Sicherheit? Check!

Die c’t-Security-Checklisten 2026



Einleitung	Seite 1	Browser	Seite 10
Mobiles Arbeiten	Seite 3	Onlinebetrug	Seite 11
Windows	Seite 4	Soziale Netzwerke	Seite 12
Smartphone	Seite 5	Onlinebanking	Seite 13
WLAN-Router	Seite 6	Datensicherung	Seite 14
E-Mail	Seite 7	Server & Hosting	Seite 15
KI-Sprachmodelle	Seite 8	Smart Home	Seite 16
Messenger	Seite 9	Passwörter	Seite 17

Bild: Jessica Nachtigall / KI / heise medien

Oft reichen wenige Handgriffe, um die Sicherheit der eigenen Geräte zu verbessern. In unseren Checklisten finden Sie zahlreiche Prüfpunkte und somit klare Hinweise, wie Sie die Wahrscheinlichkeit reduzieren, Opfer eines Cyberangriffs zu werden.

Von Wilhelm Drehling

Kaum jemand wird gezielt von Hackern oder Betrügern im Internet ins Visier genommen. Die Suche nach Angriffszielen läuft meist automatisiert und den Tätern ist jedes Opfer recht, von der Privatperson bis zum Großkonzern.

Mit unseren Tipps & Tricks schließen Sie mögliche Einfallstore und stellen sicher, dass die üblichen Angriffsmethoden ins Leere laufen. Ein Großteil der Sicherheitsmaßnahmen setzen Sie mit wenigen Klicks um. Verlieren Sie also am besten keine Zeit und fangen Sie gleich an.

Neu: Checkliste zu Smart Home

Völlige IT-Sicherheit ist eine Illusion. Die Bedrohungen verändern sich ständig, weshalb Sie nie davon ausgehen können, abschließend für alle Zeiten alles richtig abgesichert zu haben. Grund genug, dass auch wir unsere Security-Checklisten sich immer wieder an die gerade währende Bedrohungslage anpassen. Schon in den vorigen Versionen unserer Checklisten kam daher eine Liste zu Onlinebetrug (S. 11) und eine zum Umgang mit KI-Sprachmodellen (S. 8) hinzu.

In diesem Jahr finden Sie auf Seite 16 eine neue Checkliste zu IoT- und Smart-Home-Produkten. Darin geben wir unter anderem Tipps, wie Sie besonders gefährdete Geräte wie am Haus angebrachte WLAN-Kameras schützen. Sollten Sie einen eigenen Server betreiben, dann hilft Ihnen die Liste auf Seite 15 über Server und Hosting.

Frisch aufbereitet

Auch die restlichen Checklisten haben eine kritische Durchsicht und eine ordentliche Auffrischung erfahren. Wenngleich Sie die Themen schon kennen, lohnt es sich dennoch, einen Blick auf sie zu werfen, um Ihr Wissen auf dem neuen Stand zu halten.

Wie Sie es vielleicht schon von den vorherigen Checklisten gewohnt sind, haben wir die Listen nach Themengebieten grob sortiert. Sie können die Checklisten in chronologischer Reihenfolge durchflöhen oder direkt zur Seite springen, die Sie interessiert. Den Anfang macht die Liste zum Arbeitsplatz zu Hause (S. 3), gefolgt von Windows (S. 4), Smartphone (S.5) und WLAN-Router (S. 6).

Einen Schwerpunkt bildet das Phishing. Es erfährt gegenwärtig eine Renaissance und es ist durch KI gefährlicher geworden. Passen Sie also nicht nur auf, wenn jemand Unbekanntes Sie über Mail (S. 7), Messenger (S. 9) oder über Social Media (S. 12) kontaktiert. Denn auch hinter scheinbar bekannten Menschen oder Institutionen verbergen sich immer öfter Phishing-Versuche, bei denen man versucht, Sie auf eine täuschend echt aussehende Seite etwa einer Bank weiterzuleiten und Ihre Anmeldedaten abzugreifen.

In eher persönlichen Ansprachen versuchen Betrüger, Ihre Skepsis über die emotionale Schiene zu überwinden, um später aus obskuren Gründen Geld zu fordern. Seit einiger Zeit gibt es eine weitverbreitete Masche, in der man zu einer Telegram-Gruppe eingeladen oder direkt angeschrieben wird, um bestimmte Seiten gegen Bezahlung zu liken. Am Ende läuft es darauf hinaus, den Betrügern Geld zu schicken, um bessere Angebote freizuschalten.

Mehr zum Thema in der Checkliste Onlinebetrug auf Seite 11 und Onlinebanking auf Seite 13. Wie Sie Ihre Benutzerkonten am besten schützen, erfahren Sie auf Seite 17, wo es unter anderem um Passwörter geht.

Weitergeben als Gratis-PDF

Damit sich unsere Tipps möglichst weit herumsprechen, haben wir alle Checklisten in voller Länge in einem kostenfreien PDF-Booklet zusammengefasst. Dieses können Sie über ct.de/check2026 herunterladen und dann an Freunde, Familie und Bekannte verteilen. *(wid@ct.de)* c't

PDF-Booklet kostenfrei herunterladen:
ct.de/check2026



Seien Sie auf der Hut bei Nachrichten, die zum Kontakt mit anderen Nummern auffordern (links) oder Geld für einfache Dienste versprechen (rechts).

Home und Office

Security-Checkliste für die Heimarbeit

Die Arbeit hat sich vom Platz im Büro entkoppelt. 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.



Bild: Jessica Nachtigall / KI / heise medien

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 Artikel „Security-Checkliste Windows“ auf S. 4). 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. Nutzen Sie statt öffentlichen WLAN-Hotspots eine mobile Datenverbindung. Falls es unbedingt ein Hotspot sein muss, dann ist ein verschlüsseltes VPN erst recht Pflicht.

Schützen Sie Ihre Geräte und Daten auch vor direkten, physischen Zugriffen. 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 alle externen Datenträger. Defekte Speichermedien entsorgen Sie nicht selbst, sondern über die Firma. Denn die muss sicherstellen, dass sensible Informationen verlässlich 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 ganz kurz“ aus den Augen lassen (unter Windows mit Windows+L, am Mac mit Control+Command+Q). 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 das auf Ihrem Betriebssystem möglich ist.

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 automatisches Synchronisieren per Backupsoftware ein. Verzichten Sie möglichst darauf, Dokumente auf USB-Sticks und externen Platten hin und her zu tragen.

Konferenzen kontrollieren

Virenschutz hin, Firewall her: Die größte Schwachstelle in der Firmen-IT ist immer noch der Mensch. Im Homeoffice stehen Ihnen 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 beispielsweise unbedingt Fotos vom letzten Meeting veröffentlichen müssen, machen Sie vorher sensible Daten wie URLs, Meeting-IDs sowie die Gesichter der Teilnehmer unkenntlich.

Anrufe 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, ein Geschäftspartner oder der Chef telefonisch bei Ihnen, sollten Sie keine sensiblen Daten preisgeben und sich schon gar nicht auf eine Fernwartung einlassen.

Selbst den vertrauten Stimmen und Gesichtern müssen Sie zunehmend mit Skepsis begegnen, denn sie lassen sich immer besser synthetisch nachahmen. Rufen Sie die Person, die angeblich angerufen hat, beim leisesten Zweifel lieber unter der bekannten – nicht der angezeigten – Rufnummer zurück und klären Sie den Sachverhalt direkt. *(atr@ct.de)* c't

Fenster schließen

Security-Checkliste Windows



Bild: Jessica Nachtigall / KI / heise medien

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 und installieren Sie alle verfügbaren Aktualisierungen.

