Eine Extraportion Sicherheit

Die c’t-Security-Checklisten 2025

Bild: KI, Collage c’t

IT-Sicherheit muss nicht kompliziert sein: Mit unseren sorgfältig ausgesuchten Tipps & Tricks sichern Sie Smartphone, Router, Computer und vieles mehr ab. Die Sicherheitsmaßnahmen nehmen nur wenige Minuten in Anspruch und sind einfach durchzuführen.

Von Wilhelm Drehling

Das Verbrechen schläft nicht, vor allem im Internet. Die Angriffe von Online-Betrügern laufen heutzutage nicht selten vollautomatisiert ab. Bots interessiert es nicht, ob sie ein gigantisches Unternehmen angreifen oder Privatpersonen, die versäumt haben, ihre Zugänge mit einem zweiten Faktor abzusichern. „Es wird mich schon nicht treffen" ist hierbei eine ganz schlechte Ausrede. Mit unseren Checklisten brauchen Sie die nicht, denn unsere Tipps setzen Sie im Handumdrehen um und sind auf der sicheren Seite. Verlieren Sie also keine Zeit und fangen Sie am besten gleich an.

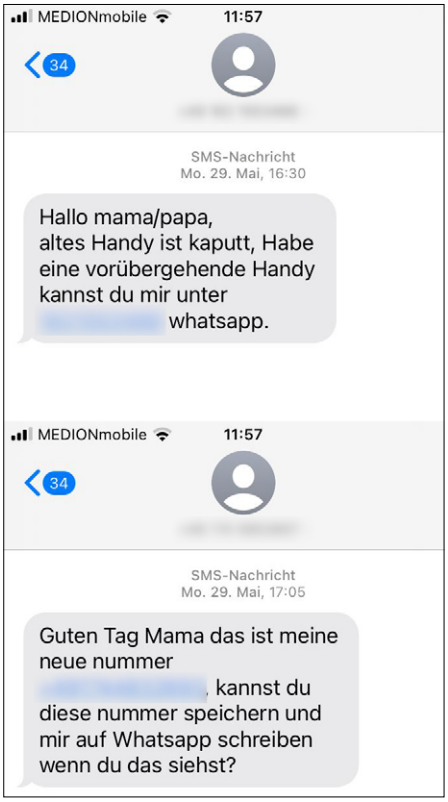
Neu: Schutz vor Online-Betrug

Da die Anzahl der Geräte, Apps und Konten immer größer wird, gibt es einen Haufen von Einfallstoren, die böswillige Dritte ausnutzen können. Deshalb haben wir wie schon die letzten Jahre unsere Security-Checklisten aktualisiert und auf die aktuelle Bedrohungslage angepasst. Darum finden Sie auf Seite 11 eine völlig neue Checkliste, die sich mit dem Schutz vor Online-Betrug auseinandersetzt.

Betrüger denken sich stetig neue Maschen aus und üben nicht selten viel Druck aus, um Ihnen Geld abzuknöpfen. Dabei ist kein Kanal geschützt: SMS (siehe Bild), Mail, Social Media oder Messenger-Apps wie WhatsApp & Co. Bleiben Sie daher bei unbekannten Kontakten immer skeptisch und kontaktieren Sie über sichere Drittkanäle Verwandte, wenn sich jemand als sie ausgibt. Mehr Tipps dazu lesen Sie in den Checklisten Social Media (S. 12), Messenger (S. 9), Browser (S. 10) und E-Mail (S. 7).

Frisch aktualisiert

Die restlichen Checklisten dürften Sie als erfahrener c't-Leser vermutlich kennen, trotzdem empfehlen wir Ihnen die Lektüre, um auch wirklich alle Einfallstore zu schließen, denn auch dort gibt es Neuerungen. Damit Sie sich gut zurechtfinden, haben wir die Checklisten chronologisch aufgebaut, angefangen mit Tipps & Tricks rund um den digitalen Arbeitsplatz (S. 3), gefolgt von Windows (S. 4), Smartphone (S. 5) und WLAN-Router (S. 6).



