c't

SECURITY-TIPPS

So schützen Sie sich vor Hackern und Viren

Hacking-Tools: Gefährlich und nützlich

Von Angreifern lernen • Tools für Einsteiger und Profis
Hacking-Stick selbst gebaut

Sicher surfen mit VPN

Was die Technik bringt
Elf Anbieter im Vergleich

Heimnetz absichern

Fritzbox & NAS richtig konfigurieren
Eigenes WLAN überwachen

Online-Konten schützen

Gut abgesichert dank zweitem Faktor
Sicherheits-Sticks im Test

12 Security-Checklisten

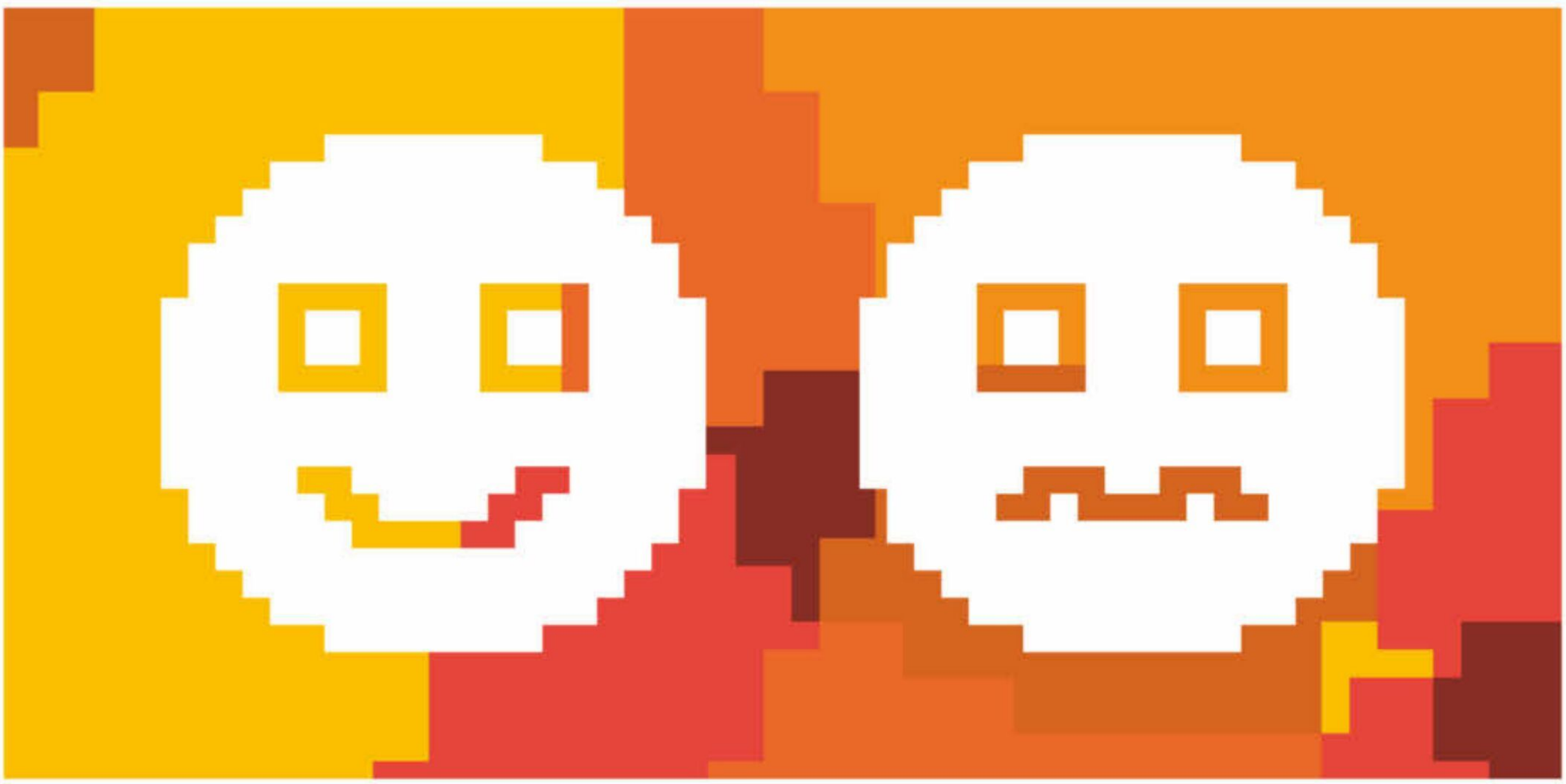
Die wichtigsten Tipps auf einen Blick
PC, Smartphone, Router & Co. schnell absichern

facebook.com/ctspecials

€ 14,90
CH CHF 27.90
AT € 16,40
LUX € 17,10

4 195957 614908 05

Die Frage ist nicht, ob ein Cyberangriff kommt. Sondern ob Sie vorher mit uns sprechen. Oder danach.



pwc

Trust in Transformation: Vertrauen Sie auf einen Partner, der bei der Transformation Ihres Unternehmens die passenden Cyber-Security-Lösungen mitdenkt, implementiert und kontinuierlich begleitet:
www.pwc.de/cybersecurity

Editorial

Liebe Leserinnen und Leser,

Hacker werden in Filmen meist als Genies dargestellt, die allein mit der Kommandozeile und ihrer Kreativität jedes System knacken. Die Wirklichkeit sieht profaner aus: Selbst die besten Hacker setzen Software ein, die ihnen einen großen Teil ihrer Arbeit abnimmt. Viele der Anwendungen sind frei verfügbar – auch Sie können sie herunterladen und damit zum Hacker werden.

Wir stellen Ihnen die spannendsten Hacking-Tools vor und helfen Ihnen bei den ersten Schritten. Die Programme sind nicht nur für fragwürdige Zwecke zu gebrauchen. Sie helfen auch dann, wenn man sein Windows-Kennwort vergessen hat oder das eigene Netzwerk überwachen will. Wer einmal mit den Hacking-Tools herumgespielt hat, versteht auch besser, wie man sich vor Angriffen schützt – los geht es ab Seite 104.

Sie haben dafür gerade nicht genug Zeit? Dann empfehlen wir Ihnen unsere Security-Checklisten (ab Seite 6). Diese verzeichnen die wichtigsten Handgriffe, mit denen Sie Ihren PC, Ihr Smartphone, Ihre Online-Accounts et cetera vor Online-Gangstern und Schnüfflern schützen. Es dauert in der Regel nur wenige Minuten, die Tipps einer Liste umzusetzen.

Danach können Sie tiefer in die Materie einsteigen. In der Rubrik „Heimnetz absichern“ erklären wir ausführlich, wie man Fritzboxen und Netzwerkspeicher (NAS) einbruchsicher konfiguriert und das eigene WLAN überwacht. Warum die Zwei-Faktor-Authentifizierung für Online-Accounts nach wie vor unersetzlich ist, erfahren Sie in den Artikeln ab Seite 62. Außerdem testen wir Gadgets, die das Konzept sicher und bequem umsetzen. Ab Seite 84 erklären wir, was VPN-Dienste leisten (und was nicht!) und vergleichen elf Anbieter. Typische Sicherheitsprobleme bei Servern und in Webanwendungen wie WordPress zeigen wir ab Seite 138 – damit Sie aus den Fehlern anderer lernen können.

Christian Wölbert

Inhalt

DIE C’T-SECURITY-CHECKLISTEN

IT-Sicherheit ganz konkret: Unsere Checklisten zeigen Schritt für Schritt, wie man PC, Smartphone, Anwendungen und Online-Konten vor Schnüfflern, Erpressern und anderen Online-Gangstern schützt.

6 Die c’t-Security-Checklisten
8 Mobiles Arbeiten
10 Windows
12 Smartphone
14 WLAN-Router
16 E-Mail
18 Messenger
20 Browser
22 Social Media
24 Onlinebanking
26 Backups
28 Passwörter & Accounts
30 Server & Hosting

HEIMNETZ ABSICHERN

Angreifer klopfen auch private Router automatisiert auf Schwachstellen ab. Mit unseren Tipps schottet man Fritzboxen und NAS dagegen ab und lernt, wie man das eigene WLAN auf verdächtige Aktivitäten überwacht.

34 Fritzboxen sicher betreiben
44 NAS sicher betreiben
52 Netzwerk-Abklopfer
54 WLAN-Alarmanlage

ONLINE-ACCOUNTS SCHÜTZEN

Das Mittel der Wahl gegen Daten- und Identitätsdiebstahl ist nach wie vor die Zwei-Faktor-Authentifizierung. Wir erklären das Prinzip und testen dafür geeignete Hardware wie FIDO2-Sticks.

62 Logins absichern mit Authenticator
66 2FA-Generator Reiner SCT Authenticator
69 Offener FIDO2-Schlüssel
70 Universal-Sicherheitsschlüssel TrustKey
71 FIDO2-Stick mit Fingerabdrucksensor
72 DiceKeys: Passwortgenerator mit Würfeln
76 Passwortmanager in Eigenregie hosten

SICHER SURFEN MIT VPN

Mit einem Virtual Private Network verschlüsselt man den Datenverkehr und surft so zum Beispiel auch in fremden WLANs sicher. Doch im VPN-Markt tummeln sich neben seriösen auch viele unseriöse Anbieter.

84 Schutz oder trügerische Sicherheit?
90 Elf VPN-Anbieter im Vergleich
98 Übersicht gängiger VPN-Varianten

MIT HACKING-TOOLS PROBLEME LÖSEN

Einfach mal ein bisschen hacken: Wir haben die spannendsten Hacking-Tools für Einsteiger und Profis herausgesucht und erklären, wie man sie zu hehren Zwecken einsetzt – zum Beispiel, um das eigene Passwort zu knacken oder aus dem System auszulesen.

104 Hacking-Tools als Problemlöser
106 Nützliche Hacking-Tools für den Alltag
114 Hacking-Werkzeug für Fortgeschrittene
122 Kali Linux auf USB-Stick einrichten
128 Rechtliche Aspekte bei Hacking-Tools
134 NitroPC: Mini-PC mit Security-Plus

SERVER & WEBANWENDUNGEN SICHERN

Täglich kommen Serverbetreibern aus aller Welt persönliche Daten von Nutzern und andere heikle Informationen abhanden oder die Daten werden zwecks Erpressung verschlüsselt. Aus solchen Fällen lässt sich lernen.

138 IoT und Industrie ungeschützt im Netz
142 IoT ungesichert im Netz
148 Hintertür zu Wordpress
152 Newsletter als Spam-Schleudern
156 Unachtsamer Phisher enttarnt
160 Datenlecks bei Test- und Impfterminen
166 Ransomware-Attacke gezielt vereiteln

ZUM HEFT

3 Editorial
170 Impressum
170 Inserentenverzeichnis

Die c’t-Security-Checklisten

Seien Sie Hackern einen Schritt voraus: Mit unseren Checklisten sichern Sie Smartphone, Rechner, WLAN-Router, Online-Accounts und vieles mehr ab. Das ist einfach und dauert meist nur wenige Minuten. So viel Zeit muss sein!

Von **Ronald Eikenberg**

Bild: Andreas Martini

Extras für c’t-Leser: PDF-Booklet und Sheriffstern

Eine Kurzfassung der c’t-Security-Checklisten können Sie als PDF-Booklet unter ct.de/check2022 kostenlos herunterladen (siehe auch auf der rechten Seite „Teilen erwünscht“).

Den auf dem Booklet abgebildeten c’t-Sheriffstern gibt es in limitierter Auflage als echt vergoldeten, geprägten 3D-Pin zum Anheften. Der Stern mit einem Durchmesser von etwa 45 Millimeter kostet inklusive Versand 7,90 Euro und wird in einem auf der Oberseite durchsichtigen Jewel-Case zum Aufklappen geliefert.

Wer einen (oder mehrere) haben möchte, schickt bitte eine formlose Mail mit der gewünschten Anzahl an sheriffstern@ct.de. Wir liefern, solange der Vorrat reicht.