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. Beachten Sie, dass Windows 10 seit dem 14. Oktober 2025 nicht mehr von Microsoft mit Sicherheitsupdates versorgt wird. Wer weiterhin Updates benötigt, kann Microsofts ESU-Programm (Extended Security Updates) nutzen: einmalig rund 30 Euro für ein Jahr, für EU-Nutzer nach einer Intervention von Verbraucherschützern sogar kostenlos. 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. 14).

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 und navigieren zu „Schutzupdates“.

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.

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. Trennen Sie hierzu die Internetverbindung während der Windows-Installation. Öffnen Sie die Eingabeaufforderung mit Umschalt+F10 und geben Sie `oobe\bypassnro` ein. Danach startet die Installation neu und Sie können nach der Länder- und Tastatureinstellung „Ich habe kein Internet“ wählen und ein lokales Konto erstellen. *(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

Mobil und sicher

Security-Checkliste Smartphone



Bild: Jessica Nachtigall / KI / heise medien

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

Betriebssystem-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. Apple versorgt seine iPhones vorbildlich mit Updates: Das aktuelle iOS 26 läuft noch auf dem iPhone 11 und SE 2 von 2019 beziehungsweise 2020.

Bei Android ist die Lage durchwachsen: Insbesondere bei preiswerten Smartphones versiegt der Update-Fluss oft nach kurzer Zeit. Google Pixel, Samsung-Flaggschiffe und Xiaomi-15-Modelle erhalten inzwischen aber sechs bis sieben Jahre Updates.

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.

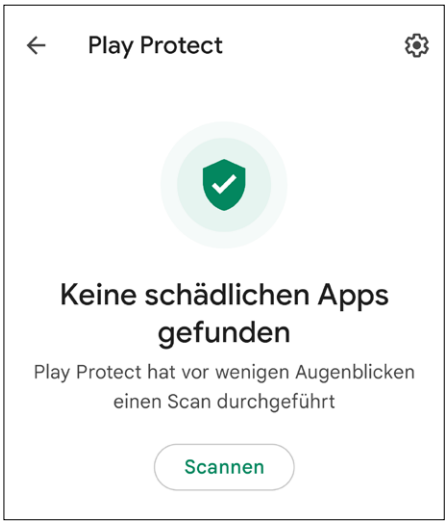
Zugriffsschutz aktivieren

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 schwer 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.



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

App-Berechtigungen

Prüfen Sie vor dem Installieren und Nutzen 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 das System tiefgreifend ändern. Das hebelt jedoch auch essenzielle Schutzfunktionen aus, sodass zahlreiche Anwendungen wie Banking-Apps den Start verweigern. *(rei@ct.de)* c't

Netz gesichert

Security-Checkliste WLAN-Router



Bild: Jessica Nachtigall / KI / heise medien

Assistenten richten den WLAN-Router zwar binnen Minuten ein, aber optimale Sicherheit braucht oft etwas Nacharbeit, selbst wenn der Netzverteiler schon gemäß WPA3 verschlüsselt.

Von Ernst Ahlers

Konfiguration abdichten

Moderne Router kommen normalerweise vollautomatisch ins Netz, nur manchmal muss man selbst noch per Browser oder Smartphone-App Hand anlegen. Dabei gehen die Assistenten aber an manchen empfehlenswerten Optionen vorbei, sodass Lücken bleiben.

Ändern Sie zuerst das voreingestellte Konfigurationspasswort. Weil es typischerweise auf dem Typenschild steht, reicht Unbefugten ein schnelles Foto, um später den Router unbemerkt manipulieren zu können. Falls vorhanden und abgeschaltet, aktivieren Sie das automatische Firmware-Update. Dann hält sich der Router selbstständig frisch, selbst wenn Sie auf Reisen sind.

Richtig verschlüsseln

Bei der WLAN-Verschlüsselung sollte der Mixed-Mode WPA2+WPA3 aktiv sein. Falls Sie wegen alter Clients auf WPA2 bleiben müssen, schalten Sie den Schutz der Steuerpakete (PMF) ein. Ändern Sie den Funknetznamen und das WLAN-Passwort, weil diese ebenfalls meist auf dem Typenschild stehen.

Verwenden Sie ein Passwort von mindestens 24, besser 30 Zeichen Länge. Denn einige Knackprogramme können WPA2-Passwörter durch Probieren herausfinden (Brute-Force-Attacke). Dafür zeichnen Angreifer den WLAN-Verkehr auf und führen diesen später einem leistungsfähigen PC zu. Ob er dann Ihr Passwort schnell findet, hängt von der Länge des Passworts ab.

Gastnetz nutzen

Aktivieren Sie das Gast-WLAN und stecken Sie Besucher, Smart-Home- und IoT-Geräte dort hinein. Auch das Gastnetz braucht ein langes Passwort. Müssen Sie fürchten, dass Besucher es weitergegeben haben, muss ein neues her, gegebenenfalls regelmäßig (Kalendertermin). Erlauben Sie im Gast-WLAN nur wenige Dienste, beispielsweise Surfen und Mailen, um unerwünschtes Filesharing zu unterbinden.

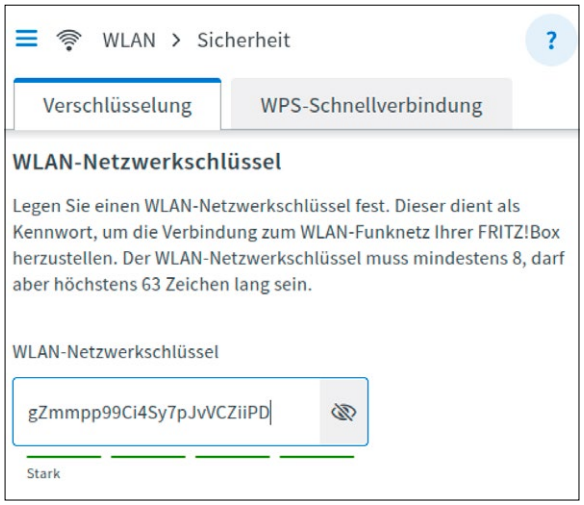
Falls die Webseite des Routers aus dem Internet erreichbar ist, muss das per HTTPS geschehen, besser aber ausschließlich per routereigenem VPN (WireGuard oder IPsec). Das gilt auch für einen Heimserver, dessen Dienste Sie unterwegs brauchen. VPN ist sicherer als Portweiterleitungen, die eine gute serverseitige Absicherung voraussetzen. Weitere Tipps für eigene Server finde Sie in der Security-Checkliste „Server & Hosting“ auf Seite 64.

WPS nur vorübergehend

Mit Wi-Fi Protected Setup genügt ein WPS-Tastendruck, um Clients ins WLAN zu bringen. So können sich auch Unbefugte in einem unbeobachteten Moment Zugang zum Heimnetz verschaffen. Schalten Sie WPS deshalb nur bei Bedarf ein und anschließend wieder aus.

Ähnliches gilt für UPnP: Über diese Router-Automatik können sich Geräte eine Portweiterleitung zum Internet selbst einrichten. Das ist bequem, erleichtert aber auch eingeschleppter Malware das Leben. Lassen Sie UPnP deshalb nur vorübergehend laufen oder schränken Sie es auf einzelne Netzwerk-Hosts ein.

Wenn der Router abgedichtet ist, exportieren Sie seine Konfiguration, damit es nach einem Defekt mit dem Ersatz durch Konfigurationsimport schnell weitergehen kann. *(ea@ct.de)* c't



Der Passwortgenerator Ihres Passwortsafes spendiert einen guten, mindestens 24 Zeichen langen WLAN-Schlüssel aus Buchstaben und Ziffern. Den muss man fast nie abtippen: Die meisten Geräte können den WLAN-Zugang per WPS-Tastendruck, Smartphones und Tablets auch per QR-Code übernehmen.