Seien Sie auf der Hut bei Nachrichten, die zum Kontakt mit anderen Nummern auffordern. Betrüger versuchen nicht selten, Ihre Skepsis über die emotionale Schiene auszutricksen. Kontaktieren Sie daher zur Sicherheit über Zweitkanäle Familie und Verwandte, um die Herkunft der SMS zu bestätigen.

Als Nächstes erwartet Sie eine Liste zum Umgang mit KI-Sprachmodellen wie ChatGPT (S. 8), die ebenfalls kürzlich erst dazugekommen ist. Bei all dem Hype darf man nicht vergessen, was für hungrige Datenmonster Chatmodelle sind: Viele verschlingen sämtliche Eingaben und trainieren sich damit weiter. Bleiben Sie also achtsam, welche privaten Daten Sie einer KI anvertrauen.

Ganz besonders haben es Betrüger auf Ihre Zugänge zu Banking-Konten (S. 13) abgesehen. Häufig läuft das über raffinierte Phishing-Versuche via Mail (S. 7) ab. Hierbei versuchen Angreifer das Opfer auf eine täuschend echt aussehende Webseite der Bank zu locken und beim Login-Versuch die Anmeldedaten abzugreifen. Benutzen Sie immer den zweiten Faktor und checken Sie genau, was Sie gerade freigeben. Prüfen Sie auch am besten Ihre Online-Accounts bei Google, Microsoft & Co. (S. 16), ob Sie hier einen zweiten Faktor einrichten können. Noch resistenter gegen Phishing oder Leaks sind Sie etwa mit Passkeys [1].

Sollten Sie zudem einen eigenen Server betreiben, ist die Checkliste auf Seite 15 einen Besuch wert. Stellen Sie sicher, dass der Server immer auf dem aktuellen Stand ist und verwenden Sie fürs Einloggen das sichere SSH-Verfahren mit dem Public-Key-Verfahren. Schützenswerte Daten sollten Sie zusätzlich in Form eines Backups aufbewahren (S. 14) – das gilt auch für private Urlaubsbilder oder wichtige Unterlagen wie eine Steuererklärung.

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/check2025 herunterladen und dann nach Belieben an Freunde, Familie und Bekannte verteilen. Und nun ran ans Werk! *(wid@ct.de)* c't

Literatur

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

PDF-Booklet kostenfrei herunterladen:
ct.de/check2025

Home und Office

Security-Checkliste für die Heimarbeit

Bild: KI, Collage c't

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.

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.

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 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 herzutragen.

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 abschließen

Security-Checkliste Windows

Bild: KI, Collage c't

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. Beachten Sie, dass Windows 10 nur noch bis zum 14. Oktober 2025 von Microsoft mit Sicherheitsupdates versorgt wird. 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 Artikel „Security-Checkliste Backups“, 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. 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. Ein Notebook klappen Sie einfach zu.

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 Shift + 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

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.

Bild: KI, Collage c't

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. Wer nicht auf dem Laufenden ist, macht es Hackern leichter als nötig. Apple versorgt seine iPhones vorbildlich mit Updates: iOS 18 erschien 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, Google-Pixel-Geräte werden indes mit am längsten versorgt.

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

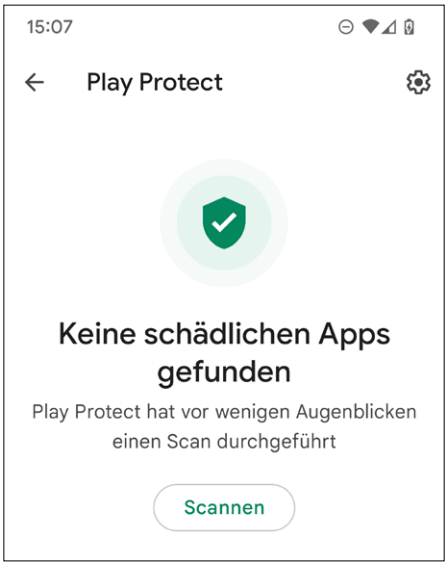
Installieren Sie Apps am besten nur aus den offiziellen Stores von Apple, Google und den Geräteherstellern. Die Apps werden zumindest bei Apple und Google einem Sicherheitscheck unterzogen. Android-Nutzer, die eine App als APK-Installationspaket installieren möchten, sollten dieses nur direkt vom Entwickler 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.

