2019

Mit Sicherheits-Checklisten

c't Security

Sicherheitsratgeber für Heim & Büro

Jenseits von Drogenhandel und Bitcoin

Vom Darknet lernen

Anonym und ultrasicher surfen • Betrugssicher handeln

Handy-Überwachung enttarnen

Spione finden • Android und iOS entwanzen

Raspi als Internet-Filter

Schluss mit Tracking und Werbung

Emotet-Trojaner abwehren

Die nächste Cybercrime-Generation greift an

Antiviren-Test 2019: Reicht der Defender?

9 Programme im Test • Windows optimal absichern

Bloßgestellt und ausgeplündert durch gekaperte Online-Konten

Identitätsklau verhindern

c't Security

Heise

Inhalt

Darknet & Cybercrime

Windows absichern

Viren & Co.

Identitätsklau

Mehr zum Inhalt des Heftes auf Seite 6!

Inhalt

Handy-Spionage

Smart und sicher

Sicherheits-Checklisten

Zum Heft

Mehr zum Inhalt des Heftes auf Seite 4!

Vom Darknet lernen

Spannende Techniken und Lösungsansätze aus dem Darknet

Auch jenseits von illegalem Schwarzmarkt und Anonymität hat das Darknet viel zu bieten. Wer sich nicht von Sensationsgeschichten blenden lässt, findet spannende Lösungen für Probleme, die uns auch im Alltag beschäftigen.

Von Jürgen Schmidt

Das Darknet – fast jeder denkt dabei sofort an illegale Waffen, Drogen und Kinderporno-Tauschringe. Ja, all das gibt es im Darknet. Doch darum soll es in den folgenden Artikeln nicht gehen. Denn das Darknet hat viel mehr zu bieten als Illegales. Es ist ein einzigartiges Biotop mit interessanten Formen der Interaktion und spannenden Lösungen für Probleme, die uns auch im ganz normalen Leben umtreiben. Wer genau hinschaut, findet im Darknet Ansätze, die sich auch auf den Alltag und die helle Seite des Internet anwenden lassen.

Zum Beispiel Marktplätze: Wer schon mal versucht hat, im Internet ein gebrauchtes iPhone zu verkaufen, kennt das Problem. Teile der ganz normalen Internet-Märkte sind derart von Kleinkriminellen dominiert, dass man seine Waren oder sein Geld auch gleich wegwerfen kann – und sich dann wenigstens den Ärger spart. Im Darknet ist die Ausgangssituation noch krasser: Man muss dort davon ausgehen, dass das Gegenüber ein gewissenloser Betrüger ist, der jede sich bietende Gelegenheit nutzen wird, einen skrupellos über den Tisch zu ziehen. Und Sie werden keinerlei Möglichkeit haben, ihn dafür zu Rechenschaft zu ziehen. Wie soll man da noch Geschäfte machen?

Doch genau das funktioniert auf manchen Schwarzmarkt-Plattformen erstaunlich gut. Der Käufer bekommt die ihm zugesicherte Ware und der Verkäufer sein Geld; Betrugsfälle sind selten. Das hat rein gar nichts mit der bekanntermaßen ohnehin nicht vorhandenen Ehre unter Dieben zu tun. Sondern es beruht auf einem raffinierten Treuhändermodell. Bei dem übrigens die Treuhänder in aller Regel ebenfalls Gauner sind. Wie das alles funktioniert, erklärt der Artikel

Doch auch wer sich weniger für sozioökonomische Studien interessiert als für solide Technik, kommt auf seine Kosten. Denn vor allem im Bereich Security und Privacy kann das Darknet mit interessanter Technik und pragmatischen Lösungen glänzen, die keineswegs auf illegale Aktivitäten beschränkt sind.

Das Tor zum Darknet

So pflegen die Tor-Entwickler einen Browser, der sich vorzüglich als unabhängiger Zweit-Browser eignet. Damit muss man seinen Alltags-Browser nicht mit unkomfortablen Einschränkungen vernageln, sondern kann für all die Fälle, in denen man gern „auf Nummer sicher“ gehen will, auf den Tor-Browser zurückgreifen. Der setzt nämlich die Sicherheit ganz kompromisslos an die erste Stelle: kein Flash, nur explizit erlaubtes JavaScript und wo immer möglich erzwungene Verschlüsselung (siehe S. 12).

Apropos Tor: Dieses Netz im Netz bildet die technische Grundlage für große Teile des Darknet. Das liegt daran, dass Tor sehr weitreichende Garantien für Anonymität und Abhörsicherheit bietet, die bei Kriminellen hoch im Kurs stehen. Doch man muss nicht kriminell sein, um sich im Internet mehr Privatsphäre zu wünschen.

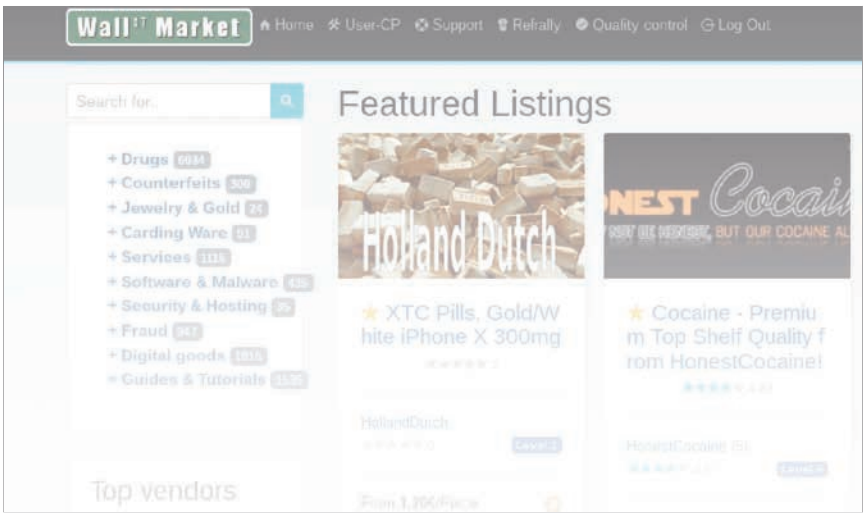
Die versprochene Anonymität erzeugt das Tor-Netz, indem das „Tor Onion Routing“ die Daten über mehrere Zwischenstationen schickt, die auf einer strikten „Need to know“-Basis operieren. Im normalen Internet trägt jedes Datenpaket die IP-Adresse des Absenders und des Empfängers; jede Station auf dem Weg kann diese Information einfach mitlesen. Bei Tor sieht jeder Netzwerkknoten immer nur den jeweiligen vorigen und nächsten Hop – aber keiner kennt sowohl Absender als auch Empfänger.

Erst wenn die Daten das Tor-Netz verlassen, um etwa an einen herkömmlichen Internet-Server geschickt zu werden, sieht der dafür zuständige Tor-Exit-Knoten die wirkliche Zieladresse. Er weiß aber nicht mehr, wer der ursprüngliche Absender war. Den kennt nur der sogenannte Tor Entry Guard – der aber weder Empfänger noch Inhalt der Daten sehen kann.