Die Checklisten im Überblick	6	Browser	20
Mobiles Arbeiten	8	Social Media	22
Windows	10	Onlinebanking	24
Smartphone	12	Backups	26
WLAN-Router	14	Passwörter & Accounts	28
E-Mail	16	Server & Hosting	30
Messenger	18		

Die Grenze zwischen Homeoffice und Privatleben verläuft längst fließend – und durch die neu gewonnene Freiheit bei der Wahl des Arbeitsplatzes, dem hybriden Arbeiten, ist das für viele die neue Normalität. Höchste Zeit also, die Schutzschilde der beteiligten Rechner, Router, Smartphones, Online-Accounts und so weiter zu überprüfen und nachzubessern. Auch wenn Sie Ihre Technik ausschließlich beruflich oder privat nutzen, empfiehlt sich ein regelmäßiger Security-Check: Denn die Bedrohungslage ändert sich täglich und wer darauf nicht reagiert, macht es Online-Ganoven leichter als nötig. Deshalb möchten wir Sie auch in diesem Jahr wieder anstiften, wenige Minuten Ihrer Zeit in die eigene IT-Sicherheit zu investieren.

Länger dauert es meist nicht, Lücken im Schutzkonzept zu erkennen und zu schließen. Auch wenn die Verteidigung gegen Hacker angesichts von Horrormeldungen über immer ausgefeiltere Angriffe aussichtslos wirken mag, sollten Sie die Flinte keinesfalls ins Korn werfen: Die allermeisten Online-Ganoven nutzen keine unaufhaltsamen Hightech-Trojaner, sondern spekulieren auf Lücken in Ihrem Basisschutz und auf Ihre Unachtsamkeit.

Besonders große Aufmerksamkeit sollten Sie Ihren beruflich genutzten Geräten und Accounts widmen. Wer weiterhin im Homeoffice arbeitet oder gar flexibel an einem Ort der Wahl, der muss sicherstellen, dass alles nach Stand der Technik abgesichert ist. Fängt man sich einen Trojaner ein, gerät dann nämlich auch schnell der Arbeitgeber in die Bredouille. Der Schädling wird sich mit hoher Wahrscheinlichkeit nicht nur auf dem infizierten Rechner umsehen, sondern auch im Intranet des Unternehmens.

Vorbereitet sein

Damit Sie den Hackern im entscheidenden Moment einen Schritt voraus sind, finden Sie in dieser c't die aktualisierte Neuauflage unserer Security-Checklisten. Die Redaktion hat die aktuelle Bedrohungslage analysiert und die bewährten Checklisten darauf zugeschnitten. Darunter ist jetzt auch eine mit den wichtigsten Handgriffen für das mobile und hybride Arbeiten an wechselnden Orten (siehe Seite 8). Wie gewohnt sind die Schutzempfehlungen thematisch gegliedert, sodass Sie sich die Checklisten leicht individuell zusammenstellen können.

Doch auch wer alles richtig macht und seine Systeme bestmöglich vernagelt, muss damit rechnen, früher oder später Bekanntschaft mit Hackern zu machen – entweder direkt oder indirekt, etwa nachdem ein genutzter Onlinedienst kompromittiert wurde oder eine bisher vertrauenswürdige Software ungefragt ein verseuchtes Update installiert hat. Spielen Sie den Ernstfall gedanklich durch und treffen Sie geeignete Präventivmaßnahmen.

Gut abgesichert

Falls zum Beispiel Ihre Passwörter nach einem Trojanerbefall im Darknet kursieren, dann ist das halb so schlimm, wenn Sie im Vorfeld bei allen wichtigen Onlinediensten die Zwei-Faktor-Authentifizierung aktiviert haben. Ein unbefugter Login-Versuch scheitert dann an der Abfrage des Zwei-Faktor-Codes, den nur Sie per App generieren können oder per SMS zugeschickt bekommen. Mehr dazu finden Sie auf Seite 28.

Der beste Schutz vor Erpressungstrojanern sind aktuelle Backups, mit denen Sie Ihr digitales Hab und Gut im Notfall ohne Lösegeldzahlung einfach wiederherstellen können. Wichtig ist, dass Sie diese Wiederherstellung auch tatsächlich getestet haben. Außerdem dürfen die Backups nicht ständig per Kabel oder Netzwerk erreichbar sein, damit sie der Trojaner nicht ebenfalls verschlüsseln kann – ein USB-Stick ist besser als nichts. Auf Seite 26 erfahren Sie, wie Sie schnell und einfach ein trojanersicheres Backup einrichten.

Teilen erwünscht

Zum Konzept unserer Checklisten gehört, dass sie verständlich sind und leicht umzusetzen. Alle sollten von einem Grundschutz vor Hackern profitieren. Sie können uns dabei unterstützen! Reichen Sie die Checklisten gern an Freunde, Verwandte und Kollegen weiter. Die wichtigsten Handgriffe haben wir wieder in einem PDF-Booklet zusammengefasst, das sich hervorragend zum Weiterverschicken eignet. So müssen Sie sich nicht von Ihrem Sonderheft trennen und können trotzdem etwas Gutes tun.

Mit dieser Gedächtnisstütze können Sie schnell weiterhelfen, wenn Sie mal wieder gefragt werden, wie man PC, Smartphone oder Instagram am besten vor Hackern schützt. Sie können das PDF einfach unter ct.de/check2022 herunterladen. Dort kann auch ein begrenztes Kontingent des gedruckten Booklets bestellt werden, zum Beispiel für Awareness-Maßnahmen in Unternehmen, Banken und Behörden.

So, genug der Vorrede – jetzt gehts frisch ans Werk! (rei) c't

Booklet zum Download

ct.de/check2022

Security-Checkliste

Mobiles Arbeiten

Präsenzkultur ade: Nach Corona wollen Arbeitnehmer nicht mehr fünf Tage die Woche zurück ins Büro, schließlich lässt es sich daheim oder im Zug genauso gut arbeiten. Das wissen auch Angreifer und konzentrieren sich zunehmend auf die schlechter abgesicherten externen Arbeitsplätze.

Von **Andrea Trinkwalder**

Bild: Andreas Martini

☑ Solider Arbeitsplatz

Sichern Sie Ihren Homeoffice-Rechner und alle mobilen Arbeitsgeräte nach dem Stand der Technik. Dazu zählen regelmäßige Betriebssystem-Updates und ein Virenscanner (siehe S. 10). 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. Meiden Sie öffentliche WLAN-Hotspots, nutzen Sie stattdessen eine mobile Datenverbindung (4G / 5G).

Schützen Sie Ihre Geräte und Daten auch vor direkten, physischen Zugriffen von Unbefugten. Ein Dieb, der Ihr Notebook geklaut hat, darf nicht auch noch Ihre Daten erbeuten. Bei mobilen Rechnern sollte die Festplatte / SSD daher verschlüsselt sein, zum Beispiel mit BitLocker oder VeraCrypt. Das gilt auch für USB-Sticks und andere externe Datenträger, die das Haus verlassen. Defekte Speichermedien entsorgen Sie nicht selbst, sondern über die Firma. Nur dann ist gewährleistet, dass sensible Informationen sicher gelöscht werden und sich nicht rekonstruieren lassen.

Aktivieren Sie Ortungs- und Fernlöschfunktionen, wenn möglich. 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 kurz aus den Augen lassen (etwa unter Windows mit Windows+L). Am besten ist ein passwortgeschützter Bildschirmschoner, der sich nach kurzer Inaktivität automatisch aktiviert.

☑ 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 Cloud-Konten 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 möglich. Samsung-Handys etwa bieten auch innerhalb eines Accounts eine abgeschottete Umgebung (Sicherer Ordner).

☑ 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 Firmenoffice wechseln. Falls Daten doch mal lokal gespeichert werden müssen, richten Sie zumindest eine automatische Synchronisierung per Backup-Software ein. Verzichten Sie möglichst darauf, Dokumente auf USB-Sticks und externen Platten hin und herzutragen.

☑ Videochat

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

☑ Sicherer Draht

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.

Anrufern und Mails sollten Sie grundsätzlich skeptisch gegenüberstehen, denn Caller-IDs und Absender können gefälscht sein. Meldet sich etwa vermeintlich Ihr Lieblingsadmin oder Geschäftspartner telefonisch bei Ihnen, sollten Sie keine sensiblen Daten preisgeben und sich schon gar nicht auf eine Fernwartung einlassen. Rufen Sie bei geringstem Zweifel lieber unter der Ihnen bekannten Rufnummer zurück. Denn, man kann es sich nicht oft genug vergegenwärtigen: Der größte Schwachpunkt im Sicherheitssystem bleibt der Mensch. (atr) c't

Security-Checkliste

Windows

Auf Windows haben es Hacker besonders häufig abgesehen – schlicht, weil es so verbreitet ist. Die gute Nachricht ist, dass Sie sich bereits mit Bordmitteln vor den meisten Angriffen schützen können.

Von **Ronald Eikenberg**

Bild: Andreas Martini

☑ Updates installieren

Microsoft liefert regelmäßig Updates, die offene Sicherheitslücken in Windows schließen. Den aktuellen Stand der Dinge erfahren Sie, indem Sie „Nach Updates suchen“ ins Startmenü tippen. Die letzte Überprüfung sollte nicht länger als ein paar Tage her sein. Klicken Sie dort auf den Knopf, der ebenfalls mit „Nach Updates suchen“ beschriftet ist, wenn die Versorgung klemmt, „Jetzt installieren“ startet verfügbare Updates. Sorgen Sie unter „Erweiterte Optionen“ dafür, dass Sie auch „Updates für andere Microsoft-Produkte“ über Windows Update bekommen.

Alte Windows-Versionen versorgt Microsoft nicht mehr mit Sicherheits-Patches, wodurch das Angriffsrisiko steigt. Nutzen Sie daher am besten ein Windows mit dem derzeit aktuellen Funktions-Upgrade (etwa 21H1). Halten Sie auch Anwendungen wie Browser, Mail-Client, PDF-Viewer und Videoplayer aktuell.

☑ Daten-GAU vorbeugen

Ihre Daten sind auf der Systemplatte oder -SSD allein auf Dauer nicht gut aufgehoben, da diese jederzeit ausfallen kann. Zudem besteht die Gefahr, dass die Daten von einem Krypto-Trojaner verschlüsselt werden. Sorgen Sie vor und legen Sie Backups aller wichtigen Daten an. Im einfachsten Fall reicht es, die Daten auf einen USB-Datenträger zu kopieren (siehe S. 26).

☑ Virenschutz überprüfen

Ein Virenschutzprogramm kann Sie zwar nicht vor allen Gefahren schützen, doch vor vielen. Bei allen aktuellen Windows-Versionen ist der Windows Defender vorinstalliert, der inzwischen mit der Konkurrenz locker mithalten kann. Stellen Sie sicher, dass er aktiv ist und mit aktuellen Virensignaturen versorgt wird. Öffnen Sie hierzu „Windows-Sicherheit“ über das Suchfeld des Startmenüs und klicken Sie anschließend auf „Viren- & Bedrohungsschutz“. Ein manuelles Signaturupdate starten Sie mit „Nach Updates suchen“ (unter Windows 11 müssen Sie vorher noch auf „Schutzupdates“ klicken).

