Die c’t-Sicherheits-Checkliste 2020

Einfache Strategien für mehr Sicherheit

Für Ihre Sicherheit können Sie beliebig viel Zeit investieren – müssen Sie aber nicht. Mit den richtigen Handgriffen können Sie Rechner, Smartphones, Router & Co. leicht vor den größten Cyber-Gefahren schützen.

Von Ronald Eikenberg

Sie haben es wahrscheinlich schon entdeckt: Die aktuelle c’t hat Verstärkung mitgebracht. Bei dem Büchlein handelt es sich um die aktualisierte Auflage unserer begehrten Sicherheits-Checklisten, die schon vielen Menschen dabei geholfen haben, ihr digitales Leben abzusichern. Die Checklisten enthalten die wichtigsten Handgriffe, um Smartphones, Rechner, Online-Accounts & Co. vor den größten Bedrohungen zu schützen. In maximal fünf Schritten sind Sie auf der sicheren Seite.

Aktuell und sicher

Einige Handlungsempfehlungen ziehen sich wie ein roter Faden durch unsere Sicherheits-Checklisten. So geht es etwa immer wieder um Updates. Mit den Aktualisierungen beheben die Hersteller nicht nur nervige Bugs, sie kümmern sich oft auch um Schwachstellen, die im Laufe der Zeit bekannt geworden sind. Ergo sollten Sie sicherstellen, dass alles auf dem aktuellen Stand ist – ganz gleich, ob es ums Betriebssystem, nachinstallierte Software wie Browser und Office oder die Firmware des Routers geht. Brenzlig wird es übrigens für Nutzer von Windows 7: Diese Windows-Version wird ab dem 14. Januar 2020 keine Sicherheits-Updates von Microsoft mehr erhalten. Noch ältere Versionen wie XP oder Vista bekommen schon jetzt keine Updates mehr. Wenn Ihr Betriebssystem nicht mehr mit Patches versorgt wird, dann sollten Sie auf eine neuere Version umsteigen, zum Beispiel auf das aktuelle Windows 10 oder ein Linux.

Vielerorts werden die Updates inzwischen automatisch installiert, allzu oft muss man allerdings nachhelfen. Wenn es einen Auto-Updater gibt, sollten Sie überprüfen, ob dieser wie erwartet funktioniert oder nicht doch mal wieder klemmt. Bei Geräten und Software ohne diese nützliche Funktion sollten Sie in regelmäßigen Abständen auf der Website des Herstellers schauen, ob ein Update zum Download bereitsteht und dieses gegebenenfalls einspielen – dies gilt insbesondere für Geräte wie Router, die mit dem Internet verbunden oder sogar aus dem Internet erreichbar sind.

Kein Backup, kein Mitleid

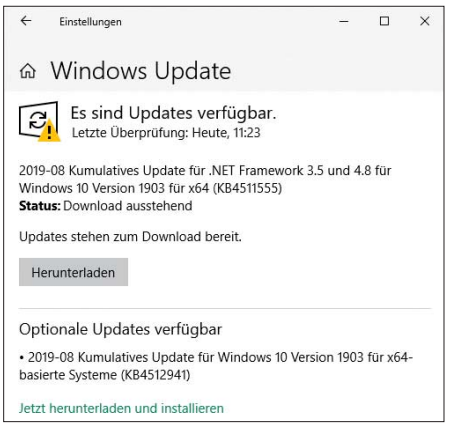
Wir können es nicht oft genug wiederholen: Legen Sie Backup-Kopien aller Dateien an, auf die Sie nicht verzichten möchten. Stellen Sie sich vor, die Festplatte Ihres Rechners oder Ihr Smartphone würde von jetzt auf gleich den Geist aufgeben oder ein Erpressungs-Trojaner würde zuschlagen. Welche Dateien sind unersetzlich und welche würden Sie schmerzlich vermissen? Diese Dateien sind das Mindeste, wovon Sie ein Backup besitzen sollten. Es ist ganz gleich, ob Sie Ihre wichtigen Daten in der Cloud, auf einem USB-Stick, einer DVD oder auf einem NAS speichern – jedes Backup ist besser als kein Backup. Wenn Sie auf Nummer sicher gehen wollen, befolgen Sie die einprägsame 3-2-1 Regel: 3 Kopien auf 2 unterschiedlichen Datenträgertypen und 1 davon außer Haus. Da das Original bereits als eine Kopie gilt, benötigen Sie nur noch zwei weitere.