App-Berechtigungen

Überprüfen 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)* **ct**



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

Netzabsicherung

Security-Checkliste WLAN-Router

Mit Einrichtungsassistenten konfigurieren Sie WLAN-Router zwar schnell, aber Sicherheitsfunktionen wie die Verschlüsselung brauchen noch etwas Nacharbeit, selbst wenn der Router schon gemäß WPA3 verschlüsselt.

Von Dušan Živadinović

Bild: KI, Collage c't

Webinterface abdichten

Viele Router lassen sich mittels Assistenten über Browser oder Smartphone-Apps konfigurieren; diese führen aber nicht durch alle empfehlenswerten Optionen, sodass oft Lücken bleiben. Ändern Sie zunächst das ab Werk eingestellte Konfigurationspasswort des Routers. Denn da es üblicherweise auf dem Typenschild steht, können Unbefugte es ablesen oder fotografieren und dann den Router unbemerkt manipulieren.

Aktivieren Sie das automatische Firmware-Update, falls vorhanden. Dann aktualisiert sich der Router selbstständig, sodass Sie nicht ständig darauf achten müssen, erst recht nicht auf Reisen.

Richtig verschlüsseln

Für die WLAN-Verschlüsselung empfiehlt sich der Mixed-Mode WPA2+WPA3. Falls nur WPA2 vorhanden, aktivieren Sie den Schutz der Steuerpakete (PMF). Ändern Sie den Funknetznamen und das Passwort des WLANs, besonders dann, wenn diese Einstellungen ebenfalls auf dem Typenschild stehen. Standard-Zugangsdaten sind oft auch in Bedienungsanleitungen und damit per Suchmaschine zu finden.

Falls Sie wegen älterer Geräte auf WPA2 nicht verzichten können: Verwenden Sie ein Passwort von mindestens 20, besser 30 Zeichen Länge. Denn einige Knackprogramme können WPA2-Passwörter durch Probieren herausfinden (Brute-Force-Attacke). Dafür zeichnen Angreifer Ihren WLAN-Verkehr auf und führen diesen später einem leistungsfähigen PC zu. Ob er dann Ihr Passwort schnell findet oder der Angreifer der Stromvergeudung nach Tagen Einhalt gebietet, hängt von der Länge des Passworts ab.

Gastnetz nutzen

Schützen Sie Ihr Heimnetz, indem Sie Besucher, Smart-Home- und IoT-Geräte ins Gast-WLAN stecken. Und auch das Gastnetz sollte ein langes Passwort erhalten, das aber gelegentlich geändert werden sollte (Kalendereintrag ;-)), denn Besucher können es ohne Rückfrage weitergeben. Erlauben Sie im Gast-WLAN nur bestimmte Dienste, beispielsweise Surfen und Mailen, um unerwünschtes Filesharing zu unterbinden.

Wenn sich der Router aus dem Internet konfigurieren lässt, sollte er diesen Verkehr per HTTPS verschlüsseln. Falls Sie einen Server betreiben, auf den Sie von außen zugreifen wollen, richten Sie eine VPN-Verbindung ins Heimnetz ein; Portweiterleitungen funktionieren zwar ebenfalls, erfordern aber eine gute serverseitige Absicherung. Manche Router bieten für Fernzugriffe aufs Heimnetz eigene VPN-Server. Weitere Hinweise zum Absichern von Servern finden Sie im Artikel „Security-Checkliste Server & Hosting“.