☑ Zugriffsschutz aktivieren

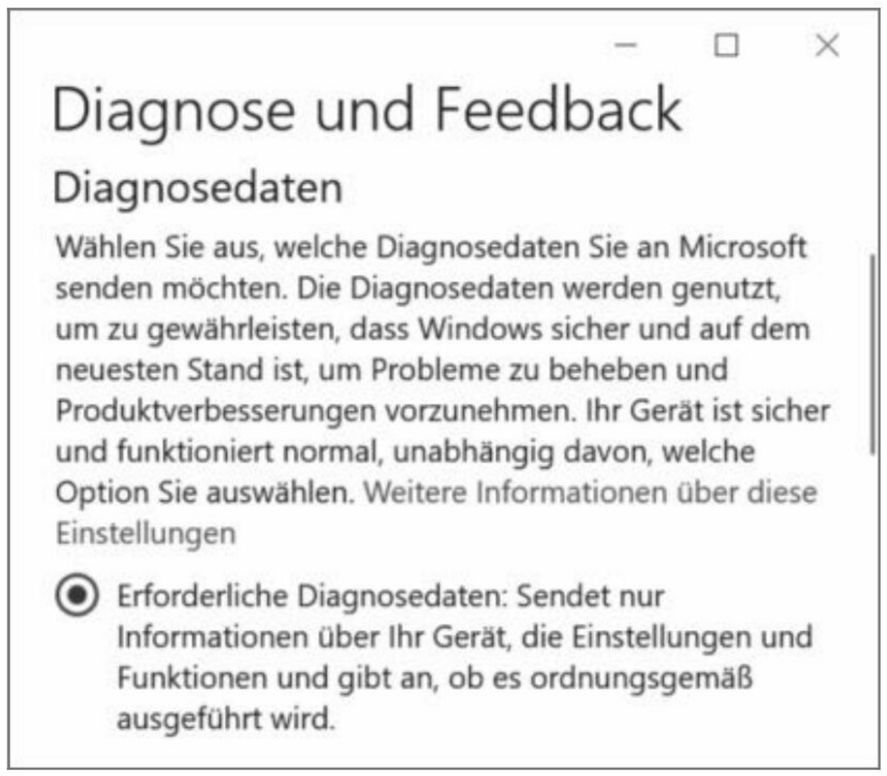
Ihr Rechner muss auch vor Angriffen von Personen, die sich dem Rechner nähern, geschützt werden. Im besten Fall verschlüsseln Sie die Festplatte oder SSD mit BitLocker oder unter der Home-Edition von Windows mit VeraCrypt [1]. So sind Ihre Daten – oder die Ihres Arbeitgebers – auch dann noch geschützt, wenn jemand an der Windows-Anmeldung vorbei direkt auf den Datenträger zugreift.

Schützen Sie Ihr Windows-Konto mit einem mindestens zehn Zeichen langen Passwort. Mit Windows Hello müssen Sie es nur selten eintippen, eine PIN reicht. Sperren Sie Ihren Rechner, wenn Sie ihn außer Augen lassen. Das klappt ganz fix mit der Tastenkombination Windows+L. Stellen Sie zudem ein, dass

sich Windows bei Inaktivität automatisch abriegelt, für den Fall, dass Sie das Sperren einmal vergessen. Öffnen Sie hierzu „Bildschirmschoner ändern“ über das Suchfeld des Startmenüs und setzen Sie das Häkchen „Anmeldeseite für Reaktivierung“. Das Feld „Wartezeit“ legt fest, nach wie vielen Minuten das System automatisch gesperrt wird.

☑ 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 sicher, dass unter „Diagnosedaten“ die Option „Erforderliche Diagnosedaten“ gewählt ist. Unter Windows 11 deaktivieren Sie hier stattdessen „Optionale Diagnosedaten senden“. Windows drängt Ihnen bei der Einrichtung das Microsoft-Konto auf, das eng mit der Cloud vernetzt ist. Nutzen Sie besser ein lokales Konto. Das klappt etwa, wenn Sie vor der Einrichtung die Netzwerkverbindung kappen [2]. (rei) c't



Die Übertragung von Diagnosedaten kann man Windows zwar nicht komplett austreiben, aber aufs Nötigste reduzieren.

Literatur

[1] Jan Schüßler, **Dicht und frei**, Windows-Partition mit VeraCrypt verschlüsseln, c't 17/2020, S. 162

[2] Axel Vahldiek, **Zurück in die Kiste!**, Windows ohne Microsoft-Konto nutzen, c't 13/2021, S. 28

Business-E-Mail für geschäftskritische Anwendungen und digitale Arbeitsplätze?

100 % DSGVO-konform?

Intelligent und ausfallsicher?

DIE SECURE EMAIL PLATFORM!

retarus.de/secure-email-platform

VIELE WICHTIGE FRAGEN. EINE GUTE ANTWORT.

retarus

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.

Von **Ronald Eikenberg**

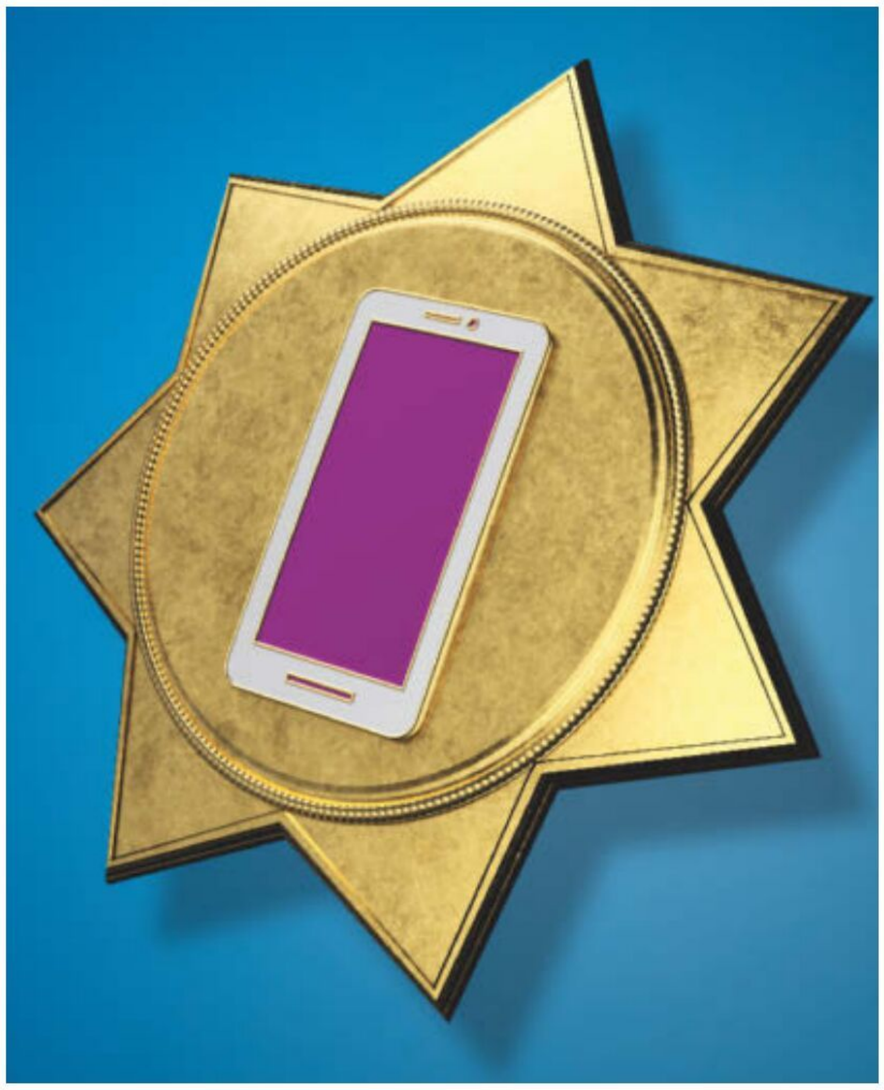


Bild: Andreas Martini

☑ Firmware-Updates

Ganz gleich, ob Sie Android oder iOS nutzen – achten Sie darauf, dass ein möglichst aktuelles Betriebssystem auf dem Gerät installiert ist. Betriebssystem-Updates schließen meist Sicherheitslücken, und wer nicht auf dem Laufenden ist, macht es Hackern leichter als nötig. Apple versorgt seine iPhones vorbildlich mit Updates: iOS 15 ist sogar noch für das sechs Jahre alte iPhone 6s erschienen. Bei Android ist die Lage durchwachsen, insbesondere bei preiswerten Smartphones versiegt der Update-Fluss oft nach kurzer Zeit.

Ob es ein Update gibt, können Sie über die Einstellungen überprüfen. Suchen Sie dort einfach nach „Update“ oder „Softwareaktualisierung“. Dort können Sie auch die Installation anstoßen. Android-Nutzer erfahren unter „Über das Telefon“ zudem das Android-Sicherheitspatch-Level, das besagt, von welchem Datum die installierten Sicherheits-Patches sind. Falls Sie ein Smartphone einsetzen, um das sich der Hersteller nicht mehr kümmert, sollten Sie mittelfristig über eine Neuanschaffung nachdenken. Informieren Sie sich vor dem Kauf, welche Hersteller ihre Geräte langfristig pflegen.

☑ 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 – ganz gleich ob Taschendieb oder neugieriger Kollege. Der Passcode sollte mindestens sechs Zeichen lang und nicht zu leicht 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, etwa nach einem Neustart. 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 Geräteherstel-

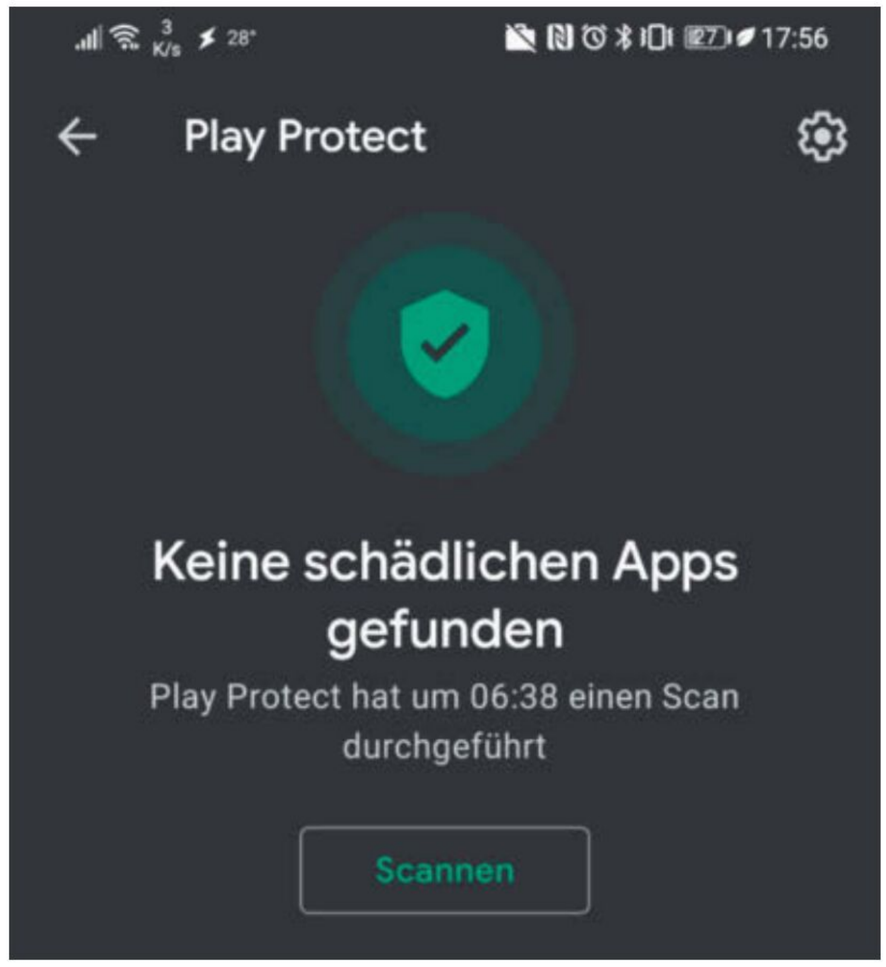
lern. Die Apps werden zumindest bei Apple und Google einem Sicherheitscheck unterzogen. Android-Nutzer, die eine App als APK-Installationspaket installieren möchten, sollten dieses nur direkt vom Entwickler der App beziehen. Stellen Sie unter Android sicher, dass der Cloud-Virenschutz Play Protect aktiv ist. Sie finden ihn im Menü des Play Store. iOS-Nutzer benötigen keinen Virenscanner.