Eine können Sie zum Beispiel auf einer USB-Platte speichern, eine weitere in der Cloud. Damit hätten Sie alle Punkte erfüllt. Die unterschiedlichen Speichertypen empfiehlt man, um Ausfallserscheinungen aufzufangen: Wenn Sie etwa zwei identische DVD-Rohlinge oder Festplatten nutzen, dann ist die Wahrscheinlichkeit hoch, dass diese zu einem ähnlichen Zeitpunkt das Zeitliche segnen. Die Kopie außer Haus lernen Sie zu schätzen, falls es mal brennt oder die Bude unter Wasser steht. Falls Sie Ihre Daten mehrere Jahre speichern möchten, sollten Sie von Flash-Speichern wie USB-Sticks, SSDs und Speicherkarten Abstand nehmen, da diese nach einiger Zeit ohne Strom zur Vergesslichkeit neigen.

Immer wieder Passwörter

Auch Passwörter sind ein Dauerbrenner – nicht nur in den Sicherheits-Checklisten, sondern allgemein in der c't. Und das nicht ohne Grund: Datenleaks beweisen immer wieder, dass viele Menschen nach wie vor leicht zu erratende Kennwörter wählen oder gar für mehrere Dienste das gleiche Passwort wählen. Letzteres ist für Cyber-Ganoven der Jackpot. Denn sie probieren geklaute Passwörter routinemäßig bei vielen Diensten aus, in der Hoffnung, dass ein Nutzer so bequem war, es auch an anderen Stellen einzusetzen. Mit diesem Generalschlüssel steht dem Angreifer oft die gesamte digitale Identität seines Opfers offen und der Schaden ist entsprechend groß. Erliegen Sie also nicht der Versuchung, Ihre Passwörter zu recyclen, wenn Ihnen Ihre Accounts etwas wert sind.

Langfristig können Sie durch das FIDO2-Verfahren bei vielen großen Diensten auf das Passwort verzichten. Sie legen dann nur noch den Finger auf einen speziellen USB-Stick oder den Fingerabdruckscanner Ihres Smartphones und sind sicher eingeloggt (siehe c't 18/2019, S. 16). Bis es soweit ist, müssen Sie sich jedoch noch mit dem guten alten Passwortverfahren arrangieren. Wenn Sie nicht zu den Gedächtniskünstlern zählen, die sich alle Passwörter merken können, dann nutzen Sie Zettel und Stift. Den Zettel bewahren Sie an einem sicheren Ort auf, etwa im Portemonnaie oder im Tresor. Es hat bislang noch kein Trojaner geschafft, dort reinzugreifen. Komfortabler geht die Passwort-Verwaltung mit einem Passwort-Manager wie KeePass oder LastPass von der Hand. Die Helferlein speichern Ihre wertvollen Passwörter in einem verschlüsselten Container, der mit einem Master-Passwort geschützt ist. Auf Knopfdruck generiert ein Passwort-Manager zudem sichere Kennwörter, die Sie sich zwar nicht mehr merken können, aber auch gar nicht mehr merken müssen. Viele Passwort-Manager können den verschlüsselten Container auch auf Wunsch geräteübergreifend synchronisieren.