Problempost

Security-Checkliste E-Mail



Bild: Jessica Nachtigall / KI / heise medien

E-Mails sind sicherheitstechnische Katastrophen, aber extrem weit verbreitet. Kein Wunder, dass Kriminelle dieses alte Medium sehr gerne nutzen. Komplette E-Mail-Abstinenz ist für kaum jemanden eine Option, also sollte man die Gefahren kennen.

Von Sylvester Tremmel

Gesunde Skepsis

Nicht nur durch KI wird es für Angreifer immer leichter, täuschend echte Fälschungen zu fabrizieren. Auch eine Mail mit bekanntem Absender, üblichen Formulierungen und passendem Kontext kann Phishing sein. Gleichzeitig wirken echte Mails leider oft wie Phishing-Attacken, weil Anbieter Links auf krude Domains einbauen oder generische Anreden und reißerische Warnmeldungen formulieren.

Misstrauen Sie E-Mails daher grundsätzlich – nicht nur, aber besonders dann, wenn Anhänge oder Geld im Spiel sind oder die Mail angeblich 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, ganz egal was Mail oder Anhang behaupten, und fragen Sie über einen anderen Kanal beim Absender nach, wenn ein Anhang unerwartet oder untypisch ist. Idealerweise öffnen Sie Anhänge mit einem Werkzeug wie Dangerzone (siehe ct.de/yspz), das darauf spezialisiert ist, riskante Dateien zu entschärfen.

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. Solche Inhalte werden gerne für (Werbe-)Tracking genutzt und sind auch immer wieder an Sicherheitslücken beteiligt.

Am besten schalten Sie auch die HTML-Ansicht aus und lassen sich bloße Textinhalte anzeigen. So sehen Sie direkt, wenn Links auf ungewöhnliche URLs zeigen. Eine Option dafür bieten viele Programme, wenn auch mitunter gut versteckt. Im verbreiteten Client Thunderbird klicken Sie in der Toolbar oberhalb einer Mail auf Mehr/Nachrichteninhalt/Reintext. Nur wenn diese Ansicht absolut unleserlich (oder leer) ist und Sie die Mail nicht unbesehen löschen wollen, sollten Sie – mit einer Extraportion Skepsis – auf die HTML-Darstellung ausweichen. Viele Mailclients erlauben, HTML-Inhalte temporär und mit einem Klick in der Mailansicht zu aktivieren. In Thunderbird rüstet das Add-on „Allow HTML Temp“ (siehe ct.de/yspz) diese Option nach.

Verschlüsselung

Die Verschlüsselung von E-Mails ist ein Trauerspiel. 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.

Einige Mailprovider erlauben, Mails nur zu versenden, wenn so eine Transportverschlüsselung auch zum Mailserver des Empfängers aufgebaut werden kann. Dann können immerhin nur noch die beteiligten Mailserver mitlesen. Sofern Ihr Anbieter diese empfehlenswerte Option anbietet, finden Sie sie in dessen Kontoeinstellungen.

Alle Lauscher aussperren können Sie nur mit Ende-zu-Ende-Verschlüsselung. Auch wenn die einschlägigen Standards S/MIME und OpenPGP mit diversen Problemen und einer geringen Verbreitung kämpfen: Falls Sie sich mit Ihren Korrespondenten auf ein Verfahren einigen können, sollten Sie es nutzen. Zum Einstieg bietet sich der erwähnte Mailclient Thunderbird an, der eine relativ nutzerfreundliche OpenPGP-Unterstützung integriert hat (siehe ct.de/yspz).

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 Ihr Konto erreicht haben. Um selbiges abzusichern, sollten Sie Zwei-Faktor-Authentifizierung (2FA) nutzen, was viele Mailprovider mittlerweile anbieten.

Bedachtes Mailen

Hinterfragen Sie auch beim Versand, wie und wofür Sie E-Mails nutzen. Idealerweise können Sie stattdessen zu einem Messenger greifen (siehe S. 58), praktisch alle sind sicherer als E-Mails. Falls es eine Mail sein soll, verschicken Sie besser reine Textmails. Das erspart den Empfängern die Risiken von HTML-Mails und ist den Verzicht auf Formatierungen wert. Verdächtige Arten von Anhängen wie ausführbare Dateien oder Office-Dokumente mit Makros sollten Sie gar nicht per Mail versenden. Ausführliche Tipps zum Versand haben wir unter ct.de/sicher-mailen aufgeschrieben. *(syt@ct.de)* c't

Erwähnte Werkzeuge und Dokumentation: ct.de/yspz

Reden ist Gold

Security-Checkliste KI-Sprachmodelle



Bild: Jessica Nachtigall / KI / heise medien

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

Von Sylvester Tremmel

Large Language Models (LLM), also große Sprachmodelle wie GPT oder Gemini, sind die Grundlage 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 einigermaßen sinnvoll (um)schreibt oder mit Ihnen chattet, können Sie davon ausgehen, dass Sie es mit einem LLM zu tun haben.

Datenschutz beachten

Wer Sprach-KIs entwickeln will, braucht möglichst viele Trainingsdaten. Um mit der Konkurrenz mitzuhalten, gestatten sich viele Hersteller in den Nutzungsbedingungen, die von Ihnen eingegebenen Texte für das weitere Training zu verwenden. Prüfen Sie die Nutzungsbedingungen also genau und vertrauen Sie einem LLM im Zweifelsfall lieber keine privaten Informationen oder Geschäftsgeheimnisse an.

Das gilt im Prinzip sogar dann, wenn Sie dem Hersteller vertrauen: Denn einmal ins Training eingeflossen, kann es passieren, dass andere Nutzer der Sprach-KI Ihre Daten durch gezielte Abfragen wieder entlocken. Das ist ein grundsätzliches Problem von LLMs: Mitunter generieren sie keinen neuen Text auf Basis ihrer immensen Trainingsdatensammlung, sondern geben einzelne Informationen oder sogar längere Abschnitte der Trainingsdaten unbeabsichtigt im Wortlaut wieder.

Ergebnisse hinterfragen

Vorsicht müssen Sie auch bei Informationen walten lassen, die aus dem System wieder herauskommen: Im Grunde versuchen KI-Sprachmodelle, Texte sprachlich möglichst plausibel zu vervollständigen, nicht faktisch möglichst korrekt. Sogenannte Halluzinationen, also falsche, mitunter aber sehr plausible Behauptungen, produzieren auch LLMs der aktuellen Generationen. Die Hersteller arbeiten daran, ihren Systemen diese Fehler auszutreiben, können sie bislang aber allenfalls reduzieren.

Wenn Sie sich solche Fehler nicht als eigene anrechnen lassen wollen, müssen Sie die KI-Antworten gründlich durch eigene Recherche prüfen. Denn mitunter bringt man zwar Sprachmodelle 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 sind KIs auch Angriffen ausgesetzt. Man forscht beispielsweise daran, ob sich die Systeme „vergiften“ lassen, indem man manipulierte Trainingsdaten einschleust, die sie in bestimmten Situationen zu unerwünschtem Verhalten verleiten.

Nicht nur erforscht, sondern immer wieder auch in der Praxis demonstriert werden Prompt Injections [1]. Dabei nutzen Angreifer aus, dass Sprach-KIs 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 die KI verschaffen, sodass sie fortan seine Anweisungen ausführt oder von ihm gewünschte Informationen ausgibt. Gerade in Kombination mit anderen Systemen erwachsen daraus enorme Risiken: Der hilfsbereite Firmen-Chatbot mutiert zum Verräter, der unauffällig die letzten E-Mails des Chefs abruft und an den Angreifer ausleitet. Der nützliche Programmierassistent fängt an, heimlich Schadcode ins Programm einzubauen. Prompt Injections können vielfältig versteckt in Daten lauern, schlimmstenfalls bekommen Sie die Attacke nicht einmal mit.