☑ App-Berechtigungen

Überprüfen Sie vor Installation und Nutzung 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. Im Zweifel verzichten Sie lieber. 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 „Rooten“ (Android) und „Jailbreaking“ (iOS) kann man sich höhere Rechte auf dem Smartphone verschaffen und tiefgreifende Modifikationen am System vornehmen, die normalerweise nicht zulässig sind. Dadurch hebelt man jedoch auch essenzielle Schutzfunktionen aus, weshalb die meisten Nutzer besser damit bedient sind, das Gerät im ursprünglichen Zustand zu belassen. Hinzu kommt, dass zahlreiche Apps auf modifizierten Smartphones den Start aufgrund von Sicherheitsbedenken verweigern. (rei) c't



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

Security-Checkliste

WLAN-Router

Einrichtungsassistenten erledigen die Grundeinrichtung von WLAN-Routern schnell, aber Sicherheitsfunktionen für das Heimnetz lassen sie meist deaktiviert. Besonders die WLAN-Verschlüsselung braucht Ihre Aufmerksamkeit, auch wenn Ihr Router schon das neue WPA3 beherrscht.

Von **Dušan Živadinović**

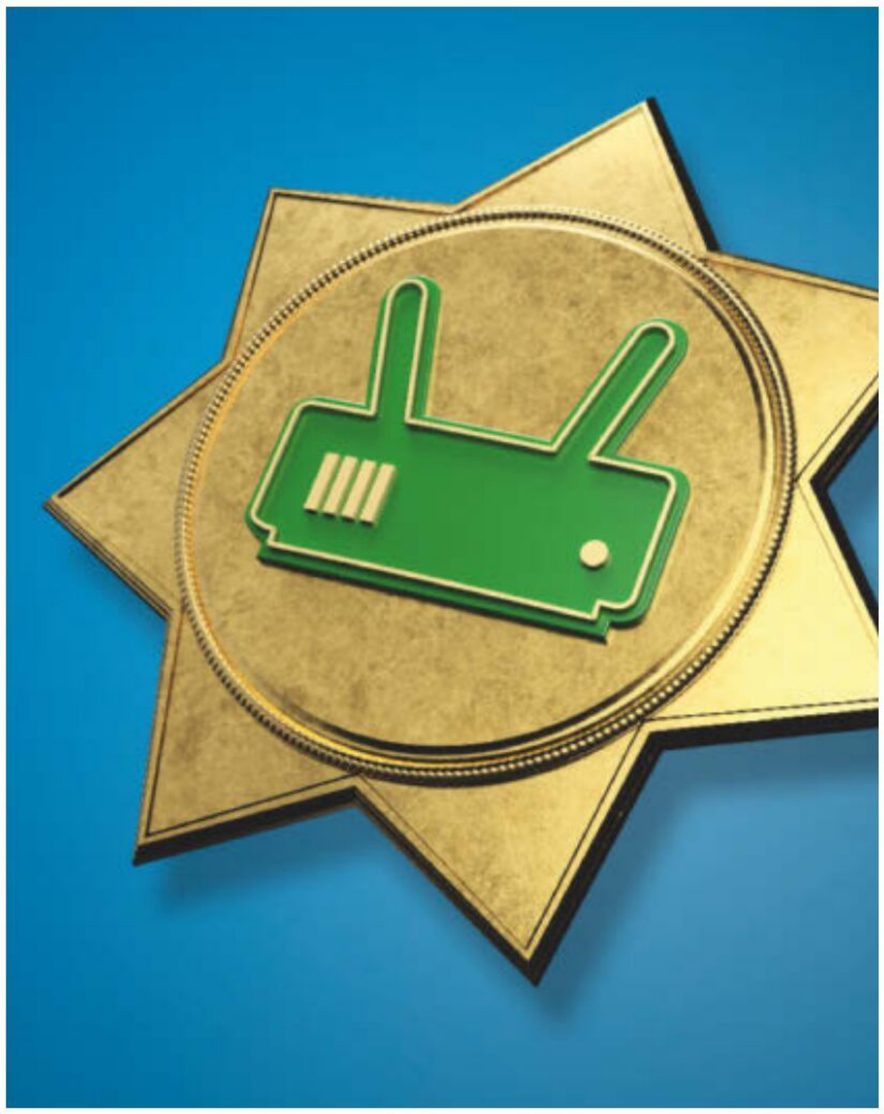


Bild: Andreas Martini

☑ Webinterface abdichten

Fast jeder moderne Router bringt einen Assistenten mit, der die wichtigsten Einstellungen abfragt und konfiguriert. Je nach Hersteller lassen sie aber diverse Lücken. Ändern Sie zunächst das ab Werk eingestellte Konfigurationspasswort. Denn viele Hersteller bringen es am Gehäuseboden an, wo es Unbefugte abfotografieren können. Mit den Zugangsdaten zu Ihrem Router kann jeder die WLAN- und VPN-Zugänge missbrauchen und ähnliches mehr.

Aktivieren Sie nach Möglichkeit das automatische Firmware-Update. So aktualisiert sich der Router, auch wenn Sie sich um anderes kümmern müssen oder für länger verreist sind.

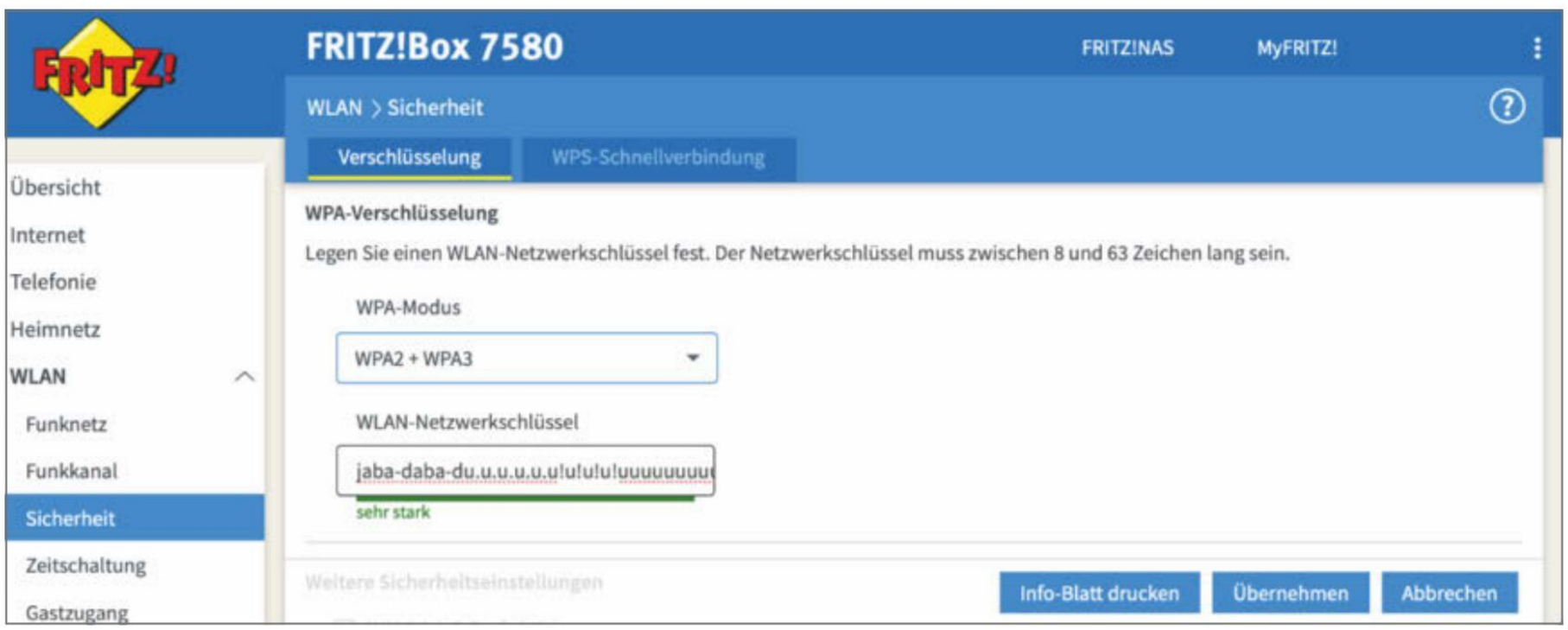
Schalten Sie bei der WLAN-Verschlüsselung den Mixed-Mode WPA2/WPA3 ein, falls vorhanden. Andernfalls aktivieren Sie wenn möglich den Schutz der Steuerpakete (PMF). Ändern Sie den Funknetznamen sowie das Passwort Ihres WLANs. Das empfiehlt sich auch dann, wenn der Hersteller seine Geräte mit individuellen Einstellungen ausliefert, denn diese sind meistens auf dem Router angebracht, sodass sie jeder auslesen und missbrauchen kann, der physischen Zugang zum Router hat.

Bei WLAN-Routern, die nur mit dem veralteten WPA2 verschlüsseln, lässt sich das Zugangspasswort per Brute-Force-Attacke ermitteln. Dafür nehmen Angreifer Aufzeichnungen Ihres WLAN-Verkehrs mit und füttern damit einen sehr leistungsfähigen PC. Ob er dann das Passwort schnell ausgibt oder der Angreifer das Herumprobieren nach Tagen wegen Aussichtslosigkeit abbricht, hängt von der Länge Ihres WLAN-Passworts ab. Nutzen Sie 20 bis 30 Zeichen, wenn Sie wegen älterer Geräte WPA2 verwenden müssen.

☑ Gastnetz einsetzen

Schützen Sie Ihre vertraulichen Geräte, indem Sie Gäste-, Smart-Home- und IoT-Geräten das Gast-WLAN zuweisen. Tragen Sie auch für das Gastnetz ein langes Passwort ein und ändern Sie es gelegentlich, denn manche Besucher geben WLAN-Passwörter ohne Rückfrage weiter.

Schränken Sie das Gast-WLAN auf bestimmte Dienste ein, beispielsweise Surfen und Mailen, um



Wenn das veraltete WPA2 eingeschaltet bleiben muss, gilt für die Sicherheit des WLAN-Passworts: Länge ist wichtiger als irgendwelche Sonderzeichenregeln.

Ärger wegen unerwünschtem Filesharing vorzubeugen.

Weil bei manchen Routern das Webinterface aus dem Internet erreichbar ist, sollte der zugehörige Datenverkehr verschlüsselt werden (HTTPS). Falls Sie auf einen Server im lokalen Netz von außen zugreifen wollen, richten Sie besser eine VPN-Verbindung ins Heimnetz ein als eine Port-Weiterleitung. Als VPN-Server eignen sich viele Router. Weitere Hinweise zum sicheren Betrieb von Servern finden Sie auf Seite 44.

☑ WPS nur bedarfsweise

Die WPS-Funktion erleichtert das Koppeln neuer WLAN-Clients, weil man dafür nur die zugehörigen Tasten am Router und am Client drücken muss. Schalten Sie diese Funktion aber immer nur bei Bedarf ein. Andernfalls können sich Dritte ohne Ihr Wissen Zugang zu Ihrem Hauptnetz verschaffen, wenn sie physischen Zugriff zum Router erhalten.

Manche Hersteller nutzen die UPnP-Funktion, um mittels ihrer Geräte eine Port-Weiterleitung von innen automatisch einzurichten. Das spart zwar Zeit, aber wenn die Funktion anhaltend aktiv ist, kann sie auch eingeschleppte Malware nutzen, um Löcher in die Firewall Ihres Routers zu bohren. Deaktivieren Sie diese Funktion nach Möglichkeit oder beschränken Sie sie auf einzelne Hosts, falls Ihr Router das ermöglicht.

Wenn alle Punkte abgehakt sind, exportieren Sie die Router-Konfiguration, damit Sie bei einem Router-Ausfall mit einem Ersatzgerät ohne Neueinrichtung fortfahren können. (dz) c't

Datenschutz-Dokumentation in Excel oder Word abhaken?

Das geht! Mit vorausgefüllten Vorlagen zum Verzeichnis von Verarbeitungstätigkeiten, technischen und organisatorischen Maßnahmen und vielen mehr.