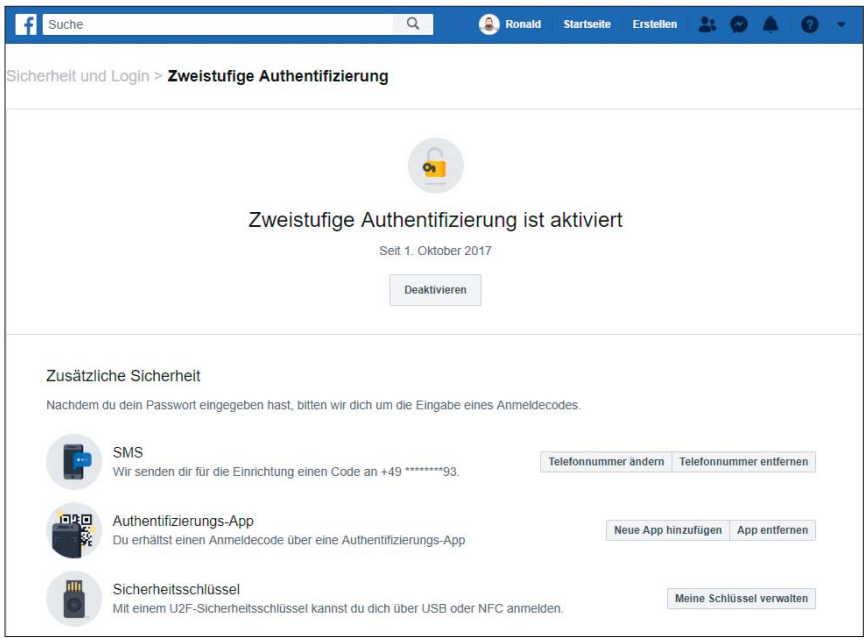


Stellen Sie sicher, dass alle verfügbaren Updates installiert sind – ganz gleich, ob es um PC, Smartphone oder Router geht.

Wenn Sie sich selbst Kennwörter ausdenken, dann achten Sie lieber auf die Länge als auf den Einsatz möglichst vieler exotischer Sonderzeichen. So sind die Kennwörter nicht nur leichter einzutippen, sondern auch schwer zu knacken. Denn je länger ein Passwort ist, desto länger beißt sich ein Angreifer die Zähne daran aus. Das gilt insbesondere bei der Schutzempfehlungen umsetzt – und Sie seltener ausrücken müssen, um verseuchte Rechner zu desinfizieren oder gehackte Accounts zurückzuerobern. Das Zauberwort heißt Awareness: Es geht dabei darum, das Grundwissen über die wichtigsten Schutzmechanismen und die größten Bedrohungen möglichst breit zu streuen. Tragen Sie Ihren Teil dazu bei, indem Sie die Sicherheits-Checklisten weitergeben.

Teilen erwünscht!

Das beiliegende Booklet haben wir bewusst so verfasst, dass es jeder versteht. Sie sind also eingeladen, es mit Familie, Freunden und Kollegen zu teilen. Falls Sie sich nicht von Ihrem Exemplar trennen mögen, können Sie es unter **ct.de/check2020** auch einzeln nachbestellen und gratis als PDF herunterladen. Geben Sie diesen Link gerne weiter! Sie erhöhen damit die Wahrscheinlichkeit, dass Ihr Umfeld die grundlegenden



Wenn Sie die Zwei-Faktor-Authentifizierung einschalten, schauen Hacker in die Röhre.

Verschlüsselung von Dateien und Festplatten; je länger Ihr Verschlüsselungs-Passwort ist, desto mehr Zeit geht fürs Knacken drauf.