Man kann KIs nur bedingt vor solchen Unterwanderungen schützen, aber es hilft, die möglichen Folgen einzudämmen: Wenn Sie einem KI-System Zugriff auf externe, also potenziell bösartige Eingabedaten geben, sollten sie ihm nicht auch Zugriff auf schützenswerte Daten geben oder erlauben, Informationen zu versenden; eine Kombination die „Tödliches Tripel“ genannt wird (siehe ct.de/wxyz): Grundsätzlich hilft es, KI-Systeme so weit wie möglich abzuschotten, keine vollautomatischen Zugriffe auf andere Systeme zu erlauben, keine Aktionen blind abzunicken und nicht reflexhaft auf jeden Link zu klicken, den Ihnen die KI präsentiert. Inhaltlich prüfen sollten Sie die Ausgaben 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

Tödliches Tripel: *ct.de/wxyz*

Sichere Nachricht

Security-Checkliste Messenger



Bild: Jessica Nachtigall / KI / heise medien

WhatsApp, Signal, Threema, Element, Telegram oder auch der Facebook-Messenger: Die Liste populärer Messenger-Apps ist lang. „Sicher" sind sie angeblich alle, aber in Wahrheit gibt es erhebliche Unterschiede, auf die man ein Auge haben sollte.

Von Sylvester Tremmel

Verschlüsselung an!

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 immer wieder 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 wirklich aktiviert ist. Einige Apps, allen voran Telegram, nutzen E2EE nämlich nur, wenn Sie als Nutzer eine spezielle Art von Chat eröffnen (oft „geheime Unterhaltung" oder ähnlich genannt) oder sie beherrschen E2EE in manchen Arten von Chats nicht, etwa in Gruppenchats. Achten Sie also gut darauf, ob und unter welchen Umständen Ihr Messenger ordentlich verschlüsselt!

Eine Ausnahme von der Regel stellen übrigens „Kanäle" dar, wie es sie seit Langem bei Telegram und 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?

Der sicherste Messenger nützt nichts, wenn man versehentlich den falschen Leuten schreibt. Prüfen Sie also immer – am besten, indem Sie Sicherheitscodes abgleichen –, dass sich hinter dem Kontakt der gewünschte Gesprächspartner verbirgt.

Außerdem bieten viele Messenger Web- oder Desktop-Clients zusätzlich zur App. Einmal auf dem Rechner eingerichtet lassen sich damit 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 Apps erlauben auch, Nachrichten nach einer einstellbaren Zeit automatisch zu löschen. „Selbstzerstörende", „selbstlöschende" oder „verschwindende" Nachrichten nennen die Messenger das. Vorsicht: Das Feature kann nicht zuverlässig verhindern, dass der Gesprächspartner die Nachricht dauerhaft speichert. Aber es eignet sich gut, um Chatverläufe kurz und Backups klein zu halten.

Account sichern

Viele Messenger binden Benutzerkonten 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 meist per SMS bestätigt, was sich manipulieren lässt. Schlimmstenfalls können Dritte dadurch Konten übernehmen. Viele 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.

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, scheitert er entweder, weil Sie noch ein Konto mit der Nummer halten, oder er hat Erfolg – und sperrt Sie unbeabsichtigt aus Ihrem Account aus. *(syt@ct.de)* c't

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



Bild: Jessica Nachtigall / KI / heise medien

Browser zählen zu den meistgenutzten Programmen überhaupt – und stehen deshalb im Fokus von Cyberkriminellen. Halten Sie Ihren Browser deshalb stets aktuell und konfigurieren Sie ihn möglichst sicher.

Von Jo Bager

Aktuell halten

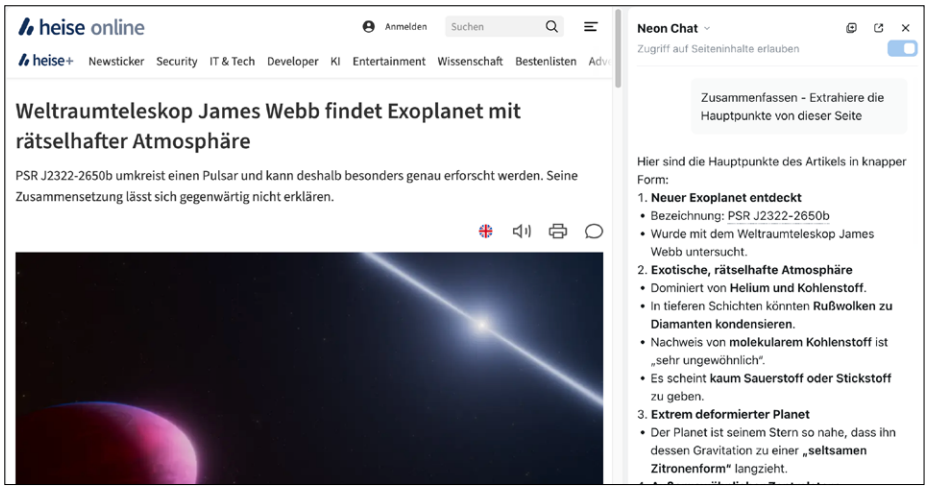
Ein aktueller Browser ist die Grundlage für sicheres Surfen. Zwar bieten alle verbreiteten Browser eine automatische Aktualisierung an, doch manchmal stockt der Update-Prozess oder der Browser muss für die Installation neu gestartet werden. Kontrollieren Sie daher regelmäßig im Menü, ob ein Neustart ansteht. Die entsprechende Funktion versteckt sich meist im Hilfe-Bereich unter „Über <Browsername>“ oder „Nach Updates suchen“.

Add-ons aufräumen

Erweiterungen können sämtliche Aktivitäten im Browser mitlesen. Überlegen Sie daher vor jeder Installation genau, ob Sie einer Erweiterung vertrauen. Laden Sie Add-ons ausschließlich aus den offiziellen Stores der Browserhersteller. Im Zweifel verzichten Sie besser auf die Erweiterung. Überprüfen Sie außerdem regelmäßig Ihre installierten Add-ons und entfernen Sie überflüssige. In Chrome und Edge erreichen Sie die Erweiterungen über das Hauptmenü, in Firefox über „Add-ons und Themes“. Selten genutzte Add-ons sollten Sie deaktivieren und nur bei Bedarf temporär einschalten.

Schnüffler blocken

Tracker verfolgen Ihr Surfverhalten und erstellen Profile über Ihre Interessen – blockieren Sie sie. Browser wie Firefox, Vivaldi und Brave bringen einen Tracking-Schutz bereits mit, den Sie nur in den Einstellungen aktivieren müssen. Alternativ helfen Add-ons wie Privacy Badger oder uBlock Origin (siehe ct.de/ys8g).



KI-Funktionen wie hier in Opera Neon können sehr nützlich sein. Man muss sich allerdings bewusst sein, dass sie mitunter Daten an externe Anbieter übermitteln.

Vorsicht ist bei den derzeit allgegenwärtigen KI-Funktionen geboten: Sie können dazu führen, dass der Browser Daten an externe Anbieter übermittelt. Achten Sie genau darauf, in welchem Zusammenhang Sie diese Funktionen einsetzen und welche Informationen dabei abfließen.

Berechtigungen prüfen

Websites fordern mitunter Zugriffsrechte auf Kamera, Mikrofon oder Standort an: Ein Videochat braucht Kamera und Mikrofon, Google Maps benötigt Ihren Standort zur Positionsbestimmung. Gewähren Sie solche Berechtigungen nur, wenn es einen nachvollziehbaren Grund gibt und Sie dem Anbieter vertrauen. Überprüfen Sie regelmäßig die bereits erteilten Freigaben und entziehen Sie überflüssige.