Hier geht's zum Sonderangebot für c't Leser: **dsgvo-vorlagen.de/ct**

☑ Ohne Cloud
☑ Direkter Download
☑ Ohne Abo
☑ Keine versteckten Kosten

DeinData GmbH – Delitzscher Str. 8 – 04509 Löbnitz – info@dein-data.de – Tel.: +49 159 018 756 1

Security-Checkliste

E-Mail

Obwohl seit Langem von zahlreichen Sicherheitsproblemen geplagt, sind E-Mails immer noch omnipräsent. Zumindest einige Probleme lassen sich umgehen, aber vor allem sollten Sie sich der Gefahren bewusst sein und Mails mit Skepsis begegnen.

Von **Sylvester Tremmel**

Bild: Andreas Martini

☑ Gesundes Misstrauen

Vielen Leuten ist nicht bewusst, mit welcher Qualität E-Mails gefälscht werden. Das mag daran liegen, dass es auch die plumpen Spam-Mails von angeblichen afrikanischen Prinzen immer noch gibt. Wer Fälschungen nur auf diesem Niveau erwartet, wird leicht Opfer einer Mail, die angeblich von einem langjährigen Kunden kommt, mit passender Anrede fehlerfrei formuliert ist und Bezug auf eine echte Nachricht von letzter Woche nimmt.

Angreifer können solche gut gemachten Fälschungen inzwischen weitgehend automatisch erstellen und verschicken sie tagtäglich. Man muss dafür keineswegs einer gezielten Attacke ausgesetzt sein. „Uns kleine Fische wird es schon nicht treffen“, ist deshalb eine ganz schlechte Annahme.

Also, misstrauen Sie *jeder* E-Mail und werden Sie besonders hellhörig, wenn Anhänge oder Geld im Spiel sind – gerade wenn die Mail scheinbar vom Chef oder der Bank kommt und ganz dringend und wichtig ist. Statt Links in einer Mail anzuklicken, rufen Sie Websites besser über Ihre eigenen Bookmarks auf. Schlagen Sie Telefonnummern nach, statt den Angaben in einer Mail blind zu vertrauen. Und ignorieren Sie keine Sicherheitswarnungen beim Öffnen von Anhängen, auch wenn die Mail Sie auffordert, das zu tun.

☑ Mailclient absichern

Ihren Mailclient können Sie so einstellen, dass er zumindest ein paar gröbere Risiken von E-Mails entschärft: Das Nachladen von externen Inhalten sollten Sie grundsätzlich verbieten. Einige Mails sehen dann unschön aus, aber externe Inhalte werden einerseits gerne für (Werbe-)Tracking genutzt und sind andererseits immer wieder an Sicherheitslücken beteiligt.

Ähnliches gilt für HTML-Mails. Schalten Sie die HTML-Ansicht am besten ganz aus und lassen Sie Ihren Client nur die Textansicht anzeigen. Nur wenn diese absolut unleserlich (oder gar nicht vorhanden) ist, sollten Sie auf die HTML-Darstellung ausweichen – und eine Extraportion Vorsicht walten lassen. Viele Mailclients erlauben, HTML-Inhalte direkt aus der Mailansicht zu aktivieren, sodass der Komfortverlust gering ist.

☑ Verschlüsselung

Die Verschlüsselung von E-Mails ist ein Trauerspiel, das sich – wenn überhaupt – nur sehr langsam zum Besseren wendet. Nicht einmal Transportverschlüsselung ist garantiert, aber zumindest dieser Minimalstandard etabliert sich nach und nach. In den Einstellungen Ihres Mailclients sollten Sie 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 Mail-Provider erlauben, Mails nur dann zu versenden, wenn so eine Transportverschlüsselung bis zum Zielserver aufgebaut werden kann. Dann können zwar immer noch die beteiligten Mailserver mitlesen, aber immerhin niemand sonst. Sofern Ihr Anbieter so eine Option bietet, finden Sie sie in den Account-Einstellungen des Providers.

Alle Lauscher aussperren können Sie nur mit Ende-zu-Ende-Verschlüsselung. Die ist leider in der Handhabung oft kompliziert und die verbreiteten Standards S/MIME und OpenPGP kämpfen mit Alterserscheinungen und Designproblemen. Verbesserungen setzen sich auch hier bestenfalls langsam durch. Wenn Sie sich mit Ihren Korrespondenten auf ein Verfahren einigen können, sollten Sie es aber nutzen: Besser als nichts sind beide Verfahren allemal.

Als Notlösung bieten manche Provider an, Mails bei Eingang automatisch per OpenPGP oder S/MIME zu verschlüsseln. Dann sind sie immerhin vor fremden Augen sicher, sobald sie Ihren Account erreicht haben. Um selbigen abzusichern, sollten Sie Zwei-Faktor-Authentifizierung (2FA) nutzen (siehe Seite 62), was die meisten Mailprovider mittlerweile anbieten.

☑ Überlegt nutzen

Hinterfragen Sie auch beim Versand, wie und wofür Sie E-Mails nutzen. Reine Textmails zu verschicken verhindert zwar schicke Formatierungen, erspart aber den Empfängern die Risiken von HTML-Mails. Ähnliches gilt für ausführbare Dateien oder Office-Dokumente mit Makros. Solche verdächtigen Inhalte wollen Sie nicht per Mail empfangen, also versenden Sie auch nichts Derartiges. Ihre Korrespondenten werden es Ihnen danken, wenn sie eine bösartige – und angeblich von Ihnen stammende – Mail erkennen, weil an der Nachricht eine DOC-Datei hängt, obwohl Sie nur PDFs verschicken.

Auch auf die Liste von Empfängern sollten Sie lieber zweimal schauen: „Allen antworten“ ist bequem, aber streut Informationen oft weiter als nötig. Prüfen Sie vor dem Versand zudem, ob wirklich die gesamte Originalmail zitiert sein muss – gerade wenn Sie den Empfängerkreis erweitern. (syt) c't

Nur wer um die Lücken weiß, kann diese auch wirksam schließen.
Im Bereich Penetrationstest sind wir Marktführer in Deutschland.

Durch einen Sicherheitstest Ihrer IT-Infrastruktur können Sie sich umfangreich **vor Angriffen**, dem Verlust von Informationen und der Störung von Maschinen **schützen**. Wir testen Ihre Systeme durch simulierte Angriffe, finden heraus, wie **sicher** die eingesetzte IT-Infrastruktur ist.

- Beugen Sie Hackerangriffen und Einbrüchen in Ihre Systeme vor
- Schützen Sie Ihre wertvollen Unternehmensdaten und Erkenntnisse
- Bauen Sie dem Ausfall digital gesteuerter Anlagen vor
- Behalten Sie die Kontrolle über Ihre Systeme

THE PENTEST EXPERTS

SySS GmbH +49 (0)7071 - 40 78 56-0 info@syss.de www.syss.de

IT Security: heute TOP-Thema im Sonderheft, immer TOP-Thema bei der SySS GmbH

Dass sich dieses Sonderheft der IT-Sicherheit widmet, hat einen guten Grund: Es vergeht keine Woche, in der Hacker nicht in Netzwerke, Server und PCs eindringen. Die IT-Sicherheitsexperten der SySS GmbH rund um Geschäftsführer Sebastian Schreiber machen es sich zur Aufgabe, Kleinunternehmen, Mittelständler und Weltkonzerne vor möglicherweise gefährlichen Sicherheitslücken in IT-Systemen und Netzwerken zu schützen. Wer beim Marktführer an einem der Standorte in Tübingen, Frankfurt/M., München oder Wien als Penetrationstester einsteigt, lernt in IT-Systeme einzubrechen und Gefahrenpotentiale zu finden, bevor andere es tun.

Vier zentrale Prinzipien leiten die Arbeit der SySS-Pentester:

Wir nehmen die *Perspektive eines Hackers* ein und finden Schwachstellen, die auch ein echter Angreifer entdecken würde. Wir folgen einem *strikten Legalitätsprinzip* und orientieren uns an unserer „Ethik für Penetrationstester“. Die Offenlegung von Schwachstellen erfolgt *verantwortungsvoll*. *Produktunabhängigkeit* garantiert die Objektivität unserer Testergebnisse.

Drei Leitlinien begleiten die Arbeit der SySS-Pentester:

In umfangreichen Schulungsprogrammen, regelmäßigen Wissenstransfer-Meetings und unserer Forschungsabteilung erweitern wir unser *Wissen* stetig.

Durch Gesundheitsvorsorge und diverse Fortbildungsangebote werden unsere Mitarbeiter ganzheitlich *gefördert*.

Ein Gleitzeitmodell, sportliche und kulturelle Teamevents sowie Firmenfeste machen aus vielen Einzelnen ein *Wir*.

Security-Checkliste

Messenger

WhatsApp, Signal oder Telegram, der Facebook-Messenger oder doch ein Matrix-Client? Dutzende Messenger buhlen um Nutzer und praktisch alle behaupten, sicher zu sein. Doch Verschlüsselung ist nicht gleich Verschlüsselung, und ganz ohne Zutun und Kontrolle geht es auch nicht.

Von **Sylvester Tremmel**

Bild: Andreas Martini

☑ Verschlüsselung nutzen

Stand der Technik ist, Nachrichten zu verschlüsseln, und zwar mit einer Ende-zu-Ende-Verschlüsselung (end-to-end encryption, E2EE). Das bedeutet, dass auch der Server, der die Nachrichten vermittelt, ihren Inhalt nicht lesen kann. Bei Messengern ist E2EE erfreulich weit verbreitet, auch wenn es im Detail Unterschiede gibt [1]. Empfehlenswert sind unter anderem die Apps Signal und Threema. Wichtig ist, dass E2EE auch tatsächlich zum Einsatz kommt. Apps wie Telegram oder der Facebook-Messenger nutzen E2EE nämlich nur, wenn Sie als Nutzer „geheime Chats“ oder „geheime Unterhaltungen“ starten. Achten Sie darauf, ob und wann Ihr Messenger von Ende zu Ende verschlüsselt.

Marktführer WhatsApp verschlüsselt immer von Ende zu Ende und bewirbt das auch gerne. Allerdings ist dieses Versprechen nur schwer zu überprüfen, weil die App nicht quelloffen ist. Außerdem schützt der Messenger Metadaten schlechter als die meisten Konkurrenten [2].

☑ 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 eingerichtet – sämtliche Konversationen bis auf Weiteres mitlesen. Die Messenger-Apps auf dem Smartphone zeigen daher (meist in den Einstellungen), welche anderen Geräte verknüpft sind. Prüfen Sie die Liste regelmäßig und löschen Sie, was Sie nicht mehr brauchen.

☑ Backups kontrollieren

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 (siehe ct.de/wesq). 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: Oft sind die Daten dort nicht so verschlüsselt, dass nur Sie Zugriff haben.

Viele Messenger erlauben es, Nachrichten nach einer einstellbaren Zeit automatisch zu löschen. „Selbstzerstörende“, „selbstlöschende“ oder „verschwindende“ Nachrichten nennen die Apps das. Vorsicht: Das Feature kann nicht verhindern, dass der Gesprächspartner die Nachricht dennoch dokumentiert. Aber es eignet sich gut, um Chatverläufe kurz und Messenger-Backups klein zu halten.

☑ Verifizierung aktivieren

Viele Messenger binden die Accounts an eine Handynummer [3]. Die wird per SMS bestätigt, was sich manipulieren lässt. Schlimmstenfalls können Dritte dadurch Accounts übernehmen. Die meisten solcher Messenger bieten daher an, 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 wollen.

Achten Sie außerdem darauf, Ihre Accounts bei einem Nummernwechsel umzuziehen und nicht unter der alten Nummer weiter zu betreiben. Die kann nämlich wieder vergeben werden. Falls der neue Besitzer denselben Messenger nutzen will und die Nummer registriert, werden Sie dadurch aus Ihrem Account ausgesperrt.

☑ Erst denken, dann klicken

Betrüger und andere Kriminelle, Kettenbriefe und unerwünschte Werbung gibt es auch bei Messengern. Man hört häufig von Fällen bei Telegram, aber auch andere Apps haben solche Probleme. Seien Sie deshalb skeptisch: Fügen Sie nicht alles und jeden ungeprüft zu Ihren Kontakten hinzu; schreiben Sie nichts Privates in Ihr (öffentliches) Account-Profil; leiten Sie Nachrichten nicht unhinterfragt oder massenhaft weiter und öffnen Sie keine Links, deren Ziel Ihnen nichts sagt. Kein noch so schlaues Sicherheits-Feature kann gesundes Misstrauen ersetzen.

