende Redakteure: Hartmut Gieselmann *(hag@ct.de)*, Jo Bager *(jo@ct.de)*

Redaktion: Holger Bleich *(hob@ct.de)*, Anke Brandt *(abr@ct.de)*, Greta Friedrich *(gref@ct.de)*, Tim Gerber *(tig@ct.de)*, Arne Grävemeyer *(agr@ct.de)*, Markus Montz *(mon@ct.de)*, Peter Schmitz *(psz@ct.de)*, Sylvester Tremmel *(syt@ct.de)*, Andrea Trinkwalder *(atr@ct.de)*, Dorothee Wiegand *(dwi@ct.de)*, Stefan Wischner *(swi@ct.de)*

Ressort Systeme & Sicherheit

Leitende Redakteure: Peter Siering *(ps@ct.de)*, Jan Mahn *(jam@ct.de)*

Redaktion: Niklas Dierking *(ndi@ct.de)*, Mirko Dölle *(mid@ct.de)*, Wilhelm Drehling *(wid@ct.de)*, Liane M. Dubowy *(lmd@ct.de)*, Ronald Eikenberg *(rei@ct.de)*, Oliver Lau *(ola@ct.de)*, Pina Merkert *(pmk@ct.de)*, Dennis Schirrmacher *(des@ct.de)*, Hajo Schulz *(hos@ct.de)*, Jan Schüßler *(jss@ct.de)*, Kathrin Stoll *(kst@ct.de)*, Keywan Tonekaboni *(ktn@ct.de)*, Axel Vahldiek *(axv@ct.de)*

Ressort Hardware

Leitende Redakteure: Christof Windeck *(ciw@ct.de)*, Ulrike Kuhlmann *(uk@ct.de)*, Dušan Živadinović *(dz@ct.de)*

Redaktion: Ernst Ahlers *(ea@ct.de)*, Christian Hirsch *(chh@ct.de)*, Benjamin Kraft *(bkr@ct.de)*, Lutz Labs *(ll@ct.de)*, Andrijan Möcker *(amo@ct.de)*, Florian Müssig *(mue@ct.de)*, Rudolf Opitz *(rop@ct.de)*, Carsten Spille *(csp@ct.de)*

Ressort Mobiles, Entertainment & Gadgets

Leitende Redakteure: Jörg Wirtgen *(jow@ct.de)*, Jan-Keno Janssen *(jkj@ct.de)*

Redaktion: Robin Brand *(rbr@ct.de)*, Sven Hansen *(sha@ct.de)*, Steffen Herget *(sht@ct.de)*, Nico Jurran *(nij@ct.de)*, André Kramer *(akr@ct.de)*, Michael Link *(mil@ct.de)*, Urs Mansmann *(uma@ct.de)*, Stefan Porteck *(spo@ct.de)*, Christian Wölbert *(cwo@ct.de)*

c't Sonderhefte
Leitung: Jobst Kehrhahn **(***keh@ct.de***)**
Koordination: Pia Ehrhardt **(***piae@ct.de***)**, Angela Meyer *(anm@ct.de)*

c't online: Ulrike Kuhlmann *(uk@ct.de)*

Social Media: Jil Martha Baae *(jmb@ct.de)*

Koordination News-Teil: Hartmut Gieselmann *(hag@ct.de)*, Christian Wölbert *(cwo@ct.de)*

Koordination Heftproduktion: Martin Triadan *(mat@ct.de)*

Redaktionsassistenz: Susanne Cölle *(suc@ct.de)*, Christopher Tränkmann *(cht@ct.de)*

Software-Entwicklung: Kai Wasserbäch *(kaw@ct.de)*

Technische Assistenz: Ralf Schneider (Ltg., rs@ct.de), Christoph Hoppe *(cho@ct.de)*, Stefan Labusga *(sla@ct.de)*, Arne Mertins *(ame@ct.de)*, Jens Nohl *(jno@ct.de)*, Daniel Ladeira Rodrigues *(dro@ct.de)*

Dokumentation: Thomas Masur *(tm@ct.de)*

Verlagsbüro München: Hans-Pinsel-Str. 10b, 85540 Haar, Tel.: 0 89/42 71 86-0, Fax: 0 89/42 71 86-10

Ständige Mitarbeiter: Detlef Borchers, Herbert Braun *(heb@ct.de)*, Tobias Engler, Monika Ermert, Stefan Krempl, Ben Schwan *(bsc@ct.de)*, Christiane Schulzki-Haddouti

DTP-Produktion: Mike Bunjes, Birgit Graff, Angela Hilberg, Jessica Nachtigall, Astrid Seifert, Ulrike Weis

Junior Art Director: Martina Bruns

Fotografie: Melissa Ramson, Andreas Wodrich

Digitale Produktion: Melanie Becker, Kevin Harte, Martin Kreft, Thomas Kaltschmidt, Pascal Wissner

