Einfach sicher

Die c’t-Security-Checklisten 2021

Bild: Andreas Martini

Das Absichern von Smartphone, Rechner, WLAN-Router und Online-Accounts kann viel Zeit in Anspruch nehmen. Dabei sind oft nur wenige Handgriffe nötig, um vor den meisten Cyber-Attacken geschützt zu sein. Mit unseren Security-Checklisten sind Sie schnell auf der sicheren Seite.

Von Ronald Eikenberg

Während Sie diese Zeilen lesen, finden weltweit Millionen Hackerangriffe statt. Möglicherweise versucht ein Bot in diesem Moment, mit erbeuteten Zugangsdaten in Ihren Mail-Account einzusteigen oder Ihren Facebook-Account zu übernehmen. Eventuell steht auch Ihr Router unter Beschuss oder ein Banking-Trojaner lauert darauf, dass Sie eine Überweisung tätigen. Wer die Gefahr auf die leichte Schulter nimmt, ist leichte Beute.

Denn die Cyber-Gangs haben es nicht nur auf hochrangige Ziele wie Regierungsorganisationen abgesehen, sondern auf jeden von uns. Und auch das Argument „Bei mir gibt es eh nichts zu holen“ zählt schon lange nicht mehr: Selbst eine veraltete Smart-Home-Zentrale ist den Angreifern noch gut genug, um sie als Bot zu missbrauchen und damit weitere Systeme auf der ganzen Welt zu infizieren. Den Ärger haben erst mal Sie, denn die Folgeangriffe gehen von Ihrer IP-Adresse aus.

Sicherheitscheck

Die gute Nachricht ist, dass Sie etwas dagegen tun können. Und das mit geringem Aufwand. IT-Sicherheit ist zwar ein komplexes Feld, die wichtigsten Abwehrmaßnahmen gegen Hacker sind jedoch so simpel, dass sie wirklich jeder umsetzen kann – und sollte. Wir haben die grundlegenden Handgriffe zum Absichern von Rechner, Smartphone, WLAN-Router, Social-Media-Accounts und vielem mehr in unseren Security-Checklisten für Sie zusammengestellt.

Es dauert in aller Regel nicht länger als fünf Minuten, um eine Checkliste durchzugehen und im Fall der Fälle nachzubessern. Sie erfahren zudem, wie Sie dem nächsten Datenverlust durch Trojaner-sichere Backups vorbeugen und was ein sicheres Passwort ausmacht. Wenn Sie sich die Tipps in diesem Heft zu Herzen nehmen, dann sind Sie gegen die häufigsten Cyber-Attacken gefeit.

Sicher im Homeoffice

Wir haben die diesjährige Ausgabe der Security-Checklisten erneut auf die aktuelle Bedrohungslage zugeschnitten und umfassend aktualisiert. Eine wichtige Neuerung ist die Homeoffice-Checkliste (Seite 20), die Ihnen zeigt, wie Sie sicher von zu Hause arbeiten. Gerade dabei darf die Sicherheit nicht zu kurz kommen: Denn wenn bei Ihnen zu Hause ein Trojaner ausbricht, kann er die gesamte Firma lahmlegen. Neu ist auch die Checkliste „Server & Hosting“ (Seite 33), die Ihnen die allerwichtigsten Schritte zur Absicherung von Servern und Webhosting-Paketen zeigt.

Einige Empfehlungen ziehen sich wie ein roter Faden durch die Security-Checklisten – und das aus gutem Grund. Dazu zählt etwa der Rat, auf den Einsatz aktueller Software zu achten. Das ist unerlässlich, denn Betriebssystem-Updates und neue Programmversionen bringen nicht nur neue Funktionen mit und beseitigen nervige Bugs, oftmals schließen die Aktualisierungen auch ernstzunehmende Sicherheitslücken. Wer Cyber-Angreifer fernhalten möchte – und wer will das nicht –, sollte Updates also zeitnah nach ihrer Veröffentlichung einspielen, ganz gleich, ob es um Windows, das Smartphone, den WLAN-Router oder die WordPress-Installation geht.

Auch Passwörter werden in den Checklisten immer wieder thematisiert. Im Netz kursieren Milliarden gehackte Passwörter und Auswertungen dieser Daten zeigen, dass nach wie vor viele Nutzer leichtfertig viel zu einfache Kennwörter wählen oder gar bei mehreren Diensten dasselbe nutzen. Das ist so, als würden Sie überall dasselbe Schloss einsetzen: Wird Ihr Briefkastenschlüssel geklaut, kann der Dieb damit nicht nur Ihre Wohnung ausräumen, sondern auch gleich mit Ihrem Auto davonfahren. Ein gutes Passwort ist nicht nur lang, sondern auch einzigartig. Es passt nur bei einem Dienst. Mehr zum Thema Passwörter erfahren Sie auf Seite 32.

Da jeder ein Anrecht auf IT-Sicherheit hat, möchten wir mit den Security-Checklisten möglichst viele Menschen erreichen. Sie können uns dabei helfen: Reichen Sie die Checklisten auch an Bekannte, Freunde, Verwandte, Kollegen und Mitarbeiter weiter, damit jeder einen soliden Grundschutz in kurzer Zeit umsetzen kann. Wenn Sie sich nicht von Ihrer c't trennen möchten, dann geben Sie einfach das kleine Büchlein weiter, das wir dieser Ausgabe beigelegt haben. Das Booklet im handlichen A6-Format enthält die wichtigsten Tipps in Kurzform.

Die Security-Checklisten enthalten bewusst nur die wichtigsten Handgriffe, die jeder umsetzen sollte, um sich vor den häufigsten Cyber-Attacken zu schützen. Wer tiefer in ein bestimmtes Thema einsteigen möchte, bekommt in c't weiterhin die Gelegenheit dazu – in vorherigen und folgenden Ausgaben.

Wenn Sie Nachschub brauchen, können Sie das Booklet unter **ct.de/check2021** nachbestellen und als PDF herunterladen. In der Vergangenheit hat das bereits gut geklappt: Die vorherigen Auflagen der Sicherheits-Checklisten wurden in Banken, Ämtern, Unternehmen und Bildungseinrichtungen im Rahmen von Awareness-Maßnahmen an Mitarbeiter verteilt.

Los gehts!

Wenn Sie die Checklisten durchgegangen sind und feststellen, dass Sie schon alles umgesetzt haben: Ausgezeichnet, jetzt ist der richtige Zeitpunkt, das Heft weiterzugeben – etwa an jemanden im Familien- oder Freundeskreis, der sich bislang eher weniger mit dem Thema IT-Sicherheit beschäftigt. Vielleicht können Sie damit sogar ein paar Notfallanfragen abfangen, zum Beispiel weil der nächste Krypto-Trojaner erfolgreich abgewehrt wird oder im Fall der Fälle zumindest rechtzeitig ein Trojaner-sicheres Backup angelegt wurde. Jetzt aber genug der Vorrede, es geht frisch ans Werk! *(rei@ct.de)* c't

Booklet nachbestellen, PDF-Download: ct.de/yhyp