Diese Anonymität hat allerdings durchaus Grenzen. Sie liegen jedoch nicht bei den bekannten technischen Limitierungen, wie unsere Recherchen zur Praxis der Strafverfolgung im Darknet zeigen. Auch Tor ist kein universeller Garant für Anonymität – im Zweifelsfall steht das Sonderkommando schneller vor der Haustür, als man es sich träumen lässt. Der Artikel auf Seite 18 erklärt, warum das so ist.

Abhörfreier Raum

Anders sieht es mit der Abhörsicherheit aus. Die von Tor eingesetzte Verschlüsse-



Lesen Sie mehr in der c’t Security 2019

Windows absichern

Mit Bordmitteln zum sicheren Rechner

Wer seinen Windows-PC vor digitalen Bedrohungen schützen möchte, kann beliebig viel Geld investieren, etwa in Virenscanner, Firewall, Verschlüsselungssoftware und so weiter. Doch notwendig ist das nicht: Alles, was man an Schutz benötigt, hat Windows 10 inzwischen an Bord.

Von Ronald Eikenberg und Axel Vahldiek

Die Zeiten, in denen man viel Geld in den Schutz seines Windows-Rechners investieren musste, sind glücklicherweise vorbei. Denn Microsoft hat die Windows-Bordmittel im Laufe der Zeit ordentlich erweitert. Das Unternehmen arbeitet kontinuierlich daran, sein Betriebssystem gegen aktuelle Bedrohungen abzusichern und rüstet immer wieder Schutzfunktionen nach. Darunter befinden sich auch solche, für die man früher separate Software installieren musste. Ein prominentes Beispiel ist die mit Windows XP SP2 eingeführte Personal Firewall, ein weiteres der Virenschutz Windows Defender, der seit Windows 8 an Bord ist. Und diese Funktionen werden stetig weiterentwickelt, was dazu geführt hat, dass die Schutzleistung inzwischen so hoch ist, dass man sich nicht mehr nach Alternativen umsehen muss. Auch mit den halbjährlichen Windows-10-Upgrades hat Microsoft immer wieder Security-Features wie den Ransomware-Schutz nachgeliefert. Mittlerweile kann sich Windows gegen die meisten Attacken selbstständig wehren – genauer: könnte. Denn manche der mächtigen Bordmittel muss man erst mal aktivieren oder konfigurieren. Lohn der Mühe: Anschließend hat man nur noch wenig zu befürchten.

Dieser und die nachfolgenden Artikel erläutern, wie Sie Ihre Windows-10-Systeme ebenso wie die von Freunden und Verwandten so konfigurieren, dass sie den meisten Angriffen standhalten. Zudem erklären wir, wie Sie die Datenschutzproblematik in den Griff bekommen, wie Sie Ihre Dateien vor Zugriffen durch Unbefugte schützen und welche zusätzlichen Maß-

Wer noch mit einer älteren Windows-Version unterwegs ist, sollte über ein Upgrade nachdenken. Das bedeutet zwar zugegebenermaßen, dass Sie sich unter anderem wegen „Windows as a Service“ ein paar andere Probleme einhandeln [1]. Doch was das Thema Sicherheit betrifft, liegt Windows 10 trotzdem weit vor dem Vorgänger. Zudem wird sich für Nutzer von Windows 7 die Lage ab Januar 2020 dramatisch zuspitzen, da Microsoft nach diesem Termin keine Sicherheits-Updates mehr für Version 7 veröffentlichen will. Wer danach weiter Windows nutzen möchte, für den wird ein Wechsel unausweichlich, sofern er den PC nicht komplett vom Internet trennt. Daher spricht wenig dagegen, schon jetzt umzusteigen und von den modernen Schutzfunktionen zu profitieren – noch geht es kostenlos. Einen c’t-Artikel mit ausführlichen Tipps zum Umstieg können Sie kostenlos über ct.de/w42s lesen. Geben Sie den Link gerne weiter.

Virenschutz ohne Frust

Studiert man die Ergebnisse des auf Antiviren-Programme spezialisierten Prüflabors AV-Test, erkennt man deutlich, dass sich bei Microsoft seit dem Herbst 2015 einiges getan hat: Damals, kurz nach Veröffentlichung von Windows 10, erreichte der mitgelieferte Virenscanner Windows Defender in Sachen Schutzwirkung gerade einmal 3,5 von 6 möglichen Punkten. Im Frühling 2018 schaffte der Defender hingegen eine Wertung von 5,5 und liegt seitdem gleichauf mit Produkten von Avast, AVG und G Data. In den Kategorien Geschwindigkeit und Benutzbarkeit schnitt der bordeigene Scanner ebenfalls mit 5,5 Punkten gut ab. Und auch im Real-World-Test des österreichischen Prüfinstituts AV-Comparatives kommt der Defender gut weg. Im Vergleich zu anderen Antiviren-Programm ist der Windows Defender erfreulich unaufdringlich, weil er seine Anschaffung nicht rechtfertigen muss. Kurzum: Es gibt wenig Gründe, unter Windows 10 einen anderen Virenscanner zu installieren.

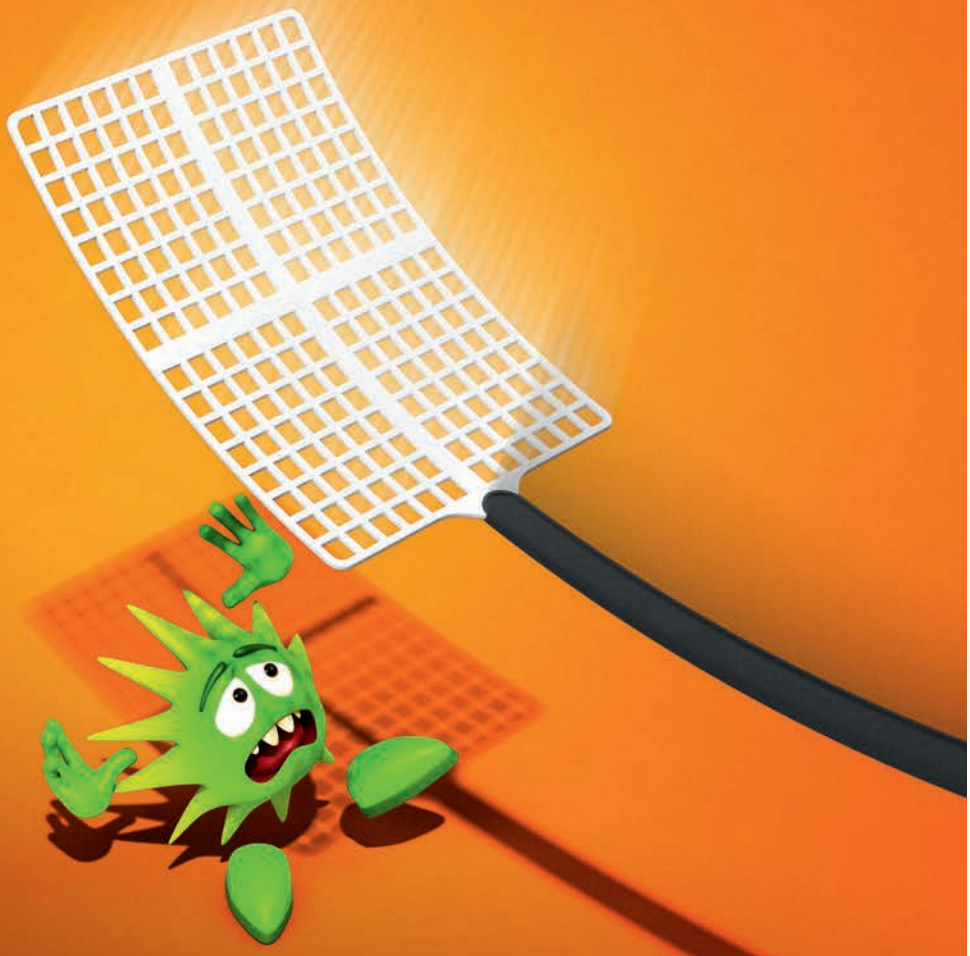
Um sicherzustellen, dass der Virenschutz aktiv ist, sollten Sie der Übersichtsseite „Windows-Sicherheit“ einen Besuch abstatten, die Sie zum Beispiel durch einen Klick auf das Defender-Symbol (der Schild) im Infobereich der Taskleiste erreichen. Falls das Symbol nicht zu sehen ist, versteckt es sich hinter dem kleinen Pfeil nach oben. Sie können es dann mit gedrücktem Mauszeiger neben die Uhrzeit ziehen, um den Sicherheitsstatus stets im Blick zu haben.