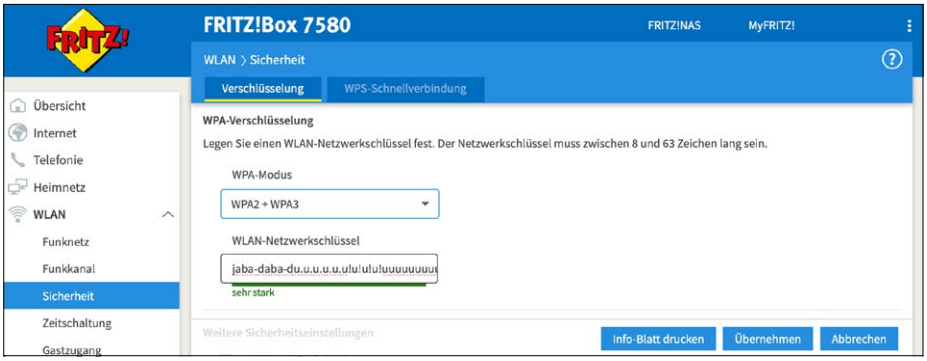
WPS nur bedarfsweise

Mittels der WPS-Funktion koppelt man WLAN-Geräte über je einen Tastendruck am Router und Client. Um Unbefugten diesen bequemen Zugang zu verwehren, schalten Sie diese Funktion nur vorübergehend bei Bedarf ein.

Manche Hersteller nutzen die UPnP-Funktion von Routern, damit sich ihre Geräte eine Portweiterleitung im Router selbst einrichten. Das spart Zeit, aber wenn UPnP aktiv ist, kann auch eingeschleppte Malware die Firewall des Routers von innen öffnen. Daher sollten Sie UPnP nur vorübergehend laufen lassen oder hilfsweise nur einzelnen Hosts gestatten.

Wenn alle Punkte abgehakt sind, exportieren Sie die 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 sich der Funkverkehr nur mit dem veralteten WPA2 verschlüsseln lässt, gilt für die Sicherheit des WLAN-Passworts: Länge ist wichtiger als irgendwelche Sonderzeichenregeln.

Löchrige Umschläge

Security-Checkliste E-Mail

Bild: KI, Collage c't

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

Viele Phishing-Mails sind schludrig gemacht und zielen auf besonders leichtgläubige Opfer, aber eben nicht alle. 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 können auch gute Fälschungen weitgehend automatisch erstellen und verschicken. Man muss also keineswegs einer gezielten Attacke ausgesetzt sein und „uns kleine Fische wird es schon nicht treffen" ist eine ganz schlechte Annahme.

Misstrauen Sie E-Mails daher grundsätzlich. Nicht nur, aber besonders dann, wenn Anhänge oder Geld im Spiel sind, die Mail scheinbar vom Chef oder der Bank kommt oder wenn sie aus anderen Gründen 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 auch 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 sehen dadurch weniger schön aus, aber externe Inhalte werden gerne für (Werbe-)Tracking genutzt und sind auch immer wieder an Sicherheitslücken beteiligt.

Am besten schalten Sie die HTML-Ansicht aus und lassen sich nur die Textansicht anzeigen. Eine Option dafür bieten viele Programme, wenn auch mitunter gut versteckt. Im verbreiteten Client Thunderbird klicken Sie beispielsweise 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. Der Komfortverlust ist dann gering; in Thunderbird rüstet das Add-on „Allow HTML Temp" (siehe ct.de/yvzx) 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 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. 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, der eine relativ einsteigerfreundliche OpenPGP-Unterstützung integriert hat (siehe ct.de/yvzx).

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 die meisten 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 Security-Checkliste Messenger), 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 das 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 haben wir unter ct.de/sicher-mailen aufgeschrieben. *(syt@ct.de)* c't

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

Reden ist Gold

Security-Checkliste KI-Sprachmodelle

Bild: KI, Collage c't

Große Sprachmodelle sind allerorten, fassen Texte zusammen, erstellen Präsentationen, beantworten Fragen 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 zum Beispiel GPT 4, 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

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 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 wieder. Die Hersteller wissen um das Problem, haben es aber nicht im Griff. Beispielsweise wies Google seine Mitarbeiter an, keinen Code oder vertrauliche Informationen mit dem eigenen KI-Chatbot zu teilen.