Auf Adressen achten

Geben Sie sensible Daten wie Passwörter oder Zahlungsinformationen ausschließlich auf verschlüsselten Websites ein. Solche Seiten erkennen Sie am Präfix https:// und am Schloss-Symbol neben der Adresszeile. Prüfen Sie URLs sorgfältig auf Auffälligkeiten: Schon ein vertauschter Buchstabe oder ein ungewöhnliches Sonderzeichen kann Sie statt zur echten Bank auf eine täuschend echte Phishing-Seite führen. Rufen Sie sicherheitskritische Websites niemals über Links aus E-Mails auf – nutzen Sie stattdessen Lesezeichen oder tippen Sie die Adresse manuell ein.

(jo@ct.de) c't

Tracking-Blocker für Chrome und andere: ct.de/ys8g

Abzockschutz

Security-Checkliste gegen Online-Betrug



Bild: Jessica Nachtigall / KI / heise medien

Online-Betrüger sind sehr erfinderisch: Sie nehmen per Anruf, SMS, WhatsApp, Mail und vielem mehr Kontakt mit ihren zukünftigen Opfern auf und versuchen sie trickreich über den Tisch zu ziehen. Mit diesen Tipps sind Sie den Ganoven einen Schritt voraus.

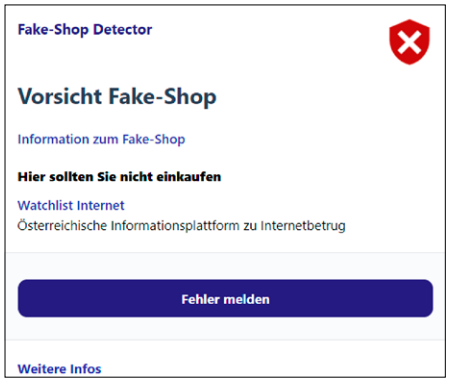
Von Ronald Eikenberg

Cool bleiben

Der erste Tipp ist zugleich der wichtigste: Bleiben Sie gelassen; Hektik hilft Ihnen nicht weiter. Egal wie sehr Betrüger Sie unter Druck setzen, legen Sie eine gesunde Portion Skepsis an den Tag und geben Sie niemals persönliche Daten, Passwörter oder Transaktionscodes heraus.

Anrufer können mit gefälschten Anruferkennungen arbeiten. Wenn Sie Zweifel an der Identität des Anrufers haben, fragen Sie nach Name, Firma und Rückrufnummer und beenden Sie das Gespräch. Anschließend können Sie die Daten in Ruhe überprüfen und entweder zurückrufen oder, wenn es sich um einen Betrugsversuch handelt, Anzeige erstatten.

Auch bei SMS, WhatsApp, Facebook, Instagram, Mail und so weiter müssen Sie vorsichtig sein. Aktuell häufen sich zudem Quishing-Angriffe: Dabei führen gefälschte QR-Codes etwa an Parkautomaten oder in Bankbriefen auf Phishing-Seiten.



Der kostenlose Fake-Shop Detector warnt Sie vor betrügerischen Online-Läden, bevor Sie dort einkaufen.

Mitunter verwenden Online-Ganoven auch Identitäten Ihrer Freunde, Verwandten oder Kollegen, um Sie zu kontaktieren. Falls Sie etwas Auffälliges beobachten, etwa unerwartete Forderungen nach Geld, sollten Sie die Ihnen bekannte Person auf einem anderen Kanal kontaktieren und fragen, ob sie tatsächlich dahintersteckt; am besten persönlich oder über eine Ihnen bekannte Telefonnummer.

Notfallkontakte

Ein wirksames Mittel gegen Online-Betrügereien sind Notfallkontakte: Das sind Personen aus dem Familien- oder Freundeskreis, die man ansprechen kann, wenn einem etwas komisch vorkommt, idealerweise, bevor man auf eine Fake SMS oder Phishing-Mail hereinfällt. Im besten Fall hat man entweder so einen Kontakt griffbereit oder ist selbst ein Notfallkontakt für sein Umfeld.

Scheuen Sie nicht, sich Hilfe zu suchen, wenn Sie sich einmal nicht sicher sind, ob Sie es mit einem Betrüger zu tun haben. Sollte Ihr Bankkonto gehackt worden sein, können Sie es über die bundeseinheitliche Notrufnummer **116 116** oder über Ihre Bank sperren lassen.

Anrufe, Mails, Links filtern

Verwenden Sie nach Möglichkeit Filterfunktionen, die Ihnen verdächtige SMS, Anrufe, Mails, Websites und vieles mehr vom Leib halten. Viele Smartphones können die lästigen Anrufe und SMS der Cyber-Ganoven erkennen und blockieren. Schauen Sie in den Einstellungen Ihrer Telefon- und SMS-App nach einer passenden Option.

Android-Nutzer können die Schutzleistung durch die Google-Apps „Telefon“ und „Messages“ aus dem Play-Store verbessern, für iOS gibt es Filter-Apps im App Store. iOS 26 bringt „Call Screening“ mit: Bei unbekannten Nummern fragt eine Siri-Stimme nach Name und Anliegen. Sie können dann entscheiden, ob Sie den Anruf annehmen.

Mails filtert in aller Regel Ihr Mailanbieter für Sie, vor gefährlichen Websites warnt Sie Ihr Browser (Safe Browsing). Schauen Sie auch hier in die Einstellungen, um den Schutz zu überprüfen und zu verbessern.

Shopping-Fallen meiden

Im Netz wimmelt es nur so von Fake Shops, aber auch auf den großen Verkaufsplattformen sind viele Betrüger unterwegs. Bevor Sie in einem neuen Online-Laden einkaufen, sollten Sie stets im Netz recherchieren, ob er vertrauenswürdig ist. Finden Sie nichts über den Shop oder hauptsächlich negative Berichte, halten Sie Abstand. Bei der Einschätzung helfen der Fake-Shop-Finder der Verbraucherzentralen und die Browser-Erweiterung Fake-Shop Detector (siehe ct.de/yrtw).

Auf den großen Shoppingportalen sollten Sie stets die Bewertungen des Verkäufers kontrollieren und sich immer an die offiziellen Bezahlwege halten, etwa PayPal mit Käuferschutz. Nutzen Sie nicht „Geld an Freunde senden“, weil Sie damit auf dem Schaden sitzen bleiben, falls Sie über den Tisch gezogen werden. *(rei@ct.de)* c't

Schutz vor Fake Shops: ct.de/yrtw

Soziale Sicherheit

Security-Checkliste Social Media



Bild: Jessica Nachtigall / KI / heise medien

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. Verwenden Sie unbedingt für jeden Account ein eigenes, komplexes Passwort. Außerdem sollten Sie, wo immer möglich, private und dienstliche Nutzung voneinander trennen, also nicht über dieselben Konten laufen lassen.

Nutzen Sie zudem alle weiteren Möglichkeiten zur Absicherung, welche die Plattformen bieten. Was in einigen anderen Checklisten bereits erwähnt ist (siehe S. 17), gilt in besonderem Maße für soziale Plattformen: Sie sollten, wo immer möglich, zusätzliche Zugangsbarrieren außer 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“ zum Meta-Account. Dort führt der Menüpunkt „Privacy Center“ über „Häufig genutzte Privatsphäre-Einstellungen“ zur „zweistufigen Authentifizierung“. 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, Threads, Bluesky, 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 die Geräte bleiben angemeldet – egal ob PC oder Smartphone. 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 etwa 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.