Überprüfen Sie zunächst unter „Viren- & Bedrohungsschutz/Updates für Viren- & Bedrohungsschutz“, ob die Bedrohungsdefinitionen auf dem aktuellen Stand sind. Diese sind die Grundlage

Lesen Sie mehr in der c’t Security 2019

Virenschutz: Zahlen oder sparen?

Der Rest der Welt gegen den Windows Defender



Virenschutzprogramme für Windows gibt es wie Sand am Meer – von gratis bis teuer. Inzwischen drängt sich allerdings die Frage auf, ob man überhaupt noch ein Schutzprogramm installieren muss. Denn der vorinstallierte Windows Defender hat mächtig aufgeholt. Wir haben nach einer Antwort gesucht.

Von Ronald Eikenberg

Virenschutz zählt seit jeher zur Grundausstattung eines jeden Windows-Rechners. Für das sichere Gefühl zahlen viele Nutzer gern, wie ein Blick in die Software-Charts großer Online-Händler zeigt. Doch ist das überhaupt noch nötig? Es gibt doch seit Jahren kostenlose Virenschutzprogramme. Die größte Konkurrenz macht den Bezahlprogrammen jedoch Microsoft: Seit Windows 8 gehört mit dem Windows Defender eine Schutzsoftware zum Lieferumfang.

Die anfängliche Theorie, dass dieser Schritt der Redmonder zu einem Massensterben der Antivirenfirmen führen könnte, hat sich nicht bewahrheitet: Die Erkennungsraten des Defender waren zu Beginn viel zu schlecht. In unserem umfangreichen Virenscanner-Test in c't 26/2014 (siehe ct.de/w2qp) erkannte der Microsoft-Schutz gerade einmal 60 Prozent der Schädlinge, die wir ihm vorsetzten. Die besten im Test verhinderten hingegen 98 Prozent der Infektionsversuche. Vor dem Defender mussten also weder Antivirenhersteller noch Cyber-Ganoven zittern.

Doch diese Zeiten sind längst vorbei. Rund ein halbes Jahr später machte der Windows Defender bemerkenswerte Fortschritte. Ablesen kann man dies an den Ergebnissen der unabhängigen Prüfinstitute AV-Test und AV Comparatives, die sich auf darauf spezialisiert haben, Antivirensoftware auf Herz und Nieren zu testen. So kletterte die Schutzleistung des Defender in der AV-Test-Bewertung von zwischenzeitlich null Punkten Anfang 2015 zunächst auf drei von sechs möglichen Punkten. Von da an ging es bergauf: Vor rund einem Jahr erzielte der Microsoft-Schutz erstmals die volle Punktzahl bei AV-Test, seitdem hält er sich im oberen Bereich der Punkteskala. Auch im Testlabor von AV-Comparatives schneidet der Defender regelmäßig gut ab. Das ist Grund genug, die Situation auf dem Antivirenmarkt neu zu bewerten.

Auferstanden aus Ruinen

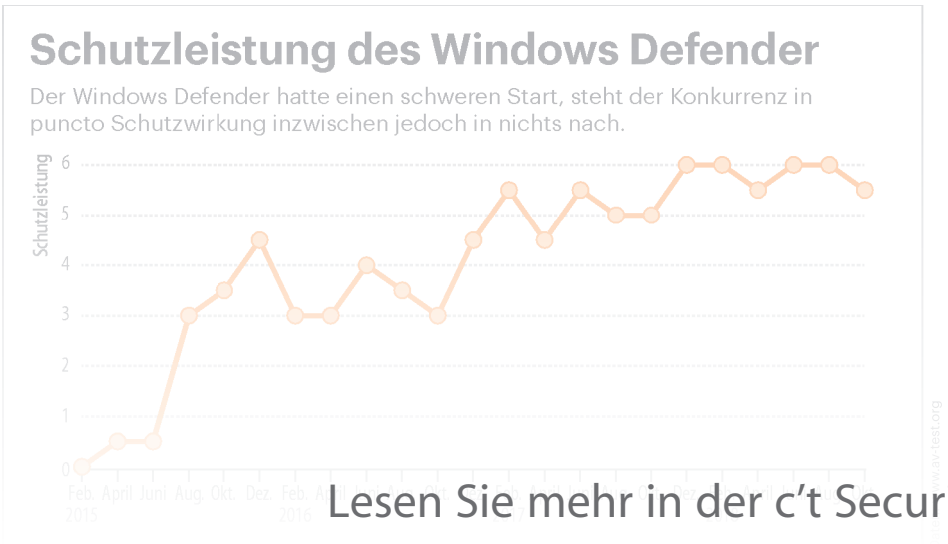
Der Aufstieg des Defender ist kein Zufall. Microsoft erklärt in seinem Security-Blog, dass die Schutzsoftware hinter den Kulissen komplett überarbeitet wurde (siehe ct.de/w2qp). Demnach geht ein großer Anteil am Leistungssprung auf das Konto künstlicher Intelligenz (KI) und maschinellen Lernens (ML). Mit diesen Verfahren versucht ein Schutzprogramm anhand vieler verschiedener Dateieigenschaften wie den Metadaten einzuschätzen, wie hoch die Wahrscheinlichkeit ist, dass von einer Datei eine Gefahr ausgeht. Bei einer hohen Wahrscheinlichkeit kann der Virenschutz eine intensivere Analyse durchführen und die Datei etwa in einer Sandbox ausführen, um Gewissheit über die Absichten zu erlangen.