(syt) c't

Literatur

[1] Jan-Keno Janssen, Sylvester Tremmel und Sebastian Trepesch, **Messengerdämmerung**, Sichere Messenger: WhatsApp und Alternativen im Test, c't 8/2021, S. 14

[2] Sylvester Tremmel, **Ohne Sendungsverfolgung**, Wie Messenger versuchen, Metadaten zu vermeiden, c't 8/2021, S. 24

[3] Sylvester Tremmel, **Zeigt her Eure Kontakte**, Warum Messenger nach Ihrer Telefonnummer fragen, c't 6/2021, S. 118

Backups

ct.de/wesq

heise Security Pro

Vernetzen, verstehen, umsetzen

Mit heise Security Pro zu mehr IT-Sicherheit.

- Mindestens 4 Security Webinare
- 1 Ticket für die secIT
- Wöchentlicher Experten-Newsletter
- Jährliche heise Security Konferenz
- heise Security Expertenplattform
- 1 heise+ & 1 Pur-Lizenz

JETZT IT-PAKET SICHERN:
heise.de/heisec-pro

Security-Checkliste

Browser

Ihr Browser kommt so oft wie kein anderes Programm mit Schadcode in Kontakt, dazu müssen Sie nicht mal auf zwielichtigen Websites surfen. Umso wichtiger ist es, ihn maximal sicher einzustellen.

Von **Jo Bager**

Bild: Andreas Martini

☑ Aktuell bleiben

Um sicher zu surfen, müssen Sie die aktuelle Version des Browsers Ihrer Wahl nutzen. Die Hersteller geben laufend Updates heraus, die Sicherheitslücken schließen. So hat etwa Google allein im Oktober mit einem Chrome-Update insgesamt neunzehn Schwachstellen beseitigt. Alle gängigen Browser lassen sich so einstellen, dass sie sich automatisch aktualisieren. Gelegentlich klemmt jedoch die Update-Versorgung oder der Browser muss zur Installation neu gestartet werden. Überprüfen Sie daher über den Info-Dialog (teilweise auch als „Über XYZ“ im Menü zu finden), ob ein Neustart nötig ist.

☑ Add-ons ausmisten

Browser-Erweiterungen (auch Add-ons oder Extensions genannt) haben Zugriff auf alles, was innerhalb des Browsers geschieht, einschließlich des Online-Bankings. Überprüfen Sie vor der Installation also genau, worauf Sie sich einlassen. Installieren Sie nur Erweiterungen aus den offiziellen Downloadkatalogen der Hersteller und achten Sie auf Downloadzahlen und Nutzerbewertungen. Verzichten Sie im Zweifel lieber zugunsten der Sicherheit. Überprüfen Sie auch gelegentlich, welche Erweiterungen bereits installiert sind, und misten Sie gründlich aus. Bei Chrome finden Sie die Erweiterungen im Menü unter „Weitere Tools“, bei Firefox klicken Sie auf „Add-ons und Themes“. Im Edge-Menü klicken Sie einfach auf „Erweiterungen“. Deaktivieren Sie Add-ons, die Sie nur selten nutzen, und schalten Sie sie bei Bedarf wieder ein.

☑ Tracker blockieren

Blockieren Sie Tracker, die Ihr Surfverhalten überwachen und Ihre Interessen ausspionieren. Einige Browser wie Firefox und Edge können das bereits von Haus aus, Sie müssen den Tracking-Blocker nur noch in den Einstellungen unter „Datenschutz & Sicherheit“ scharf schalten. Probieren Sie zunächst die Einstellung „Streng“. Falls es anschließend Probleme bei Ihren Lieblingswebsites gibt, können Sie den milderen Standardmodus einstellen. Nutzer anderer Browser wie Chrome können sich mit Add-ons wie Privacy Badger oder uMatrix behelfen (siehe ct.de/wsmy). uBlock Origin beseitigt zudem aufdringliche (und mitunter verseuchte) Werbung.

☑ Berechtigung checken

Websites können Berechtigungen einfordern, um etwa auf Kamera, Mikrofon und Standort zuzugreifen. Stimmen Sie nur zu, wenn es einen triftigen Grund gibt und Sie dem Dienst vertrauen. Ein Videochat-Dienst benötigt natürlich den Zugriff auf Kamera und Mikro, Google Maps kann Ihren aktuellen Standort nur mit Ihrer Zustimmung ermitteln. Kontrollieren Sie die bereits erteilten Berechtigungen und misten Sie gründlich aus. In den Chrome-Ein-

stellungen finden Sie die Berechtigungen unter „Datenschutz und Sicherheit/Website-Einstellungen“, in den Firefox-Einstellungen unter „Datenschutz & Sicherheit/Berechtigungen“. Edge-Nutzer schauen in den Einstellungen unter „Websiteberechtigungen“.

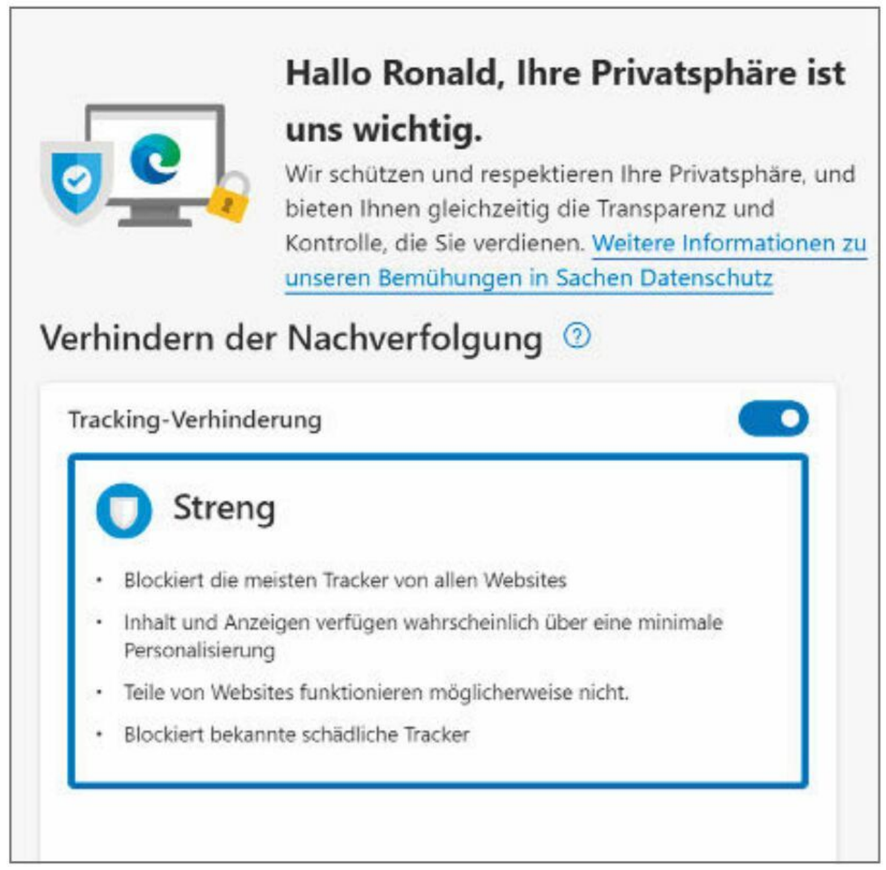
☑ Auf Adressen achten

Geben Sie persönliche Daten, Passwörter und Finanzdaten nur auf Websites ein, die verschlüsselt übertragen werden (Webadresse beginnt mit https:// beziehungsweise der Browser zeigt ein geschlossenes Vorhängeschloss neben der Adresse an). Darüber hinaus sollten Sie die Adressen genau auf Ungereimtheiten untersuchen: 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 häufig besuchte Websites am besten über Lesezeichen an und nicht über Links, die Sie per Mail erhalten haben.

(jo) c't

Tracking-Blocker für Chrome und andere

ct.de/wsmy



Datenschutz inklusive: Browser wie Microsoft Edge bringen einen Tracking-Schutz mit, den Sie scharf schalten sollten.

VPN → ZTNA

Der smarte Zero-Trust Network Access für alle Bereiche!

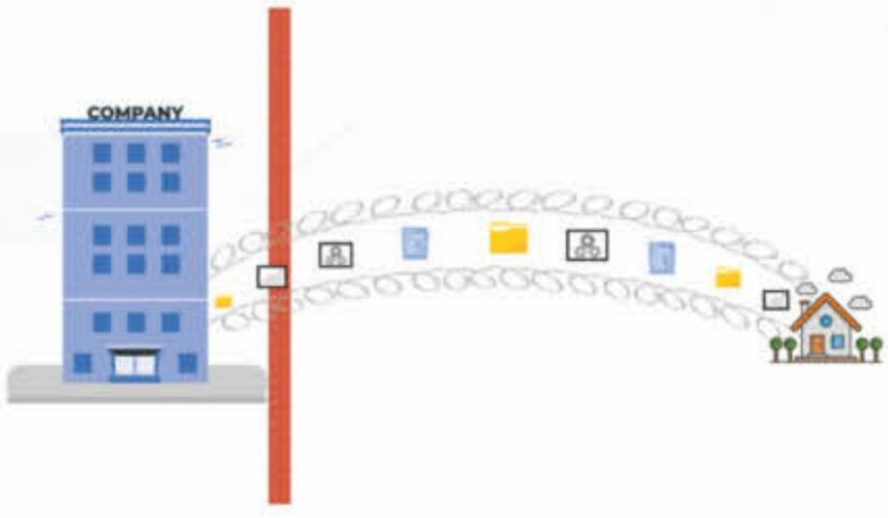
Cordaware bestzero®

Starten Sie jetzt!

✔Sichere Remote-Arbeit unabhängig vom eigenen Standort (Homeoffice / mobil)
✔Zero-Firewall-Config - Keine offenen eingehenden Ports
✔LDAP-basierte & skalierbare Zugriffsberechtigungen

Was Sie nicht benötigen!!

✘ Kostenintensive VPN Soft- und Hardware
✘ Hacking-anfälliges RDP durch offene Ports
✘ Keine aufwändige Firewall-Verwaltung



CORDAWARE INFORMATIONSLOGISTIK

+ 49 (0) 8441 – 85 93 200 info@cordaware.com www.cordaware.com

Security-Checkliste

Social Media

Social-Media-Konten bilden de facto die digitale Identität vieler Nutzer ab. Die Plattformen bieten deshalb Schutzfunktionen, die Sie anwenden sollten. Und: Schalten Sie bei sozialen Kontakten nicht den gesunden Menschenverstand aus.

Von **Holger Bleich**

Bild: Andreas Martini

☑ Zwei Faktoren nutzen

Werden Ihre Konten bei Facebook, Instagram oder LinkedIn gekapert, kann das nicht nur für Sie, sondern auch für Freunde und Geschäftspartner katastrophale Folgen haben. Der Schutz solcher Accounts ist deshalb besonders wichtig. Nutzen Sie dazu alle Möglichkeiten, die die Plattformen bieten. Was in den anderen Checklisten bereits erwähnt ist, gilt in besonderem Maße für soziale Plattformen: Sie sollten, wo immer möglich, weitere Zugangsbarrieren neben dem Passwort aufbauen, also auf eine Zwei-Faktor-Authentifizierung (2FA) setzen.

Auf der Facebook-Website gelangen Sie über den Pfeil neben der Hilfefunktion in die „Einstellungen“, wo der Menüpunkt „Sicherheit und Login“ zur „zweistufigen Authentifizierung“ führt. Dort 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.

Damit die Abfrage nicht jedes Mal nervt, merken sich die Plattformen Geräte-IDs oder setzen Cookies und bleiben auf dem Gerät angemeldet. Dies kann zum Sicherheitsproblem werden, wenn sich mehrere Menschen einen Rechner teilen oder 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 Facebook etwa finden Sie diese Liste im oben genannten Menü unter „Autorisierte Logins“. Dort lässt sich der Zugriff selektiv unterbinden.