Zwei Faktoren für die Sicherheit

Die Zwei-Faktor-Authentifizierung (2FA) ist ein Segen: Sie schützt Ihre Online-Accounts effektiv vor Online-Ganoven jeglicher Art. Schalten Sie diese Schutzfunktion wo immer möglich ein. Das klappt etwa bei vielen großen Online-Diensten wie Google, Facebook und GMX. Eine Übersicht der Dienste, bei denen Sie 2FA einschalten können, finden Sie unter ct.de/check2020. Ist die Schutzfunktion aktiv, dann ist zum Einloggen neben dem Passwort ein einmalig gültiger Code nötig, den Ihnen der Dienst zum Beispiel per SMS zuschickt. In vielen Fällen können Sie diesen Code auch selbst mit einer App wie dem Google Authenticator generieren. Manchmal genügt es sogar, eine Push-Nachricht auf dem Smartphone zu bestätigen. Entscheidend ist, dass Sie eine Aktion ausführen müssen, die ein Cyber-Gauner nicht ausführen kann. Dieser kann zwar Ihre Zugangsdaten entwenden und damit einen Login-Versuch unternehmen. Er kann jedoch nicht Ihr Handy greifen, um an den 2FA-Code zu gelangen. Mit der 2FA sind Ihre Accounts also selbst dann geschützt, wenn der Angreifer Ihren Nutzernamen und Ihr Passwort kennt.

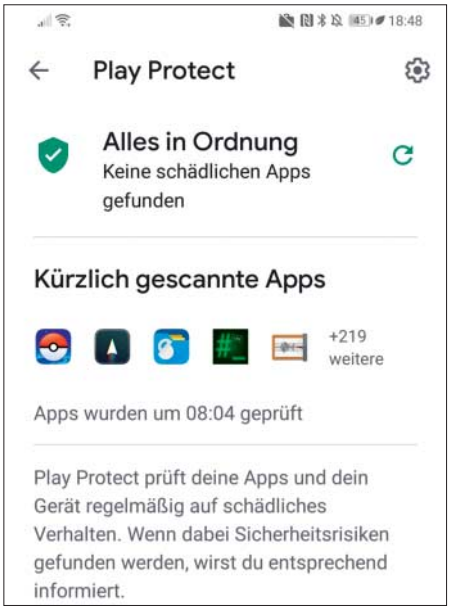
In vielen Fällen können Sie die Schutzfunktion so einstellen, dass sie nur beim ersten Login auf einem Gerät nach dem Code fragt. Wenn Sie Ihren Rechner, Ihr Smartphone oder Tablet also einmalig per 2FA authentifiziert haben, gilt es dann als vertrauenswürdig und der Code ist dort nicht mehr gefragt. Dadurch bemerken Sie im Alltag nicht mal, dass der Schutz aktiv ist. Sie können das Schutzniveau weiter erhöhen, indem Sie einen FIDO2- oder U2F-Sicherheitsschlüssel als zweiten Faktor mit dem Account verknüpfen. Diese Geräte haben meist den Formfaktor eines USB-Sticks und kosten rund 20 Euro. Ist ein Online-Account mit einem solchen Schlüssel verknüpft, können Sie sich nur noch einloggen, wenn der Schlüssel mit dem Rechner verbunden ist. So wehren Sie Angriffe mit entwendeten Zugangsdaten effektiv ab.

Virenschutz tut not, aber

Sie wundern sich vielleicht, warum das Thema Virenschutz so spät Erwähnung findet. Das liegt daran, dass es zwar nach wie vor wichtig ist, jedoch an Bedeutung verloren hat. Denn das wichtigste Ziel der Schädlinge – richtig, Microsoft Windows – kümmert sich inzwischen selbst um die Virenabwehr. Und das gar nicht mal schlecht: Der Windows Defender, der seit Windows 8 vorinstalliert ist, hat sich vom Rohrkrepierer zum zuverlässigen Virenschutzprogramm gemausert. In den Analysen unabhängiger Prüfinstitute ist der Defender in letzter Zeit regelmäßig vorn dabei. Wer gut geschützt sein will, muss also nicht länger einen Virenscanner nachinstallieren.