Künstliche Intelligenz gegen reale Bedrohungen

Auf diese Weise können auch zuvor unbekannte Schädlinge überführt werden, während die zur Verfügung stehenden Rechenkapazitäten möglichst effizient genutzt werden. In seinem Blog dokumentiert Microsoft detailliert, wie KI und ML konkret dazu beigetragen haben sollen, Schädlingswellen wie Emotet zu stoppen. Microsoft hat den Einsatz speziell trainierter ML-Modelle bei der Virenjagd jedoch nicht erfunden, auch die traditionellen Antivirenhersteller setzen seit Längerem darauf, um der Schädlingsflut Herr zu werden.

Je nach Hersteller wird die KI-Magie unterschiedlich eingesetzt, teilweise laufen einfache KI-Modelle lokal auf dem zu schützenden Client, während aufwendigere Operationen in der Hersteller-Cloud ausgeführt werden. Sinnigerweise ordnet man die verschiedenen Schutzverfahren von einfach und schnell bis hin zu aufwendig und langsam hintereinander an. Nur, wenn ein Schritt nicht ausreichend Klarheit verschafft, wird der nächste bemüht.

Aber auch bewährte Erkennungsverfahren wie Virensignaturen, Verhaltensüberwachung und Heuristik kommen weiterhin zum Einsatz. Die signaturbasierte Erkennung war lange der Maßstab für die Schutzleistung einer Antivirensoftware. Dem Schutzprogramm wird dabei eine Sammlung tausender Schädlinge vorgesetzt, die im Vorfeld zusammengetragen wurde. Es gilt, möglichst viele davon zu erkennen. Diese Ergebnisse sind inzwischen jedoch nur noch wenig aussagekräftig. Die Antivirenindustrie ist gut untereinander vernetzt und so dauert es nicht



Im Namen des anderen

Identitätsklau nimmt zu und wird raffinierter

Ihre digitale Identität ist zum begehrten Angiffsziel geworden. Die Gefahr steigt, dass Fremde in Ihrem Namen auf Shopping-Tour gehen oder Ihre Daten illegal veröffentlichen. Doch wenn Sie die Methoden der Identitätsdiebe kennen, können Sie sich selber schützen.

Von Holger Bleich

Es war ein lang geplanter Urlaubstrip nach New York. Simone Peters freute sich darauf, ihren 33. Geburtstag zusammen mit ihrer besten Freundin im Big Apple zu feiern. Als sie am Flughafen ihren Pass zur Einreise überprüfen ließ, erschienen drei uniformierte Beamte: „Kommen Sie mit“, forderte einer sie auf. In einem Hinterzimmer sah sich Peters unvermittelt grimmig dreinschauenden, bewaffneten Polizisten gegenüber.

Später stellte sich heraus, dass die Bankerin ohne ihr Wissen auf einer US-Fahndungsliste gelandet war – jemand hatte ihre Identität digital dazu missbraucht, einen betrügerischen Online-Shop zu eröffnen und dort gefälschte Louis-Vuitton-Taschen zu verkaufen. Die Vorladungen gingen an eine Fake-Adresse, sodass Peters als flüchtig deklariert wurde. Erst einen Tag später hatte sich der Fall geklärt und Peters durfte einreisen.

Dies ist eine von vielen wahren Geschichten, die die Journalistin Tina Groll und der Polizist Cem Karakaya erzählen. Die beiden haben jüngst ein Buch veröffentlicht, in dem sie anhand konkreter Beispiele viele Facetten des Identitätsdiebstahls beleuchten [1]. Da geht es etwa um Stalker, die Facebook-Konten kapern, um den illegalen Handel mit ergaunerten persönlichen Daten, und vor allem um Warenbetrug, der die Opfer mitunter um viel Geld bringt.

Schwammiger Begriff

Der Klau, oder präziser gesagt: der Missbrauch von Identitätsdaten hat sich in den letzten Jahren zu einem massiven Pro-

schon einmal Opfer eines Identitätsklaus. Je sechs Prozent berichteten, dass mit ihren Daten ein gefälschter Account angelegt wurde – etwa bei ebay oder Facebook –, oder dass die Kreditkartendaten gestohlen und missbraucht wurden. Drei von zehn der Betroffenen hatten demnach einen finanziellen Schaden erlitten (siehe Abbildung auf S. 81).

Zwar ist der Begriff Identitätsdiebstahl in aller Munde, doch was er genau beschreibt, bleibt oft schwammig. Es fehlt arglosen Konsumenten oft die Fantasie, sich vorzustellen, was böswillige Täter mit einigen wenigen privaten Informationen anfangen können – das muss nicht einmal ein Passwort sein. Deshalb ist vielen potenziellen Opfern nicht klar, welche Angriffsvektoren Täter nutzen, um an fremde Daten zu kommen.

Fiese Tricks

Der Journalist Richard Gutjahr berichtete einmal launisch in seinem Blog, wie er im Flughafen-Wartebereich genervt dem Handy-Gespräch eines Geschäftsmanns neben ihm zuhörte: „Offenbar war er gerade dabei, eine Limousine zu buchen. Irgendwann zückt er seinen Geldbeutel, beginnt damit, seine Kreditkartendaten vorzulesen. Reflexartig fahre ich die Tastatur meines iPads aus und tippe mit. Ziffer für Ziffer der Kartennummer, dann das Gültigkeitsdatum und die Prüfnummer. Warum ich das tue? Weil ich es kann.“

Gutjahr brachte es auf den Punkt: „Auf einmal wird mir klar, ich könnte jetzt weiß Gott was mit seinen Daten anstellen: einkaufen, Online-Konten bei eBay, Amazon oder Apple einrichten.“ Seinem Bericht zufolge beließ er es dabei, dem „Opfer“ seines Identitätsdiebstahls über den Druck- und Lieferservice der Deut-

Hans-Joachim Henschel, Kriminalhauptkommissar am Landeskriminalamt (LKA) Niedersachsen, berichtete c't auf Anfrage von derzeit häufig gemeldeten Angriffsmethoden. Da wären beispielsweise die arglosen Nutzer von eBay und anderen Miet- oder Verkaufsplattformen. Von ihnen fordern Täter wahlweise als Käufer, Verkäufer oder Vermieter einen Echtheitsnachweis, etwa einen Scan des Personalausweises, eine Zulassungsbescheinigung, einen Mietvertrag oder einen Gehaltsnachweis. Diese Daten sammeln sie, um sie später selbst zu missbrauchen oder zu verkaufen.

Beliebt sei es derzeit, das Videoident-Verfahren bei Jobsuchenden zu missbrauchen. Die Täter schalten dafür gefakte Stellenangebote bekannter Unternehmen, beispielsweise Tchibo oder der Deutschen Bahn, und bauen deren Bewerbungsportale nach. Sie bringen die Jobsuchenden dazu, das Videoident-Verfahren einer Bank zu nutzen, um sich vorgeblich im Online-Bewerbungsverfahren zu authentifizieren. In Wirklichkeit bestätigen die Opfer hier der Bank, dass sie ein Konto eröffnen wollen.