Gezielt teilen

Digitale Inhalte sind schnell kopiert und weiterverteilt. Das kann Ihnen auch mit Onlinefreunden passieren, die Sie gut kennen. Es muss nicht einmal böser Wille dahinterstehen. Daher ist eine gute Richtschnur, digital nur Inhalte zu veröffentlichen, die Sie auch Fremden auf der Straße zeigen würden.

Bei Facebook, aber auch bei anderen Anbietern wie LinkedIn kann man festlegen, mit wem man Inhalte teilen möchte. Behalten Sie Ihre Zielgruppenvoreinstellung 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 Privatsphäreneinstellungen unter „Deine Aktivität“ ändern.

Anfragen checken

Freundschaft und Vertrauen sind auch auf Facebook, Instagram, LinkedIn oder TikTok begehrte Statussymbole. 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 und ohne weitere Prüfung Ihre persönliche oder dienstliche 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



Bild: Jessica Nachtigall / KI / heise medien

Bankkonten und Kreditkarten versprechen fette Beute. Logisch, dass Cyberkriminelle scharf auf deren Daten und Passwörter sind. Absolute Sicherheit gibt es nicht, aber Sie können es den Tätern ziemlich schwer machen.

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 immer ab, wenn er nicht zu passen scheint. Bei Online-Überweisungen und Kartenzahlungen 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 und Bezahlen auf dem PC oder Smartphone muss das System frei von Schadsoftware sein. Sorgen Sie speziell auf einem Windows-PC dafür, dass ein Virenscanner mit aktuellen Updates läuft. Der bei Windows mitgelieferte Defender bietet hinreichenden Schutz, siehe Artikel „Security-Checkliste Windows“. 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. Diese stammen vorgeblich von Ihrer Bank, einer offiziellen Stelle wie der Polizei oder anderen Institutionen. Manche davon enthalten schädliche Anhänge oder Links. Darüber schleusen die Täter Schadcode ein oder greifen Zugangsdaten ab (Phishing). Die meisten solchen Mails sollen Sie aber dazu bewegen, in Eingabemasken auf Fake-Webseiten Ihre Onlinebanking-Zugangsdaten oder Kreditkartendaten preiszugeben.

Schöpfen Sie Verdacht, wenn eine persönliche Anrede fehlt, Rechtschreibfehler enthalten sind oder jemand Angst oder Zeitdruck erzeugt. Klicken Sie in Mails, die eine Bank als Absender enthalten, prinzipiell nicht auf Links. Mails oder Textnachrichten, denen zufolge Sie Ihr Konto mit PIN und TAN oder App-Freigabe „bestätigen“ sollen, sind immer Betrugsversuche. Öffnen Sie Anhänge niemals, denn eine Bank schickt Ihnen wichtige Dokumente postalisch zu oder stellt sie in Ihrem Onlinebanking-Postfach bereit.

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. Das gilt ebenso für zugelassene Drittdienste, die zum Beispiel im Auftrag Ihres Geschäftspartners über das Konto Ihre Identität verifizieren. Solche Dienste verzeichnet die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) auf ihrer Homepage (siehe ct.de/y5vr).

Mitunter rufen Betrüger auch mit gefälschten Absender-Rufnummern an und geben sich beispielsweise als Bankberater oder Polizist aus. Eine Masche besteht darin, Sie vor einer angeblichen Gefahr zu warnen, um Sie zu unüberlegten Handlungen zu manipulieren. Beenden Sie das Gespräch und rufen Sie die Bank über die Telefonnummer in Ihren Unterlagen zurück.

Belege überprüfen

Kontrollieren Sie jede Kreditkartenabrechnung und reklamieren Sie unbefugte Abbuchungen umgehend bei Ihrer Bank. 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 Sie sich außerdem per Mail, SMS oder Push-Nachricht über neue Transaktionen oder Ereignisse wie das Unterschreiten eines bestimmten Kontostands benachrichtigen lassen.

Handy nicht rooten

Banking auf Smartphones ist sicher. Rooten oder jailbreaken Sie Ihr Smartphone oder Tablet aber nicht, mit dem Sie Onlinebanking betreiben. Geben Sie Apps auch keine solchen Rechte. Andernfalls legen Sie wichtige Schutzfunktionen lahm. Das ist besonders dann gefährlich, wenn Sie beim Smartphone-Banking den zweiten Faktor auf dem gleichen Gerät haben – auch wenn viele Apps von Banken unter modifiziertem Android oder iOS gar nicht mehr starten.

Generell ist es empfehlenswert, ein ungerootetes Smartphone mit einem Betriebssystem zu verwenden, das noch Sicherheitsupdates bekommt. Mindestens aber müssen Sie den Vorgaben Ihrer Bank folgen: Solange Sie ein Betriebssystem nutzen, das die App Ihrer Bank offiziell noch unterstützt, kommen Sie Ihren Sorgfaltspflichten an dieser Stelle nach.

(mon@ct.de) c't

BaFin-Datenbank: ct.de/y5vr

Backup! Jetzt!

Security-Checkliste Datensicherung

Üblicherweise vermeiden wir den inflationären Einsatz von Ausrufezeichen, doch der Aufruf zum Backup kann gar nicht laut genug sein. Sonst ist die Frage nicht, ob Sie Datenverlust erleiden, sondern nur wann.



Bild: Jessica Nachtigall / KI / heise medien

Von Axel Vahldiek

Jetzt!

Es ist furchtbar trivial und vermutlich jedem völlig klar, trotzdem sei darauf hingewiesen: Ein Backup kann im Ernstfall nur dann helfen, wenn es wirklich vorhanden ist. Zudem sollte es möglichst aktuell sein, was nach ständiger Wiederholung schreit. Es gibt daher eine simple Antwort auf die Frage, wann der richtige Zeitpunkt fürs nächste Backup ist, denn es ist immer der gleiche: jetzt! Denn Sie denken ohnehin gerade übers Backup nach, also los!

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. Für Laien oft einfacher ist aber das Ausdrucken auf Papier. Diese Art von Backup ist sogar langlebig: Eine 60 Jahre alte Fotografie mag vergilbt aussehen, das Motiv ist aber immer noch erkennbar. Zum Vergleich: Versuchen Sie doch 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 überallhin. Kurzum: Das Backup muss raus aus dem Haus. Lagern Sie beispielsweise eines Ihrer Backupmedien bei Verwandten. Leicht merken lässt sich das als 3-2-1-Regel: 3 Kopien auf 2 Datenträgern, davon 1 außer Haus. Eine simple Form der Umsetzung ist beispielsweise, eine Kopie Ihrer Dateien auf der lokalen Festplatte und zwei weitere auf zwei externen Laufwerken wie USB-Sticks oder -Platten zu speichern, von denen Sie eines bei Verwandten, Freunden oder am Arbeitsplatz beziehungsweise daheim parken.

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, das nach dem Sichern abgestöpselt wird, ist technisch getrennt – doch Obacht: Wenn Sie es für die nächste Sicherung wieder anstöpseln, ist es eben nicht mehr getrennt. Dagegen hilft nur, mehrere Sicherungsmedien im Wechsel 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; achten Sie beim Kauf auf das Kürzel DIS. Alternativ hilft das Verschlüsseln des Backups – dann bekommt der Dieb mangels Schlüssel nur Datenmüll zu sehen.

Wichtig: Probieren Sie unbedingt aus, ob Sie das Backup im Ernstfall entschlüsseln können.