Sie sollten jedoch überprüfen, ob der mitgelieferte Schutz aktiv ist und mit aktuellen Virensignaturen versorgt wird. Haben Sie einen vorkonfigurierten Windows-Rechner gekauft, ist darauf möglicherweise die Testversion eines Virenjägers installiert, die nach einiger Zeit abläuft. Stellen Sie sicher, dass der Windows Defender im Anschluss den Betrieb aufnimmt. Sie finden den Virenwächter durch eine Startmenü-Suche nach „Windows-Sicherheit“. Auch macOS bringt einen rudimentären Virenschutz mit. Da es ohnehin nur wenige Schädlinge gibt, die es auf das Apple-Betriebssystem abgesehen haben, brauchen Sie nichts mehr zu unternehmen. Bei Linux sind vor allem die Server gefährdet, die aus dem Internet erreichbar sind. Wenn Sie einen solchen betreiben, sollten Sie Betriebssystem und Anwendungen immer auf dem aktuellen Patch-Stand halten, um Online-Schurken keine Angriffsfläche in Form von Sicherheitslücken zu bieten.

Bei den Smartphone-Betriebssystemen ist insbesondere Android gefährdet und auch hier ist inzwischen mit Google Play Protect ein Virenschutz an Bord. Wer sich von dubiosen Download-Quellen fernhält und die Apps ausschließlich über Google Play installiert, hat wenig zu be-



Virenschutz frei Haus: Auch Android bringt inzwischen einen Virenscanner namens Play Protect mit.

fürchten. iOS wird kaum attackiert, weil es die Angreifer hier besonders schwer haben – Apples mobiles Betriebssystem führt nur Apps aus, die zuvor von Apple untersucht und für ungefährlich befunden wurden. Auch hier können Sie sich einen Virenschutz sparen.

Beim Surfen schützt Sie ein Skriptblocker vor Schadcode und aufdringlichen Anzeigen. Sie können zum Beispiel zu uBlock Origin greifen (siehe ct.de/check2020), der als Erweiterung für alle wichtigen Browser angeboten wird.

Die gesunde Portion Skepsis

Selbst wenn Sie alle technischen Maßnahmen umgesetzt haben, um Rechner, Smartphone, Accounts & Co. vor üblen Gestalten zu schützen, gibt es immer noch eine Schwachstelle. Und das sind Sie. Wer sich allzu leichtfertig durch das Netz bewegt, der ist leichte Beute für Online-Gauner. Die Angriffe erfolgen zumeist über E-Mails – hier ist also besonders viel Vorsicht geboten. Begegnen Sie eingehenden Mails mit einer gesunden Portion Skepsis. Selbst wenn eine Nachricht anscheinend von einer Person kommt, die Sie kennen, muss das noch lange nicht so sein, da sich der Absender leicht fälschen lässt. Wenn Ihnen etwas seltsam vorkommt, dann fragen Sie beim Absender über einen anderen Kommunikationsweg nach (zum Beispiel per Telefon), ehe Sie den Aufforderungen in der Nachricht nachkommen und auf einen Link oder Anhang klicken. In Dateianhängen lauern oft Schädlinge, das gilt insbesondere für ausführbare Dateitypen wie .EXE, .BAT, .CMD, .JAR oder auch Skriptformate wie .VB, .VBS, .PSC1 oder .WSF. Die Schädlinge können sich auch in Dateiarchiven (wie .ZIP) verstecken. Ein hohes Gefahrenpotenzial geht von Office-Dokumenten aus. Aktivieren Sie auf keinen Fall Makrocode in solchen Dateien, sofern Sie sich nicht absolut sicher sind, dass alles mit rechten Dingen zugeht. Der Absender einer Virenmail wird versuchen, Ihre Neugier zu wecken und Sie damit zum Öffnen des Anhangs zu motivieren. Gängige Maschen sind etwa gefälschte Rechnungsmails oder vermeintliche Bewerbungsschreiben.