Die Täter stellen sich beim Schriftverkehr zwischen Videoident-Verfahren, Bank und Jobsuchenden. Alle von der Bank benötigten Unterlagen werden über die Täter geleitet, sodass die beiden anderen Parteien nichts davon mitbekommen: „Der Jobsuchende wird dann hingehalten oder letztendlich doch nicht ‚eingestellt‘. Dass in seinem Namen ein Bankkonto existiert, bemerkt er nicht oder erst, wenn die polizeilichen Ermittlungen gegen ihn laufen. Bereits wenige Tage und Wochen reichen den Tätern, um ein Konto zum Beispiel für Geldwäsche zu missbrauchen“, beschreibt das LKA.

Geweckte Begehrlichkeiten

Je mehr Geschäfte wir online abwickeln, je mehr Prozesse aus der Offline-Welt sich über unsere digitale Identität im Internet erledigen lassen, desto begehrenswerter werden die zugehörigen Daten. Und Kriminelle entwickeln immer ausgefeiltere Methoden, um sie zu ergattern. Sicherheitsbehörden mahnen derzeit verstärkt, dieses Problem ernstzunehmen. Die European Union Agency for Network and Information Security (ENISA) etwa kategorisierte in ihrem Jahresbericht die

Alptraum Handy-Wanze

Smartphone-Spionage-Apps als Stalker-Werkzeuge

Sie sind die Erfüllung der Träume von eifersüchtigen (Ex-)Partnern oder Stalkern: Komplett-Sets aus Handy-Spyware und Cloudservice ermöglichen es, Standortdaten, Chat-Verläufe, Fotos, Gespräche und vieles mehr in Echtzeit zu überwachen. Der Einsatz von FlexiSpy, mSpy und Co. ist verboten, doch das schert viele Kunden nicht.

Von Holger Bleich

Wenn Eifersucht im Spiel ist, schieben misstrauische Partner mitunter alle moralischen Bedenken beiseite. Dann werden Schubladen durchwühlt, Freunde heimlich befragt oder gar Detektive engagiert. Steht die ungeteilte Zuneigung in Frage, führt der Argwohn dazu, dass der legitime Anspruch der oder des Liebsten auf Privatsphäre mit Füßen getreten wird. Niedere Instinke verdrängen die Vernunft.

Genau auf diese Instinkte setzen dubiose Anbieter von Spionage-Apps für Smartphones, und das offenbar sehr erfolgreich: „Wenn Sie in einer festen Beziehung sind, haben Sie ein Recht zu wissen!“ So wirbt der thailändische App-Hersteller Vervata für sein bedienungsfreundliches Handy-Trojaner-Set FlexiSpy. Nachdem man knapp 200 US-Dollar überwiesen hat, kann man drei Monate lang „lautlos alle Unterhaltungen, Standorte, und Nutzerverhalten eines Smartphones von sämtlichen Webbrowsern aus“ überwachen, lockt Vervata auf seiner Homepage.

Offensichtlich lockt er auch hierzulande erfolgreich: Geleakte Kundendaten aus den letzten Jahren zeigten, dass Vervata allein in Deutschland über 1000 zahlende Kunden hat. Das Online-Magazin Vice bekam diese Daten in die Finger. Man habe unter anderem „Rechtsanwälte, Firmengründer, Mitarbeiter von Reinigungsfirmen, Sicherheitsunternehmen, Party-Veranstalter, Friseurinnen und Internisten“, gefunden, berichtete Vice. Die Mehrzahl der Kunden seien Männer, doch immerhin mehr als ein

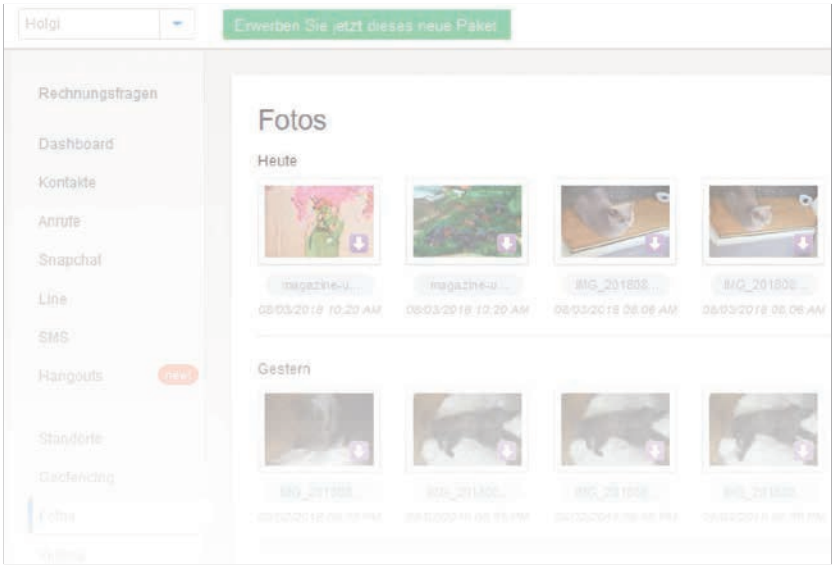
ter jedem einzelnen Account eines oder gar mehrere Schicksale von Personen stehen, deren Privat- und vielleicht auch Intimsphäre über eine Handy-Wanze ausspioniert werden, lässt das erschaudern. Hinzu kommt, dass das Urgestein FlexiSpy mittlerweile zig Mitbewerber hat, die ebenso um die Gunst von eifersüchtigen Ehepartnern, Stalkern, übersorgenden Eltern oder kontrollsüchtigen Arbeitgebern buhlen. Der populärste davon ist mSpy des US-amerikanischen Herstellers My Spy, der mindestens eine ähnlich große Kundenzahl wie Vervata haben dürfte und mit lediglich 100 Euro pro drei Monaten vergleichsweise günstig daherkommt.