Testen

Erst wenn Sie Ihr Backup testweise wiederhergestellt haben, gilt es als zuverlässig. 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. *(axv@ct.de)* c't

Schotten dicht

Security-Checkliste Server & Hosting



Bild: Jessica Nachtigall / KI / heise medien

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 öffentlich bekannt, weil die Zertifizierungsstellen Certificate Transparency herstellen [1]. Durchsuchbar ist die Liste aller ausgestellten Zertifikate zum Beispiel über die Website 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. 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 IDs 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. 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". Wenn Sie mitbekommen wollen, von welchen IP-Adressen potenzielle Angriffe kommen, können Sie ein Werkzeug wie fail2ban einrichten.

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 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 nach, ob die Funktion in Planung ist, oder suchen Sie sich einen neuen Hoster mit einem zeitgemäßen Angebot.

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 öffentlich!

Die Portweiterleitung 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. Die sichere Alternative zur Portweiterleitung ist ein VPN-Tunnel.

(jam@ct.de) c't

Werkzeuge: ct.de/y7z8

IoT, aber sicher

Security-Checkliste: Smart Home



Bild: Jessica Nachtigall / KI / heise medien

Heute steckt in fast jedem Haushaltsgerät ein kleiner Computer, der meist den Anschluss ans Internet anstrebt – oft lassen sich die sogar ohne gar nicht erst in Betrieb nehmen. Ein paar Kniffe helfen, dass solche Geräte nicht zu viel Eigenleben entwickeln können.

Von Peter Siering

Angriffspunkte minimieren

Gehen Sie davon aus, dass potenzielle Angreifer es auf das schwächste Gerät aus Ihrem Smart-Home-Zoo abgesehen haben. Beispielsweise physisch im Außenbereich montierte und zugängliche WLAN-Kameras bilden ein leicht zugängliches Ziel, um das Passwort Ihres WLANs auszulesen. Ein übers Internet erreichbares Aufzeichnungsgerät der Kameras, dessen Linux seit einem Jahrzehnt ungepatcht und veraltet ist, kommt einer Einladung gleich. Hinterfragen Sie, ob Geschirrspüler oder Herd wirklich ins WLAN müssen: Oft ist der Komfortgewinn so klein, dass er die Mehrausgaben für den Standby-Strom nicht rechtfertigt. Prüfen Sie bei Bluetooth-fähigen Geräten, ob sie neue Verbindungen akzeptieren; gelingen die ohne Bestätigung auf dem Gerät, schalten Sie Bluetooth ab. Sorgen Sie dafür, dass Geräte nicht physisch zugänglich sind. Widerstehen Sie der Versuchung, Geräte direkt per Portweiterleitung übers Internet erreichbar zu machen. Nutzen Sie eine VPN-Verbindung in das Netz mit den IoT-Geräten, sodass Dritte die Dienste nicht direkt erreichen können.

Geräte isolieren

Wenn Sie das WLAN selbst nicht schützen können, aktivieren Sie die Isolation der einzelnen Geräte, sodass diese nicht direkt miteinander kommunizieren können, sondern nur mit dem Router. So stellen Sie sicher, dass potenzielle Angreifer sich nicht von Gerät zu Gerät hangeln können. Behalten Sie im Hinterkopf, dass Geräte, die sowohl über eine Mobilfunkanbindung als auch WLAN-Zugang verfügen, etwa Wallboxen, Angreifern als Brücke in Ihr Netzwerk dienen könnten. Entscheiden Sie sich für eine Zugangstechnik. Schaffen Sie ein eigenes Netzwerk für IoT-Geräte oder nutzen Sie wenigstens ein vorhandenes Gastnetzwerk.

Ausgangssperre verhängen

Verbieten Sie den Geräten, direkt mit dem Internet zu kommunizieren. Begrenzen Sie die Gegenstellen, mit denen diese Kontakt aufnehmen können. Wenn sich ein Gerät nur per Clouddienst konfigurieren lässt, erteilen Sie ihm nur vorübergehend die Erlaubnis, direkt mit dem Internet zu sprechen. Konfigurieren Sie das Gerät idealerweise so, dass es ausschließlich mit von Ihnen kontrollierten Diensten spricht, und nur über Ihre Smart-Home-Zentrale gesteuert werden kann. Nutzen Sie dafür einen eigenen vermittelnden MQTT-Server und nicht solche fremder Betreiber.

Freie Firmware

Verwenden Sie statt der Hersteller-Firmware lieber Open-Source-Alternativen. Die sind zwar nicht unbedingt sicherer, aber in der Regel beäugen mehr Personen den Quelltext kritisch, als das bei Closed-Source-Entwicklungen der Fall ist. Oft verteilt sich die Last der Entwicklung auch über mehrere Schultern, sodass Ihre Geräte unabhängig von gewinn- oder datenabschöpfenden Eskapaden eines Investors sind. Viele Geräte gerade aus Fernost kommen zwischenzeitlich sogar mit Open-Source-Firmware wie Tasmota aus der Fabrik.

Individuelle Passwörter

Wenn Sie Konfigurationsdaten auf den Geräten hinterlegen müssen, um sie etwa mit einem MQTT-Server oder Clouddiensten sprechen zu lassen, halten Sie sich dabei an die üblichen Empfehlungen für sichere Kennwörter. Verwenden Sie individuelle Zugangsdaten und keine Rudelaccounts, sodass diese etwa in einer Smart-Home-Zentrale oder auf einem MQTT-Server nur die für das Gerät relevanten Informationen manipulieren dürfen. Auf die Weise erhält ein Angreifer nicht gleich Vollzugriff. Wenn es nicht ohne Cloud geht: Verwenden Sie separate Accounts, die keine Rückschlüsse auf Ihre Person oder Ihre Adresse zulassen.

Updates dosieren

Die aus Sicherheitssicht nahezu immer richtige Empfehlung, stets alle erhältlichen Updates zu installieren, gilt im Smart Home nur für Gerätschaften, die von außen erreichbar sind, zum Beispiel ein MQTT-Server oder ein Aufzeichnungsgerät für Kameras. Geräte, die nur intern, in einem separaten Netz erreichbar sind, sollte man dosierter zu Werke gehen lassen. Oft nämlich ändert sich durch das Einspielen einer neuen Firmware auf Kleingeräten wie WLAN-Steckdosen deren Verhalten – möglich, dass sie nach einem Update nicht mehr von der Smart-Home-Zentrale gefunden werden oder unerwartete Antworten geben. Einen separaten Kanal, der ausschließlich Sicherheitsupdates bereitstellt, gibt es für solche Geräte meist nicht. Im Zweifel testet man Updates zuerst auf einem Gerät und beglückt den ganzen Zoo erst nach einer Karenzzeit. *(ps@ct.de)* c't

Passwort: sicher

Security-Checkliste Passwörter



Bild: Jessica Nachtigall / KI / heise medien

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

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 für Dienste, 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 Datenleck.

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.

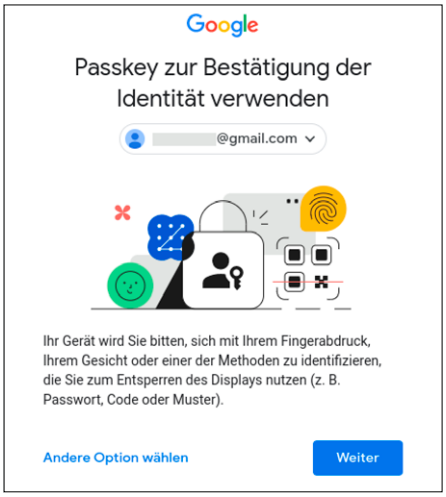
Passwortmanager

Nehmen Sie einen Passwortmanager wie KeePassXC 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 [1]. Der Passwortmanager Ihres Betriebssystems oder Browsers ist im Zweifel besser als gar keiner.

Darknet-Leaks checken

Cyber-Ganoven erbeuten immer wieder und im großen Stil Datenbanken mit Zugangsdaten. Überprüfen Sie von Zeit zu Zeit in öffentlichen Verzeichnissen, 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/yg8d).