Hinter Links in Mails lauern oft Phishing-Seiten, die es auf Ihre Zugangsdaten abgesehen haben. Fahren Sie vor dem Anklicken eines Links mit der Maus darüber und überprüfen Sie unten im Fenster, welche Adresse sich tatsächlich dahinter verbirgt. Häufig werden solche Phishing-Mails im Namen von Banken oder Zahlungsdienstleistern wie PayPal verschickt. Oft setzen die Online-Gauner auch große Mail-Provider als Absender ein. Teilweise geben sie vor, dass die Mail von den Admins Ihres Arbeitgebers stammt. Die Absender behaupten dann etwa, dass der verfügbare Speicherplatz für das Mail-Postfach aufgebraucht sei und man sich daher dringend einloggen müsste, um weiter Mails empfangen zu können. Fallen Sie nicht darauf rein.

Phishing- und Virenmails sind mit bloßem Auge kaum von ungefährlichen Mails zu unterscheiden.

Was sonst noch zählt

Mit den oben beschriebenen allgemeingültigen Tipps sind Sie vor den häufigsten Online-Attacken geschützt. Doch nicht nur im Netz lauern Gefahren, manchmal ist der Angreifer auch ganz in Ihrer Nähe und nutzt zum Beispiel WLAN, um auf Ihre Systeme zuzugreifen. Am wichtigsten ist, dass Sie Ihr eigenes WLAN gut schützen. Nutzen Sie ein individuelles, langes WLAN-Passwort, um Unbefugte aus dem lokalen Netz fernzuhalten. Stellen Sie darüber hinaus regelmäßig sicher, dass die Router-Firmware auf dem aktuellen Stand ist und deaktivieren Sie die Komfortfunktion WPS. Diese war in der Vergangenheit bei vielen Router-Modellen von Sicherheitslücken betroffen. Außerdem kann sich über WPS jeder Zugriff auf Ihr Netz verschaffen, der an Ihren Router kommt – ein Knopfdruck genügt (WPS Push Button).

Richten Sie ein Gastnetz für Personen ein, die nur vorübergehend auf Ihr Netz zugreifen sollen. Ein angenehmer Nebeneffekt ist, dass Sie die Gäste damit auch aus Ihrem privaten Heimnetz und von den daran angeschlossenen Geräten wie Netzwerkspeichern (NAS) fernhalten können. Dort können Sie auch vernetzte IoT-Geräte betreiben, die unbedingt ins Internet wollen – etwa die sprachgesteuerte Schaltsteckdose aus Fernost.

Falls Sie unterwegs in fremden Netzen surfen, dann nutzen Sie so viele Dienste wie möglich verschlüsselt – etwa, indem Sie die HTTPS-Version ansteuern. Die beste Lösung ist ein VPN Zugang, da darüber sämtlicher Datenverkehr verschlüsselt wird. Wenn zum Verbindungsaufbau mit einem Netz kein Passwort nötig ist, wie es etwa bei vielen Hotspots der Fall ist, werden nämlich sämtliche Daten im Klartext an den Router geschickt. Jeder in Funkreichweite kann diese Datenpakete aufzeichnen und mitlesen. Nutzen Sie im Zweifel lieber Ihre Mobilfunkverbindung, um unterwegs aufs Internet zuzugreifen. Die lässt sich nicht ohne weiteres anzapfen.

Last, but not least sollten Sie davor gewappnet sein, dass eine unbefugte Person versucht, direkt auf Ihr Smartphone, Tablet oder Ihren Rechner zuzugreifen. Setzen Sie also eine Bildschirmsperre mit Passcode – im Idealfall eine PIN mit mindestens 6 Zeichen oder ein Passwort. Zum Entsperren können Sie Fingerabdruck oder Gesichtsscan nutzen.

Natürlich können wir in einem Artikel wie diesem nur die nötigsten Tipps unterbringen. Zu allen Themen finden Sie tiefer schürfende Artikel in älteren c't-Ausgaben. Eine Auswahl haben wir unter ct.de/check2020 zusammengestellt. Weitere konkrete Tipps liefert Ihnen unser Booklet, das dieser c't-Ausgabe beiliegt. Sollte es fehlen, können Sie es kostenlos unter ct.de/check2020 als PDF herunterladen. *(rei@ct.de)* c't

Booklet, weitere Tipps und Artikel:
ct.de/check2020