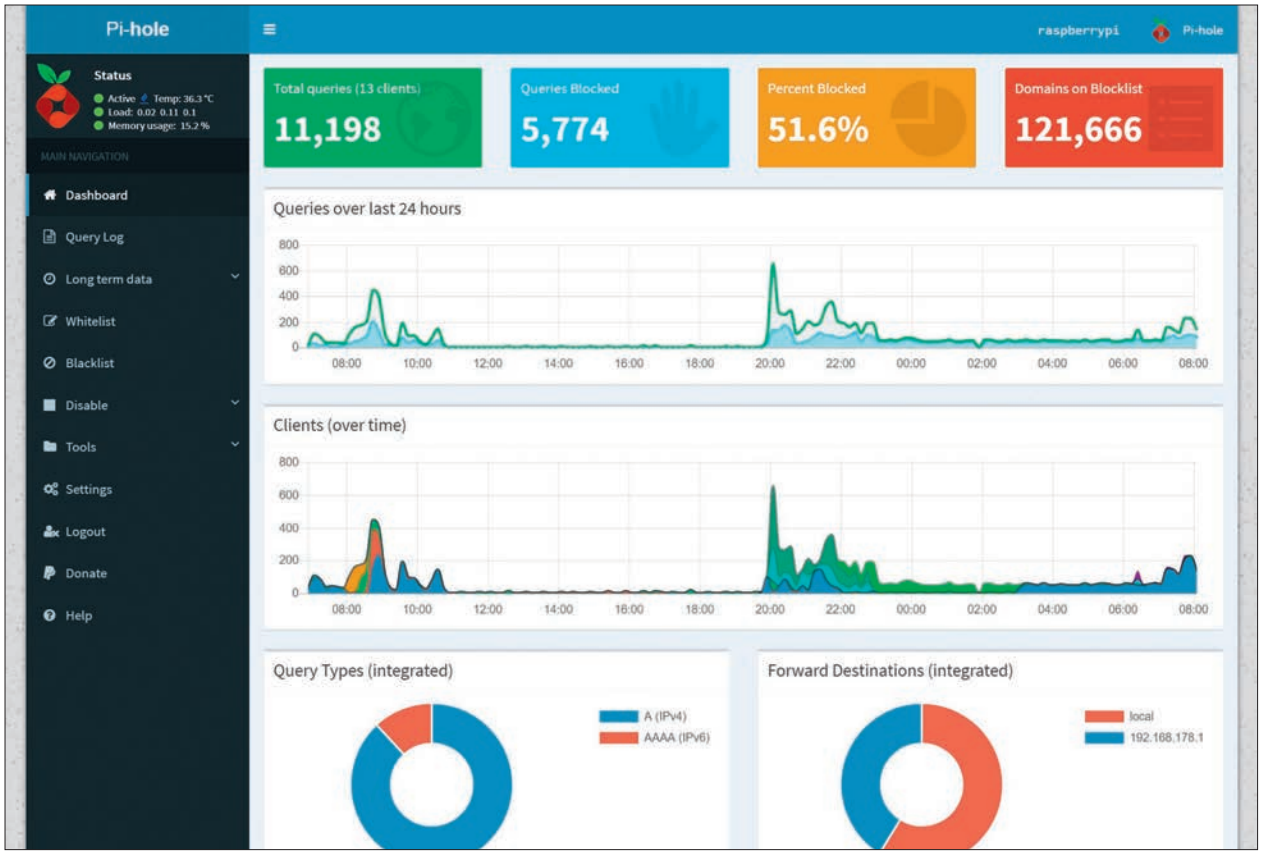
Der Funktionsumfang beider Trojaner-Services unterscheidet sich nicht erheblich. Beide bieten nur bei gerooteten Android-Smartphones vollen Remote-Zugriff. Die versteckte Installation auf nicht gerooteten Android-Geräten beschränkt Möglichkeiten und erleichtert Opfern das Aufspüren der Spionage-App (siehe S. 112). Vervata unterstützt iOS, allerdings wegen der restriktiven Rechte auf Apple-Geräten nur mit Jailbreak. My Spy bietet dagegen mSpy auch für aktuelle iOS-Versionen ohne Jailbreak an.

Wege aufs Handy

Die Anmeldung und Bezahlung bei den Services klappt problemlos, sofern man der englischen Sprache mächtig ist: Um hiesige Kunden anzulocken, scheinen alle Werbetexte mittels Translator-Services in radebrechendes Deutsch übersetzt worden zu sein, an vielen Stellen haben Vervata und My Spy ganz drauf verzichtet. Die Spyware-Lizenzen gestatten es lediglich, ein einziges Gerät zu verwanzen. Möchte der Stalker ein zweites Gerät anmelden, muss er das bisherige abmelden oder eine zweite Lizenz erwerben.

Die Spionage-Software landet je nach Betriebssystem auf unterschiedlichen Wegen auf dem Handy. Bei ungerooteten Android-Versionen etwa installiert man das APK-Paket entweder via USB oder über den Download mit dem Browser. Erforderlich ist auf jeden Fall der physische, entsperrte Zugang zum Gerät. Die Anbieter erläutern mit Schritt-für-Schritt-Anleitungen, welche Sicherheitsbarrieren und Stealth-Modi aktiviert werden müssen, damit die App nicht sofort vom Betriebssystem entdeckt wird. mSpy nutzt auf iPhones ohne Jailbreak zur Datenausleitung das iCloud-Backup. Der Möchtegern-Spion muss also die





Filterbeere

Schadcode und Werbung mit Raspberry Pi und Pi-hole filtern

Manche Dinge möchte man von vornherein aus dem Internetverkehr fernhalten: etwa Kryptogeld-Sauger, Phishing-Seiten, Tracking-Code und aggressive Werbeanzeigen. Pi-hole filtert so was gleich fürs ganze (W)LAN heraus. Es lässt sich leicht installieren und bequem per Browser konfigurieren.

Von Ronald Eikenberg

Pi-hole funktioniert wie ein schwarzes Loch im Netzwerk, das schädliche und nervige Inhalte verschluckt – daher der Name. Die technische Grundlage ist schnell erklärt: Pi-hole sitzt als DNS-Proxy zwischen den Clients im LAN und dem DNS-Server des Providers. Anhand von Filterlisten entscheidet der Proxy, welche DNS-Anfragen er an den DNS-Server weiterleitet und welche er blockiert. Fragt etwa ein Client nach der IP-Adresse von heise.de, leitet der Proxy die Anfrage durch und sendet die darauffolgende Antwort mit den IP-Adressen 193.99.144.80 (IPv4) sowie 2a02:2e0:3fe:1001:302:: (IPv6) anschließend an den Client zurück.

Möchte der Client jedoch die IP-Adresse zu einer Domain erfahren, die auf einer schwarzen Liste steht, beantwortet der Proxy die Anfrage mit seiner eigenen IP-Adresse. Versucht der Client daraufhin, eine HTTP-Verbindung dorthin aufzubauen, liefert Pi-hole eine Website mit dem Hinweis zurück, dass der Zugriff blockiert wurde. Der DNS-Proxy filtert Verbindungen auf diese Weise effektiv, ohne dass der gesamte Datenverkehr umgeleitet werden muss – eine Beeinträchtigung der Performance ist nicht spürbar. Pi-hole kümmert sich auf Wunsch zentral um alle Clients im lokalen Netz; von PCs über Smartphones bis hin zu Smart-TVs und IoT-Geräten. Eine Software-Installation auf den Clients ist dafür nicht nötig.

Das Pi-hole-Projekt erfindet das Rad nicht neu, sondern setzt auf verbreitete Open-Source-Tools wie den DNS-Server dnsmasq und den Webserver lighttpd. Zum Filtern nutzt es etablierte Blacklists, auf denen insgesamt über 100.000 Domains stehen – zumeist von Werbefirmen.