Illustrationen

Jan Bintakies, Hannover, Rudolf A. Blaha, Frankfurt am Main, Thorsten Hübner, Berlin, Albert Hulm, Berlin, Sven Hauth, Schülp, Thomas Kuhlenbeck, Münster, Timo Lenzen, Berlin, Andreas Martini, Wettin, Moritz Reichartz, Viersen, Michael Vogt, Berlin
Editorial: Hans-Jürgen „Mash" Marhenke, Hannover, Schlagseite: Ritsch & Renn, Wien, c't-Logo: Gerold Kalter, Rheine

c't-Krypto-Kampagne: Infos zur Krypto-Kampagne unter https://ct.de/pgp. Die Authentizität unserer Zertifizierungsschlüssel lässt sich mit den nachstehenden Fingerprints überprüfen:

```
Key-ID: 5C1C1DC5BEEDD33A
ct magazine CERTIFICATE <pgpCA@heise.de>
D337 FCC6 7EB9 09EA D1FC 8065 5C1C 1DC5 BEED D33A
Key-ID: 2BAE3CF6DAFFB000
ct magazine CERTIFICATE <pgpCA@ct.heise.de>
A3B5 24C2 01A0 D0F2 355E 5D1F 2BAE 3CF6 DAFF B000
Key-ID: DBD245FCB3B2A12C
ct magazine CERTIFICATE <pgpCA@ct.heise.de>
19ED 6E14 58EB A451 C5E8 0871 DBD2 45FC B3B2 A12C
```

heise Investigativ: Über diesen sicheren Briefkasten können Sie uns anonym informieren.
Anonymer Briefkasten: https://heise.de/investigativ
via Tor: ayznmonmewb2tjvgf7ym4t2726muprjvwckzx2vhf2hbarbbzydm7oad.onion

Verlag

Heise Medien GmbH & Co. KG
Postfach 61 04 07, 30604 Hannover
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, Beate Gerold

Mitglieder der Geschäftsleitung: Jörg Mühle, Falko Ossmann

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

Anzeigenpreise: Es gilt die Anzeigenpreisliste Nr. 40 vom 1. Januar 2023.

Anzeigen-Auslandsvertretung (Asien): Media Gate Group Co., Ltd., 7F., No. 182, Section 4, Chengde Road, Shilin District, 11167 Taipei City, Taiwan, www.mediagate.com.tw Tel: +886-2-2882-5577, Fax: +886-2-2882-6000, E-Mail: mei@mediagate.com.tw

Leiter Vertrieb und Marketing: André Lux (-299)

Werbeleitung: Julia Conrades (-156)

Service Sonderdrucke: Julia Conrades (-156)

Druck: Firmengruppe APPL, appl druck, Senefelderstr. 3-11, 86650 Wemding

Kundenkonto in der Schweiz: PostFinance, Bern, Kto.-Nr. 60-486910-4, BIC: POFICHBEXXX, IBAN: CH73 0900 0000 6048 6910 4

Vertrieb Einzelverkauf:

DMV Der Medienvertrieb GmbH & Co. KG
Meßberg 1
20086 Hamburg
Tel.: 040/3019 1800, Fax: 040/3019 1815
E-Mail: info@dermedienvertrieb.de

c't erscheint 14-täglich

Einzelpreis 5,90 €; Österreich 6,50 €; Schweiz 9.90 CHF; Belgien, Luxemburg 6,90 €; Niederlande 7,20 €; Italien, Spanien 7,40 €, Dänemark 64,00 DKK

Abonnement-Preise: Das Jahresabonnement kostet inkl. Versandkosten: Inland 144,20 €, Österreich 155,40 €, Europa 165,20 €, restl. Ausland 191,80 € (Schweiz 236.60 CHF); ermäßigtes Abonnement für Schüler, Studenten, Auszubildende (nur gegen Vorlage einer entsprechenden Bescheinigung): Inland 105,00 €, Österreich 99,40 €, Europa 124,60 €, restl. Ausland 152,60 € (Schweiz 145.60 CHF). c't-Plus-Abonnements (inkl. Zugriff auf das c't-Artikel-Archiv sowie die App für Android und iOS) kosten pro Jahr 25,00 € (Schweiz 30.80 CHF) Aufpreis. Ermäßigtes Abonnement für Mitglieder von AUGE, bdvb e.V., BvDW e.V., /ch/open, GI, GUUG, ISACA Germany Chapter e.V., JUG Switzerland, VBIO, VDE und VDI (gegen Mitgliedsausweis): Inland 108,15 €, Österreich 116,55 €, Europa 123,90 €, restl. Ausland 143,85 € (Schweiz 177.45 CHF). Luftpost auf Anfrage.

Leserservice:

Bestellungen, Adressänderungen, Lieferprobleme usw.
Heise Medien GmbH & Co. KG
Leserservice
Postfach 24 69
49014 Osnabrück
E-Mail: leserservice@ct.de
Telefon: 05 41/8 00 09-120
Fax: 05 41/8 00 09-122

c't abonnieren: Online-Bestellung via Internet (*www.ct.de/abo*) oder E-Mail *(leserservice@ct.de)*.

ISSN 0724-8679 AWA LAE