Gibt es einen Treffer, ist das betroffene Passwort kompromittiert; ändern Sie es bei allen Diensten, bei denen Sie es verwenden. Rechnen Sie außerdem mit einem Anstieg an Phishingmails an die zugehörige Mailadresse, die sich möglicherweise sogar auf den gehackten Dienst beziehen.



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

Zwei Faktoren nutzen

Viele Onlinedienste bieten eine 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 unsichere SMS-Verfahren. Nutzen Sie besser „Time-based One-time Password“ (TOTP), bei dem Sie die Codes selbst mit einer App wie Google Authenticator oder Authenticator Pro generieren.

Am sichersten ist FIDO2, das einige Webdienste bereits als Anmeldemethode anbieten. Die Eingabe eines Passworts oder 2FA-Codes ist damit nicht mehr nötig, Sie verwenden stattdessen einen sogenannten Passkey [3], der zum Beispiel auf Ihrem Smartphone gespeichert ist. Nutzen Sie diese Möglichkeit, wenn sie angeboten wird. Das klappt unter anderem bereits bei Google, Microsoft, Amazon und PayPal. *(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

Darknet-Leaks checken: ***ct.de/yg8d***

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

Titelthemenkoordination in dieser Ausgabe: „Glasfaser ohne Stolperfallen“: Christian Wölbert *(cwo@ct.de)*, „c't-Security-Checklisten 2026“: Wilhelm Drehling *(wid@ct.de)*
Chefredakteure: Torsten Beeck *(tbe@ct.de)* (verantwortlich für den Textteil), Dr. Volker Zota *(vza@heise.de)*
Stellv. Chefredakteure: Martin Fischer *(mfi@heise.de)*, Axel Kossel *(ad@ct.de)*, Jan Mahn *(jam@ct.de)*
Chefin vom Dienst New Media: Hannah Monderkamp *(mond@heise.de)*
Chefin vom Dienst c't Magazine & Qualität: Angela Meyer *(anm@ct.de)*
Magazin & Qualität: Pia Groß *(piae@ct.de)*, Oliver Lau *(ola@ct.de)*, Michael Link *(mil@ct.de)*, Hajo Schulz *(hos@ct.de)*
Koordination Heftproduktion & 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: Robin Ahrens *(rah@ct.de)*, 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)*, Dr. Sabrina Patsch *(spa@ct.de)*, Peter Schmitz *(psz@ct.de)*, Andrea Trinkwalder *(atr@ct.de)*, Stefan Wischner *(swi@ct.de)*, Tom Leon Zacharek *(tlz@ct.de)*
Ressort Systeme & Sicherheit
Leitende Redakteure: Peter Siering *(ps@ct.de)*, Sylvester Tremmel *(syt@ct.de)*
Redaktion: Georgiy Belashov *(geb@ct.de)*, 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)*, Dennis Schirrmacher *(des@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)*
Redaktion: Ernst Ahlers *(ea@ct.de)*, Christian Hirsch *(chh@ct.de)*, Ansgar Kossowski *(aki@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)*, Christian Wölbert *(cwo@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)*, Urs Mansmann *(uma@ct.de)*, Stefan Porteck *(spo@ct.de)*
Leiter c't 3003: Jan-Keno Janssen *(jkj@ct.de)*
Redaktion c't 3003: Lukas Rumpler *(rum@ct.de)*, Sahin Erengil-Schulz *(sahe@heise.de)*, Pascal Schewe *(pas@heise.de)*
c't Sonderhefte
Leitung: Jobst Kehrhahn *(keh@ct.de)*
Koordination: Pia Groß *(piae@ct.de)*
c't online: Sylvester Tremmel *(syt@ct.de)*, Niklas Dierking *(ndi@ct.de)*
Social Media: Jil Martha Baae *(jmb@ct.de)*
Koordination News-Teil: Hartmut Gieselmann *(hag@ct.de)*, Kathrin Stoll *(kst@ct.de)*, Christian Wölbert *(cwo@ct.de)*
Redaktionsassistenz: Susanne Cölle *(suc@ct.de)*, Tim Rittmeier *(tir@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)*, 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, Georg Schnurer *(gs@ct.de)*, Ben Schwan *(bsc@ct.de)*, Christiane Schulzki-Haddouti
DTP, Layout und Grafik: Mike Bunjes, Leia Marie Göbser, Birgit Graff, Angela Hilberg, Jessica Nachtigall, Astrid Seifert, Ulrike Weis
Junior Art Director: Martina Bruns
Fotografie: Melissa Ramson, Andreas Wodrich
Digitale Produktion: Melanie Becker, Martin Kreft, Thomas Kaltschmidt, Pascal Wissner
Illustrationen: Rudolf A. Blaha, Frankfurt am Main, Thorsten Hübner, Berlin, Albert Hulm, Berlin, Sven Hauth, Schülp, 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: 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. 42 vom 1. Januar 2025.
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: Mohn Media Mohndruck GmbH, Carl-Bertelsmann-Straße 161M, 33311 Gütersloh
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 6,50 €; Österreich 7,20 €; Schweiz 10.80 CHF; Belgien, Luxemburg 7,70 €; Niederlande 7,90 €; Italien, Spanien 8,20 €
Abonnement-Preise: Das Jahresabonnement kostet inkl. Versandkosten: Inland 161,20 € (Digital 153,40 €), Österreich 170,30 €, Europa 185,90 €, restl. Ausland 214,50 € (Schweiz 260.00 CHF); ermäßigtes Abonnement für Schüler, Studenten, Auszubildende (nur gegen Vorlage einer entsprechenden Bescheinigung): Inland 110,50 €, Österreich 122,20 €, Europa 124,80 €, restl. Ausland 153,40 € (Schweiz 154.70 CHF). c't-Plus-Abonnements (inkl. Zugriff auf das c't-Artikel-Archiv sowie die App für Android und iOS) kosten pro Jahr 24,70 € (Schweiz 29.90 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 120,90 €, Österreich 128,70 €, Europa 140,40 €, restl. Ausland 161,20 € (Schweiz 195.00 CHF). Luftpost auf Anfrage.
Leserservice:
Bestellungen, Adressänderungen, Lieferprobleme usw.
Heise Medien GmbH & Co. KG
Leserservice
Postfach 110 242
69071 Heidelberg
E-Mail: leserservice@heise.de
Telefon: 0511/647 22 888
c't abonnieren: Online-Bestellung via Internet (www.ct.de/abo) oder E-Mail *(leserservice@heise.de)*.

Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion vom Herausgeber nicht übernommen werden. Kein Teil dieser Publikation darf ohne ausdrückliche schriftliche Genehmigung des Verlags in irgendeiner Form reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden. Die Nutzung der Programme, Schaltpläne und gedruckten Schaltungen ist nur zum Zweck der Fortbildung und zum persönlichen Gebrauch des Lesers gestattet.
Für unverlangt eingesandte Manuskripte kann keine Haftung übernommen werden. Mit Übergabe der Manuskripte und Bilder an die Redaktion erteilt der Verfasser dem Verlag das Exklusivrecht zur Veröffentlichung. Honorierte Arbeiten gehen in das Verfügungsrecht des Verlages über. Sämtliche Veröffentlichungen in c't erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes.
Warennamen werden ohne Gewährleistung einer freien Verwendung benutzt. Hergestellt und produziert mit Xpublisher: www.xpublisher.com. Printed in Germany. Alle Rechte vorbehalten. Gedruckt auf chlorfreiem Papier.
© Copyright 2026 by Heise Medien GmbH & Co. KG
ISSN 0724-8679 AWA LAE