Die Installation und Konfiguration von Pi-hole übernimmt ein Setup-Skript. Es bringt den DNS-Filter in wenigen Schritten an den Start und setzt keine tiefergehenden Netzwerktechnik- oder Linux-Kenntnisse voraus. Die wichtigsten Einstellungen wie die Verwaltung der Filterlisten nimmt man anschließend über ein übersichtliches Webinterface vor. Dieses liefert auch interessante Statistiken über die DNS-Anfragen der Clients. Wer tiefer in die Materie einsteigen möchte, kann das offene Do-it-yourself-System nach Gusto modifizieren. Pi-hole ähnelt in seiner Funktionsweise der in c't 21/17

auf Seite 158 vorgestellten Konfiguration mit dem DNS-Server Unbound, ist jedoch deutlich einsteigerfreundlicher.

Bei den Anforderungen an die Hardware ist Pi-hole genügsam: Es ist für den Einsatz auf einem Raspberry Pi mit mindestens 512 MByte RAM ausgelegt, läuft aber auch auf anderen Linux-Maschinen unter Ubuntu, Debian, Fedora oder CentOS. Es reicht ein altes Raspi-Modell, das sich möglicherweise noch in irgendeiner Schublade findet. Dieser Artikel beschreibt die Einrichtung auf dem Raspi in einem Fritzbox-Netz. Wer auf Docker setzt, findet unter ct.de/wkhf ein Pi-hole-Image, das etwa auch erweiterbare NAS von QNAP, Synology & Co. zum filternden DNS-Proxy macht. Wir haben allerdings arg mit der IPv6-Inbetriebnahme in solchen Szenarien gekämpft und können diese Betriebsweise deshalb nicht empfehlen.

Raspi-Schnellstart

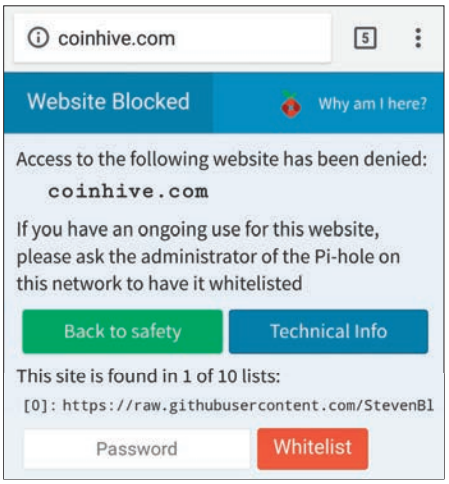
Ein Raspberry Pi für Pi-hole ist schnell an den Start gebracht. Haben Sie bereits einen Raspi konfiguriert, können Sie direkt zum Abschnitt „Pi-hole installieren“ springen. Laden Sie zunächst die aktuelle Raspbian-Version herunter und entpacken Sie das Image. Für Pi-hole genügt das aufs Nötigste reduzierte Raspbian Stretch Lite. Schreiben Sie das Raspbian-Image anschließend auf eine mindestens vier GByte große Speicherkarte, die Sie für diesen Zweck abgestellt haben – deren ursprünglicher Inhalt geht verloren. Unter Windows kommen Sie mit dem Win32 Disk Imager schnell ans Ziel: Wählen Sie unter „Image-Datei“ das entpackte Raspbian-Image und bei „Datenträger“ den Laufwerksbuchstaben des Kartenlesers. Der Knopf „Schreiben“ kopiert das Image auf die Karte. Nach dem Schreiben finden Sie auf der Karte eine FAT32-Partition namens „boot“. Damit Sie über SSH auf den Raspi zugreifen können, legen Sie dort eine leere Datei namens „ssh“ an.

Da DNS latenzempfindlich ist, sollten Sie den Raspberry nach Möglichkeit über LAN mit Ihrem Netzwerk verbinden. Wenn es nicht anders geht – etwa, weil Sie einen Raspbi Zero W ohne LAN-Schnittstelle nutzen –, können Sie den Minirechner wie folgt ins WLAN hängen: Legen Sie auf der boot-Partition einfach eine Datei namens wpa_supplicant.conf mit dem folgenden Inhalt an:

```
ctrl_interface=DIR=/var/run/wpa_↵
    ↳supplicant GROUP=netdev
update_config=1
country=DE

network={
    ssid="<SSID Ihres WLAN>"
    psk="<WLAN-Passwort>"
    key_mgmt=WPA-PSK
}
```

Topfen Sie nun die Speicherkarte in den Raspberry um. Nachdem Sie den Raspi mit Strom versorgt haben, fährt er hoch und ist innerhalb einer Minute im Heimnetz unter dem Hostnamen „raspberrypi“ erreichbar. Als Nächstes bauen Sie eine SSH-Verbindung mit dem Host auf, um Raspbian zu konfigurieren und Pi-hole zu installieren.



Versucht man, eine blockierte Domain zu kontaktieren, liefert Pi-hole eine Hinweisseite zurück.

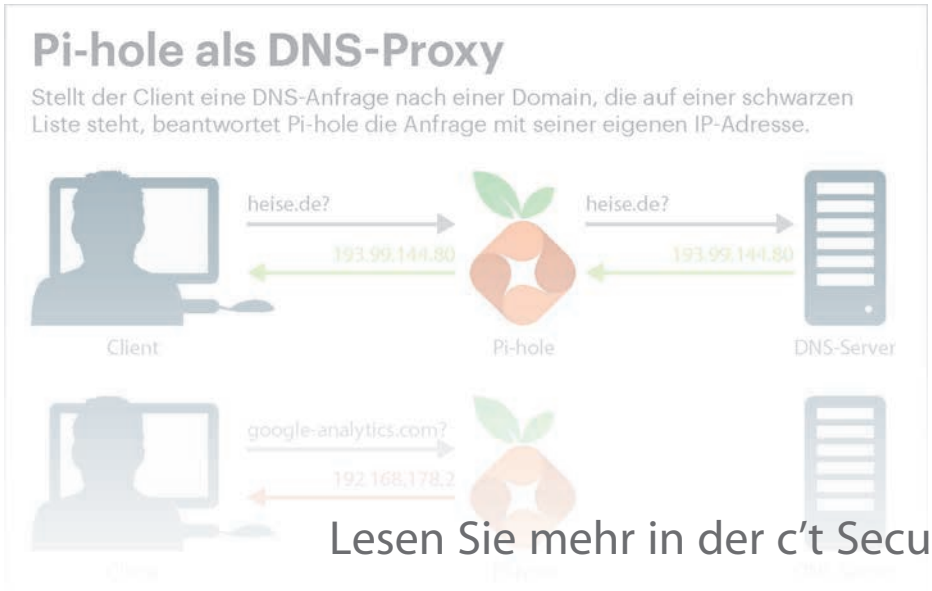
Bei Linux und macOS ist bereits ein SSH-Client an Bord, unter Windows 10 können Sie mit wenigen Klicks einen OpenSSH-Client aktivieren: Suchen Sie über das Startmenü nach „Apps & Features“, klicken Sie auf „Optionale Features verwalten/Feature hinzufügen“ und installieren Sie dort den „OpenSSH Client (Beta)“. Nach einem Neustart kennt die Eingabeaufforderung das ssh-Kommando. Der folgende Befehl baut die Verbindung zum Raspi auf: `ssh pi@raspberrypi`

Geben Sie das vorkonfigurierte Passwort „raspberry“ ein und Sie sind als Standard-User pi angemeldet. Als Erstes ändern Sie das Standardpasswort mit `passwd`. Sparen Sie nicht beim Passwort, denn jeder, der es kennt und sich im gleichen Netz befindet, kann sich an Ihrem Raspi anmelden und ihn via `sudo` mit Root-Rechten beliebig manipulieren – und damit auch den Internetverkehr analysieren, umleiten und fälschen. Wählen Sie also ein möglichst langes Kennwort und notieren Sie es in Ihrem Passwort-Manager.