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. Ob solche Fehler sich je komplett ausschließen lassen, ist ungewiss, obwohl die Hersteller fleißig daran arbeiten.

Wenn Sie sich solche Fehler nicht als eigene anrechnen lassen wollen, müssen Sie die KI-Antworten gründlich durch eigene Recherche überprüfen. 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 gezielten 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 die letzten E-Mails des Chefs abruft und an den Angreifer ausleitet. Die Prompt Injection kann weiß-auf-weiß oder anderweitig versteckt in den Daten lauern und den Bot anweisen, 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. Ein wirksames Gegenmittel ist noch nicht gefunden. Es hilft, die Systeme 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 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

Verlässliche Boten

Security-Checkliste Messenger

Bild: KI, Collage c't

WhatsApp, Signal, Threema, Matrix, 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 tatsächlich zum Einsatz kommt. 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. Beispielsweise verschlüsselt der Facebook-Messenger zwar mehr und mehr Arten von Chats Ende-zu-Ende, aber noch nicht alle. 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?

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 auf dem Rechner 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 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

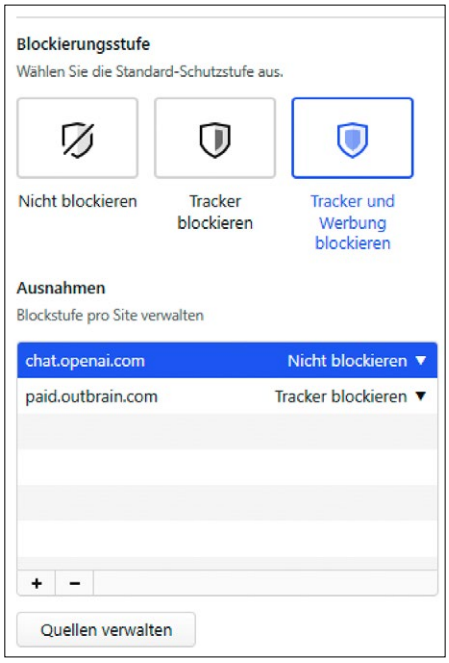
Weil jeder Browser nutzt, sind sie ein beliebtes Ziel für Angreifer. Sie sollten Ihren Browser daher aktuell halten und maximal sicher einstellen.

Bild: KI, Collage c't

Von Jo Bager

Aktuell halten

Um sicher zu surfen, sollte Ihr Browser immer auf dem neuesten Stand sein. Die Hersteller geben laufend Updates heraus, die Sicherheitslücken schließen. Alle gängigen Browser lassen sich so einstellen, dass sie sich automatisch aktualisieren. Es kann aber vorkommen, dass die Update-Versorgung klemmt oder 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“.



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

Add-ons aufräumen

Browser-Erweiterungen, auch Add-ons oder Extensions genannt, haben Zugriff auf alles, was innerhalb des Browsers geschieht, zum Beispiel auf das Online-Banking oder den Webmailer. 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 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, Vivaldi und Brave können das bereits von Haus aus, Sie müssen den Tracking-Blocker in den Einstellungen nur scharf schalten. Probieren Sie zunächst die strengste Einstellung. Falls es anschließend Probleme bei Ihren Lieblingswebsites gibt, können Sie den milderen Standardmodus wählen. Benutzen Sie Chrome, sollten Sie über einen Wechsel zu einem Browser mit Tracking-Blocker nachdenken. Ansonsten können Sie sich mit Add-ons wie Privacy Badger oder uBlock Origin Lite behelfen (siehe ct.de/y7ev). Letzteres beseitigt zudem aufdringliche und mitunter verseuchte Werbung.

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 Zustimmung ermitteln. Erlauben Sie das nur, 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“ und bei Edge 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 dann mit https:// und der Browser zeigt ein geschlossenes Vorhängeschloss neben der Adresse an. Untersuchen Sie Adressen genau auf Ungereimtheiten: 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/y7ev

Abzockschutz

Security-Checkliste gegen Online-Betrug

Bild: KI, Collage c't

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. Betrüger versuchen, Sie unter Druck zu setzen, um Sie zu unüberlegten und leichtsinnigen Handlungen zu bewegen. Ganz gleich, ob die Kontaktaufnahme telefonisch oder schriftlich erfolgt: 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.