☑ Zugriffe prüfen

Bei vielen sozialen Netzen können Sie externen Diensten und Fremd-Apps Zugriff auf Ihren Account gewähren, beispielsweise für Single-Sign-on-Logins auf verbundenen Websites. Bisweilen räumen sich Apps viel mehr Rechte als nötig ein. Sie sollten die Aktivitäten und Berechtigungen der Apps im Auge behalten. Facebook gewährt Ihnen Kontrollmöglichkeiten in den Einstellungen unter „Apps und Websites“.

Besonders beliebt sind Apps bei Instagram-Nutzern. Unter „Apps und Websites“ in den Profileinstellungen listet der Dienst die aktiven Apps auf. Kontrollieren Sie diese Liste ab und an und entfernen Sie nicht mehr benötigte Apps. Twitter führt diese Option unter „Apps und Sitzungen“ im Account-Profil. Dort entfernen Sie auch autorisierte Geräte, die keinen Zugriff mehr erhalten sollen.

☑ Gezielt teilen

Bei Facebook, aber auch bei anderen Anbietern wie LinkedIn kann man festlegen, mit wem man Inhalte teilen möchte. Behalten Sie Ihre Zielgruppen-Voreinstellung 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 und Ihr Haus leersteht. Die Voreinstellung sollte eher defensiv sein. Sie lässt sich etwa bei Facebook in den Privatsphäre-Einstellungen unter „Deine Aktivität“ ändern. Dort können Sie auch die Sichtbarkeit vergangener Beiträge beschränken.

☑ Anfragen checken

Freundschaft und Vertrauen sind auch auf Facebook, Instagram oder LinkedIn ein begehrter Status. Befreundete Kontakte sehen je nach Profileinstellungen viel mehr Privates. Oft stecken hinter Freundschaftsanfragen Versuche, persönliche Daten abzugreifen, die Person zu stalken oder gar Geld zu ergaunern. Checken 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. Sie können das Foto über die Google-Bildersuche vielleicht als Bilderklau enttarnen.

☑ 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 sein Facebook-Account gehackt und übernommen, und nun versucht jemand, Ihr Vertrauen zu missbrauchen. Überweisen Sie keinesfalls Geld und rücken Sie nicht unbedacht Ihre Handy-Nummer heraus, bevor Sie sich von der Identität überzeugen konnten – zum Beispiel mit einer Frage, die garantiert nur die befreundete Person beantworten kann.

(hob) c't

Security-Checkliste

Online-banking

Auf Ihrem Bankkonto liegt Ihr Geld – logisch, dass Betrüger und Cyberkriminelle scharf darauf sind. Absolute Sicherheit gibt es beim Onlinebanking nicht, aber Sie können es Kriminellen extrem schwer machen.

Von **Markus Montz**

Bild: Andreas Martini

☑ Transaktionen checken

Fast alle Überweisungen erfordern eine Zwei-Faktor-Authentifizierung, zum Beispiel mit PIN beim Login und TAN bei der Transaktion. Checken Sie bei Online-Überweisungen jeweils Empfänger-IBAN und Betrag auf Ihren Geräten, bevor Sie eine Überweisung freigeben. Diese Kontrollmöglichkeit gibt Ihre Bank Ihnen in Anlehnung an die Zweite Europäische Zahlungsdiensterichtlinie (PSD2) [1]. Vergleichen Sie die Daten auch mit der Angabe auf der Rechnung, wenn Ihnen eine vorliegt.

☑ Banking virenfrei

Banking mit dem PC oder Smartphone ist nur sicher, wenn das System frei von Schadsoftware ist. Sorgen Sie auf einem Windows-PC dafür, dass ein Virenscanner mit aktuellen Updates mitläuft – der ab Windows 8.1 mitgelieferte Defender bietet hinreichenden Schutz (siehe auch Seite 10).

Laden Sie Anwendungen aus dem Netz nur von seriösen Websites herunter. Achten Sie auf dem Smartphone darauf, allgemein nur Apps aus vertrauenswürdigen Quellen zu installieren. Im Zweifel ist das bei Android der Google Play Store und bei iOS der App Store.

☑ Phishing erkennen

Bei der überwiegenden Zahl von Betrugsfällen im Onlinebanking verschicken Betrüger manipulativ gestaltete Mails oder erstellen Fake-Websites. Damit wollen sie falsche Handlungen bei unbedarften Nutzern provozieren (Social Engineering). Kriminelle senden beispielsweise massenhaft Mails im Namen von Bankinstituten. Darüber schleusen sie Trojaner und andere Schadprogramme ein, verlinken auf Websites mit Schadcode oder greifen Zugangsdaten ab (Phishing).

Prüfen Sie alle Mail-Anhänge sorgfältig, auch von scheinbar bekannten Absendern. Eine seriöse Bank schickt Ihnen niemals unangekündigt Dokumente in einer Mail und insbesondere keine Links, um Ihr Konto mit PIN und TAN zu „bestätigen“. Prüfen Sie bei allen anderen Links zuerst die Ziel-URL. Schöpfen Sie Verdacht, wenn eine persönliche Anrede fehlt oder Sie zur Eile getrieben werden. Achten Sie auf

Sprache – deutschsprachige Banken schreiben mit korrektem Satzbau, Umlauten (ä, ö, ü) und korrekter Rechtschreibung. Geben Sie Ihre Zugangsdaten im Browser nur auf der Webseite der Bank ein, nachdem Sie die Adresse selbst eingetippt oder per Bookmark angesteuert haben. Sicher sind auch die App der Bank oder eine seriöse Onlinebanking-Anwendung. Nutzen Sie Ihre zweiten Faktoren umsichtig (siehe oben).

☑ Belege überprüfen

Insbesondere Kreditkartennutzer sollten jede Abrechnung kontrollieren und unbefugte Abbuchungen umgehend bei ihrer Bank reklamieren. 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 sich Nutzer 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, da Sie damit wichtige Schutzfunktionen lahmlegen. 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 auf modifizierten Geräten aus diesen Gründen gar nicht erst [2].

Generell ist es empfehlenswert, ein ungerootetes Smartphone mit einem Betriebssystem zu verwenden, das noch Sicherheitsupdates bekommt – obwohl das nicht heißt, dass ältere Betriebssysteme per se unsicher sind. Aus Haftungsgründen empfiehlt es sich, mindestens den Vorgaben Ihrer Bank zu folgen: Solange die App Ihrer Bank ein älteres Betriebssystem noch unterstützt und Sie es nutzen, kann Ihr Kreditinstitut Ihnen zumindest daraus keine grobe Verletzung der Sorgfaltspflichten ableiten. Ohne solch eine grobe Verletzung haften Sie für Schäden selbst mit maximal 50 Euro [3]. (mon) c't

Literatur

[1] Markus Montz, **Zweitschlösser**, Neue Onlinebanking-Regeln ab September, c't 18/2019, S. 66

[2] Sylvester Tremmel, **FAQ Banking-App-Sicherheit**, c't 11/2020, S. 70

[3] Stefan Hessel, **Datenfänger und Haftungsflüchtlinge**, Smartphone-Banking aus rechtlicher Sicht, c't 11/2020, S. 66

Heft + PDF mit 29 % Rabatt

Ihr Erste-Hilfe-Set:

Das Notfall-System für den Ernstfall

Mit der neuen Version **c't Desinfec't 2021/22** sind Sie für den Ernstfall bestens gerüstet:

- Vier der neuesten Viren-Scanner
- Notfallsystem, das Ihre Daten retten kann
- Notfallarbeitsplatz
- Verbesserte Hardware-Kompatibilität

Heft für 14,90 € • PDF für 12,99 € • Bundle Heft + PDF 19,90 €

shop.heise.de/desinfect21

Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 €.
Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

heise Shop

Security-Checkliste

Backups

Egal, wie lästig es sein mag: Das regelmäßige Anfertigen von Backups Ihrer Daten ist unverzichtbar. Doch ist Ihr Backup auch zuverlässig?

Von **Axel Vahldiek**

Bild: Andreas Martini

☑ Los jetzt!

Damit Sie im Ernstfall keine Daten verlieren, brauchen Sie ein Backup davon. Auf welche Art Sie das erstellen, ist an sich erst mal egal, denn jedes Backup ist besser als kein Backup. Wichtig ist stattdessen, dass Sie es auch wirklich machen. Der richtige Termin dafür ist immer der gleiche: jetzt! Sichern Sie zuerst die wichtigsten Daten. Starten Sie mit Daten, die nur als Unikat vorliegen wie Diplomarbeit, Steuerunterlagen und anderen Arbeitsergebnissen. Denken Sie auch 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 mag schon ein USB-Laufwerk oder eine DVD als Speichermedium reichen. Für Laien oft einfacher ist das Ausdrucken auf Papier. Diese Art von Backup ist sogar langlebig: Ein 60 Jahre altes Foto mag vergilbt sein, das Motiv ist aber immer noch erkennbar. Zum Vergleich: Versuchen Sie mal, etwas von einer nur halb so alten CD auszulesen.

☑ Feuerfest

Wenn in Ihrer Wohnung Feuer ausbricht, verbrennt eine neben dem PC liegende USB-Platte gleich mit. Also muss das Sicherungsmedium woanders hin. Keller und Dachboden mögen naheliegend sein, reichen aber nicht, denn das Löschwasser läuft in den Keller und das Feuer kommt überall hin. Kurzum: Das Backup muss raus aus dem Haus. Nehmen Sie eines Ihrer Backupmedien aus dem Büro beispielsweise abends mit nach Hause oder lagern Sie es bei Verwandten. Leicht merken lässt sich das als 3-2-1-Regel: 3 Kopien auf 2 Datenträgern, davon 1 außer Haus.

☑ 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, welches nach dem Sichern abgestöpselt wird, ist technisch getrennt – doch Obacht: Wenn Sie es für die nächste Sicherung wieder anstöpseln, ist es eben wieder nicht mehr getrennt. Dagegen hilft nur, mehrere Sicherungsmedien im Wechsel oder Einmalmedien wie DVDs 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: Stellen Sie sicher, dass Sie das Backup im Ernstfall wieder entschlüsseln können.

☑ Wiederherstellen

Solange Sie Ihr Backup nicht testweise wiederhergestellt haben, darf es nicht als zuverlässig gelten. 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. Sensibilisieren Sie sich aber dann dafür, auch das Ausbleiben der Logs/Mails zu bemerken!

☑ Ruhiger schlafen

Ihr Backup erfüllt alle Anforderungen? Herzlichen Glückwunsch! Falls nicht: In c't 10/2020 finden Sie ab Seite 16 gleich drei Artikel mit Tipps zum Einrichten von Backups für Admins sowie für ein zentrales Backup für Ihre ganze Familie, egal, wie verstreut die Verwandten leben. (axv) c't

Wie wichtig Daten sind

Die Farben helfen beim Priorisieren von Backups: grün: muss nicht; gelb schadet nicht; orange: besser ist das; rot: unbedingt!

	leicht ersetzbar	schwer ersetzbar	Unikat
weniger wichtig	Betriebssystem; freie Tools: Browser, Mailer, Packer, Bildbetrachter	Spielstände	Betriebssystem-einstellungen, Anwendungsein-stellungen
wichtig, aber nicht dringend	gekaufte Musik, Filme, E-Books; Dokumentation als PDF; installierte Software; Fotos von Freunden und Verwandten	gerippte/bearbeitete Musik und Videos; bearbeitete Kopien eigener Fotos; Software-Lizenzen	selbst gemachte Fotos, Musik, Videos, Hochzeits-planung, Einladung
unverzichtbar	beruflich genutzte Software und deren Lizenzen	beruflich genutzte, proprietäre Rohdaten und Arbeitsmittel: Firmendatenbank, Schriften, Vorschrif-ten, interne Kommunikation	Diplomarbeit, Steuerunterlagen, eigene Arbeitser-gebnisse

Security-Checkliste

Passwörter & Accounts

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

Von **Ronald Eikenberg**

Bild: Andreas Martini

☑ Nicht recyceln

Nutzen Sie für jeden Dienst ein anderes Kennwort. Sollten Sie Passwörter recycelt haben, gehen Sie am besten alle wichtigen Accounts durch und legen Sie individuelle Passwörter fest – insbesondere bei Diensten, bei denen es um persönliche Daten oder um Geld geht.