Danach bringen Sie Betriebssystem und Komponenten mit `sudo apt-get update` und `sudo apt-get upgrade` auf den aktuellen Stand. Das kann eine Viertelstunde dauern; danach ist der Raspi startklar.

Pi-hole installieren

Die Installation von Pi-hole geht leicht von der Hand. Die Entwickler bieten ein Installations-Skript an, das Sie mit einem



Sicherheits-Checklisten

So viel Schutz muss sein

Zum Absichern von PCs, Smartphones, Routern & Co. kann man beliebig viel Aufwand betreiben – für ein gesundes Maß an Sicherheit reichen jedoch meist wenige Handgriffe. Mit unseren Sicherheits-Checklisten können Sie Ihre Technik schnell und einfach vor den größten Bedrohungen schützen.

Von Ronald Eikenberg

Die meisten Gefahren des digitalen Lebens sind vorhersehbar – und wer sich gezielt davor schützt, hat wenig zu befürchten. Dafür sind nur wenige Schritte nötig, die wir für Sie in unseren Sicherheits-Checklisten zusammengetragen haben. Mit den insgesamt vierzehn Checklisten sichern Sie im Handumdrehen Ihre Rechner, Smartphones, Router, Online-Accounts et cetera ab. Und natürlich auch die von Freunden, Verwandten und Kollegen. Alles, was Sie brauchen, sind Bordmittel und fünf Minuten Zeit.

Weniger ist mehr

Getreu dem Motto „Weniger ist mehr“ haben wir einige festgetretene Sicherheitsempfehlungen bewusst weggelassen oder kurz gehalten. Dazu zählt das Thema Virenschutz, das inzwischen eine deutlich geringere Bedeutung als noch vor wenigen Jahren hat. Die Annahme etwa, dass zu einem sicheren Windows-System die Installation eines Virenscanners oder gar einer Internet-Security-Suite gehört, ist zumindest im Fall von Windows 10 (S. 138) überholt: Microsoft hat den mitgelieferten Virenschutz Windows Defender im Laufe der Zeit erheblich verbessert.

Das Bordmittel kann inzwischen locker mit nachinstallierbaren Schädlingsbekämpfern mithalten – ohne mit Abogebühren oder Werbeeinblendungen zu nerven. Auch unter Android können Sie sich die Installation einer Virenscan-App sparen, wenn Sie sich an unsere Checkliste (S. 140) halten.

Update muss sein

Ein wiederkehrendes Thema in den Checklisten sind Updates: Klemmt irgendwo ein Update, können gefährliche Sicherheitslücken klaffen. Dann reicht schon der Besuch einer vermeintlich harmlosen Webseite, um sich einen fiesen Erpressungstrojaner ins Haus zu holen.

Dies ist nur eine von vielen Situationen, in denen Ihnen veraltete Software zum Verhängnis werden kann. Eine zügige Installation von Sicherheits-Updates ist daher essenziell – nicht nur bei Windows, macOS, Android und iOS, sondern insbesondere auch bei Smart-Home-Geräten, Routern und NAS.

Passwort-Tricks

Auch das Thema Passwörter zieht sich wie ein roter Faden durch die folgenden Seiten. Passwörter sind unbequem, jedoch oft der einzige Schutz, der zwischen Online-Angreifern und Ihrem digitalen Leben steht. Deshalb erfahren Sie auf Seite 153, wie Sie mit minimalem Aufwand ausreichend sichere Kennwörter einsetzen. Der größte Fehler, den man machen kann, ist das gleiche Passwort an verschiedenen Stellen einzusetzen. Man erschafft damit einen Generalschlüssel, der in den falschen Händen viel Schaden anrichten kann.

Oft gibt es Schutzfunktionen wie die sogenannte Zwei-Faktor-Authentifizierung, mit denen Sie durch wenige Klicks für einen erheblichen Gewinn an Sicherheit sorgen können. Ist der Schutz aktiv, sind Ihre Accounts selbst dann noch sicher, wenn der Angreifer das korrekte Passwort kennt. Sie finden in dieser Ausgabe konkrete Tipps zum Zwei-Faktor-Schutz von Google (S. 145), Social-Media-Accounts (S. 146) und WhatsApp (S. 144).

Ein weiterer wichtiger Punkt des Schutzkonzepts sind Backups: Denn die Wahrscheinlichkeit, dass früher oder später ein Speichermedium ausfällt oder dessen Inhalt von einem Erpressungstrojaner in Beschlag genommen wird, ist vielleicht nicht hoch – aber doch größer als null. Um dann nicht mit leeren Händen dazustehen, sollten Sie sich auf diesen Tag vorbereiten und Sicherungen Ihrer wichtigsten Dateien erstellen. Auf Seite 152 erfahren Sie, wie das mit minimalem Aufwand geht. Auch vor neugierigen Mitmenschen können Sie sich leicht schützen. An den passenden Stellen finden Sie Tipps, wie Sie den Zugriffsschutz richtig konfigurieren und Ihre Daten verschlüsseln.

Los gehts!

Der beste Zeitpunkt, die Sicherheits-Checklisten durchzugehen, ist jetzt! Schnappen Sie sich Ihr Smartphone oder Ihren Rechner und überprüfen Sie, ob Sie alle Punkte der dazu passenden Checkliste abhaken können – oder ob noch Nachbesserungsbedarf besteht. Im letzteren Fall genügen wenige Handgriffe, um die Schlupflöcher zu schließen. Animieren Sie auch Ihr Umfeld, sich fünf Minuten Zeit zu nehmen, um Online-Ganoven & Co. im entscheidenden Moment einen Schritt voraus zu sein. *(rei@ct.de)* c't

Checklisten als Booklet im PDF-Format:
ct.de/w3rq

Sicherheit für alle

In dieser c't-Ausgabe finden Sie ein handliches Booklet mit leicht verständlichen Kurzfassungen aller Sicherheits-Checklisten. Geben Sie es gern an Familienmitglieder, Freunde und Kollegen weiter, damit auch diese ihre Technik schützen können. Oder heben Sie es einfach auf – die nächste Neuanschaffung, die sicher konfiguriert werden muss, kommt bestimmt. Wir bieten das Booklet unter ct.de/check2018 auch