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 dahinter steckt; 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. Das gilt insbesondere dann, wenn das Kind schon in den Brunnen gefallen ist und die Täter bereits zugeschlagen haben. In diesem Fall ist schnelles Handeln gefragt, um abgezocktes Geld zurückholen zu können, Passwörter zu ändern und so weiter. 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. Denn, was schon im Vorfeld aussortiert wird, kann Sie auch nicht auf dem falschen Fuß erwischen. 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. 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.

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

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 ist der Fakeshop-Finder der deutschen Verbraucherzentralen (siehe ct.de/y7k1) eine große Hilfe, die Browser-Erweiterung Fake-Shop Dector (siehe ct.de/y7k1) warnt Sie auch aktiv.

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/y7k1***

Soziale Sicherheit

Security-Checkliste Social Media

Bild: KI, Collage c't

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 Artikel „Security-Checkliste Passwörter“), 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, 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 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 Finanz-IT

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

Bild: KI, Collage c't

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 auf einem Windows-PC dafür, dass ein Virenscanner mit aktuellen Updates läuft. Der bei Windows 10 und 11 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 oder einer offiziellen Stelle wie der Polizei. 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/yemu).

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 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

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. 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/yemu***

Sicher sichern

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: KI, Collage c't

Von Axel Vahldiek

Jetzt!

Damit Sie im Ernstfall keine Daten verlieren, brauchen Sie ein Backup. Wie Sie das erstellen, ist an sich erst mal egal, denn jedes Backup ist besser als kein Backup. Wichtig ist, dass Sie es wirklich machen. Der richtige Termin 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. 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 überall hin. 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. Heutzutage wird die gern zur 3-2-1-1-0-Regel erweitert, wobei die zweite 1 für eine trojanersichere Offline-Kopie steht und die 0 für null Fehler beim Testen. Dazu mehr in den beiden nachfolgenden Abschnitten.

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. Alternativ hilft das Verschlüsseln des Backups; dann bekommt der Dieb mangels Schlüssel nur Datenmüll zu sehen. Wichtig: Probieren Sie 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.

Ruhiger schlafen

Ihr Backup erfüllt alle Anforderungen? Herzlichen Glückwunsch! Falls nicht: Eine Auswahl von weiterführenden c't-Artikeln mit vielen Tipps finden Sie über den nachfolgenden Link. *(axv@ct.de)* c't

Auswahl von c't-Artikeln: ct.de/ybas

Schotten dicht

Security-Checkliste Server & Hosting

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

Bild: KI, Collage c't

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 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. 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/yee2

Passwort: sicher

Security-Checkliste Passwörter

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

Bild: KI, Collage c't

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 und 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.

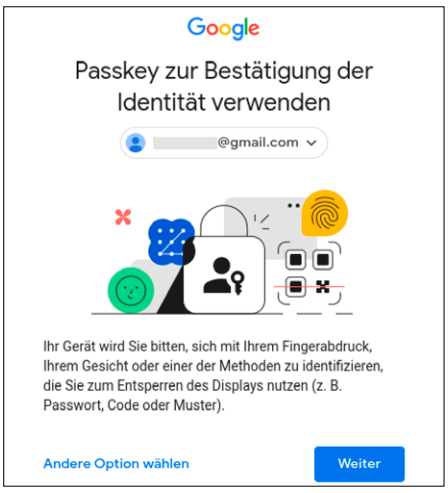
Passwortmanager

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].

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/y37x). Google-Nutzer können sich über den „Dark Web Report" auch benachrichtigen lassen, wenn damit beobachtete Daten im Darknet auftauchen.

Gibt es einen Treffer, ist das betroffene Passwort kompromittiert; ändern Sie es. 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 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 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, 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/y37x***