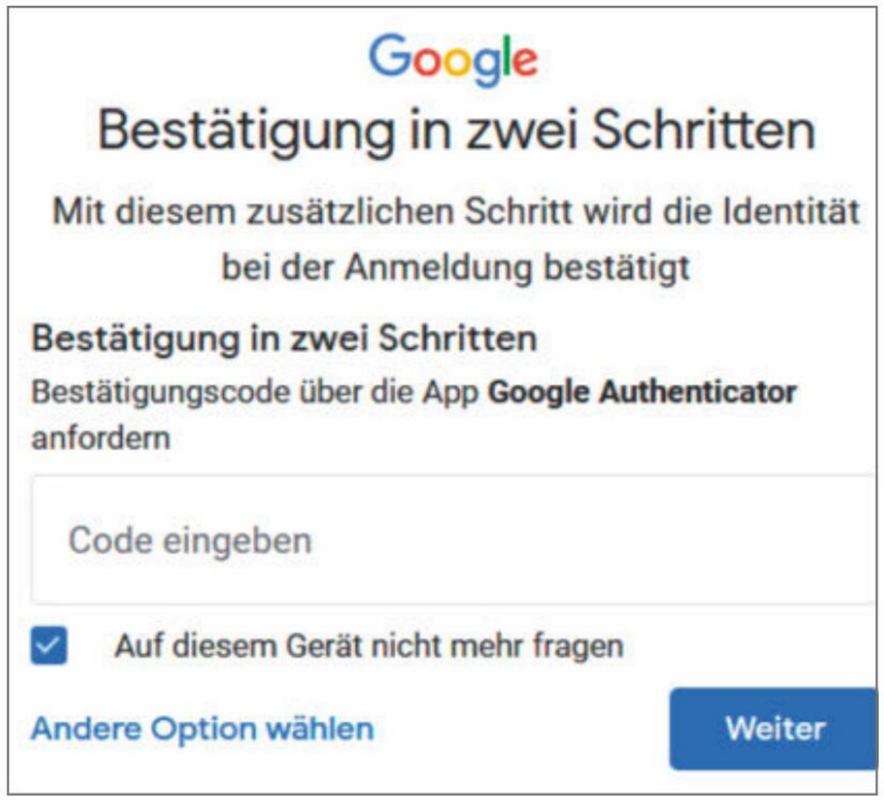
☑ Besser lang

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 ist oder wenn ein Account gehackt wurde.

Ein gutes Passwort muss alltagstauglich sein und sich auch am Smartphone eintippen lassen. Besser als möglichst viele Sonderzeichen ist es, möglichst lange Passwörter einzusetzen: Die Länge ist der größte Hebel, um die Sicherheit zu erhöhen. Insbesondere bei Verschlüsselung (Dateien, Festplatten, PGP & Co.) sollten Sie so viele Zeichen nutzen, wie Sie handhaben können. Ein Weg zum Ziel ist die Aneinanderreihung von Wörtern zu „Passphrasen“, absichtliche Schreibfehler sorgen für mehr Sicherheit.

☑ Passwortmanager

Nutzen Sie am besten einen Passwortmanager wie KeePass 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 c’t 5/2021 [1].



Die Zwei-Faktor-Authentifizierung ist ein wirksamer Schutz vor Hackern.

Der Passwortspeicher des Browsers ist nur bedingt zu empfehlen: Standardmäßig kommt jeder, der Zugriff auf Ihr Nutzerkonto hat, an alle gespeicherten Zugangsdaten. Um das zu verhindern, sollten Sie bei Firefox ein Masterpasswort setzen, das der Browser daraufhin jeweils beim ersten Passwortzugriff nach dem Start abfragt. Sie setzen es in den Firefox-Einstellungen unter „Datenschutz & Sicherheit/Zugangsdaten und Passwörter/Hauptpasswort verwenden“. Wenn Sie die Sync-Funktion von Chrome nutzen, sollten Sie Ihre Zugangsdaten zumindest vor der Übertragung in die Google-Cloud mit einer Passphrase verschlüsseln.

☑ Darknet-Leaks checken

Cyber-Ganoven erbeuten immer wieder und im großen Stil Datenbanken mit Zugangsdaten. Sie müssen damit rechnen, dass es auch die von Ihnen genutzten Dienste früher oder später trifft. Überprüfen Sie von Zeit zu Zeit in öffentlichen Datenbanken, ob und für welche Ihrer Accounts 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/check2022). Gibt es einen Treffer, sollten Sie das betroffene Passwort als kompromittiert betrachten und ändern. Rechnen Sie außerdem mit einem Anstieg an Spam- und Phishingmails bei der betroffenen Mail-Adresse, die sich möglicherweise sogar auf den gehackten Dienst beziehen.

☑ Zwei Faktoren nutzen

Viele Onlinedienste bieten 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. Das ist zum Beispiel ein Code, den Sie per SMS erhalten. Noch sicherer ist eine Authenticator-App wie Google Authenticator. Alternativ können Sie auch einen Sicherheitsschlüssel (FIDO2 oder U2F) als zweiten Faktor nutzen. Dieser hat meist das Format eines USB-Sticks. Ab Seite 34 gehen wir näher auf Authenticator-Apps und Sicherheits-Sticks ein. (rei) c't

Literatur

[1] Jan Schüßler, Marvin Strathmann, **Ich kaufe ein ******, 25 Passwortmanager für PC und Smartphone, c't 5/2021, S. 16

Ergebnis Ihrer Anfrage bei HPI Identity Leak Checker

Achtung: Ihre E-Mail-Adresse taucht in mindestens einer gestohlenen und unrechtmäßig veröffentlichten Identitätsdatenbank (so genannter Identity Leak) auf. Folgende sensible Informationen wurden im Zusammenhang mit Ihrer E-Mail-Adresse frei im Internet gefunden:

Betroffener Dienst	Datum	Verifiziert	Betroffene Nutzer	Passwort	Vor- und Zuname	Geburtsdatum
verifications.io	Feb. 2019	✓	763.002.527	–	–	–
Combolist	Jan. 2019		1.247.433.080	Betroffen	–	–
	Der Ursprung der Daten ist unklar. Auch ist nicht bekannt, wie alt die Daten sind bzw. älterer Leaks und Daten aus Phishingkampagnen.					
Unknown (Collection #1-#5)	Jan. 2019		2.191.498.885	Betroffen	–	–
	Dieser Datensatz wurde im Januar 2019 veröffentlicht und enthält riesige Listen von					
animoto.com	Jul. 2018	✓	22.439.713	Betroffen	Betroffen	Betroffen
pemiblanc.com (Combolist)	Apr. 2018		479.496.221	Betroffen	–	–

Ein Leak-Check verrät, ob die eigenen Daten und Passwörter bereits im Darknet kursieren.

Security-Checkliste

Server & Hosting

Wer einen über das Internet erreichbaren Server betreibt, muss damit rechnen, dass diesen nicht nur freundlich gesinnte Internet-Nutzer kontaktieren. Sichern Sie Ihren Heim- oder Mietserver oder das Webhosting-Paket also besser ab.

Von **Jan Mahn**

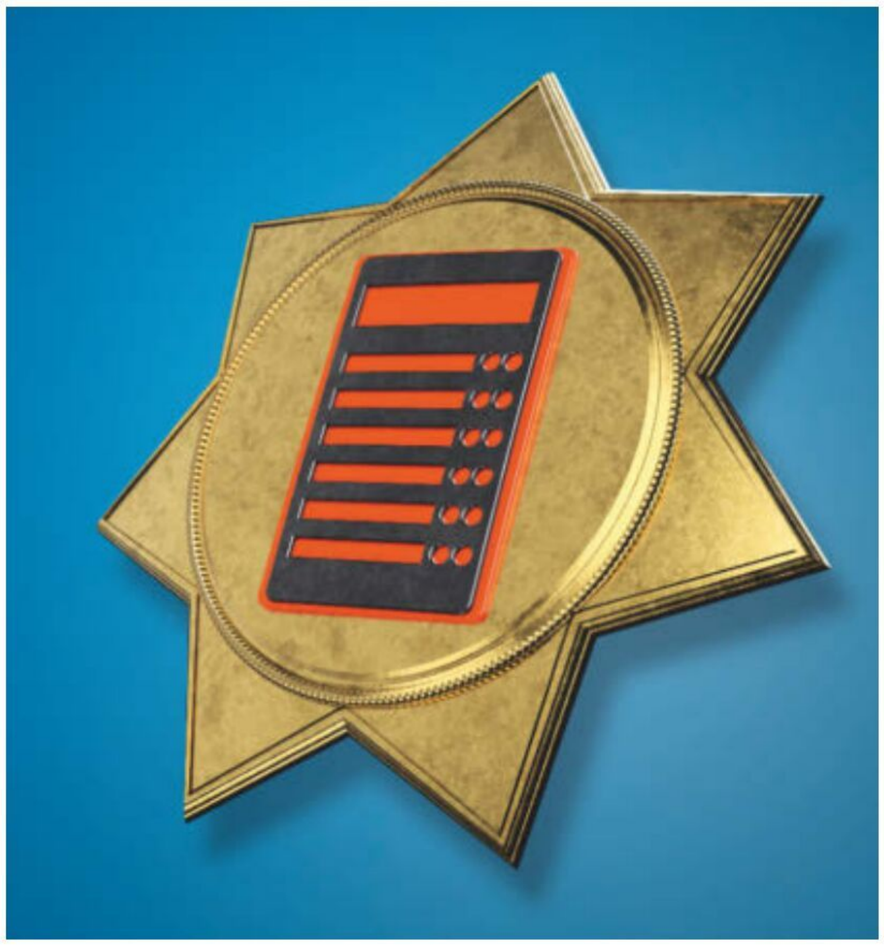


Bild: Andreas Martini

☑ Zweiten Faktor nutzen

Wenn Ihr Hoster einen zweiten Faktor für die Administrationsoberfläche anbietet, nutzen Sie diese Funktion. Ein einziges Kennwort als Schutz für die gesamten Web-Angebote eines Unternehmens ist heute nicht mehr zeitgemäß! Wer sich Zugang zur Verwaltungsoberfläche verschafft hat, 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 beim Kundenservice nach, ob die Funktion in Planung ist.

☑ Datenlecks schließen

Angreifer suchen gezielt nach veralteten Versionen von Servern und Skript-Interpretern, wenn diese bekannte Lücken enthalten. Extrem einfach macht man es ihnen, wenn der Server die Versionsnummern per HTTP-Header bei jedem Aufruf bereitwillig petzt. Die Gesprächigkeit der Webserver Nginx und Apache schränken Sie in der jeweiligen Konfigurationsdatei ein (Dokumentation siehe ct.de/wwd8). Der am häufigsten eingesetzten Skriptsprache PHP gewöhnen Sie das Rausposaunen mit `expose_php = Off` in der Datei php.ini ab. Um zu sehen, ob die Maßnahmen erfolgreich waren, öffnen Sie die Entwicklerwerkzeuge des Browsers (meist mit F12 oder Strg+Umschalt+I) und werfen einen Blick auf die Netzwerkanfragen und die Antworten des Servers.

☑ 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 gänzlich verhindern. Das macht Brute-Force-Attacken unmöglich. 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“. Angreifer, die es gezielt auf Ihren Server abgesehen haben, finden Ihren SSH-Server mit einem Portscan auch auf jedem anderen Port in endlicher Zeit.

☑ 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). Am besten

automatisieren Sie die Updates , damit sie regelmäßig ausgeführt werden.

Logfiles sollten Sie nicht nur 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. Eine Software wie Fail2ban (Unix) oder RdpGuard (Windows) entdeckt Brute-Force-Attacken in den Logs und sperrt die IP-Adressen der Angreifer automatisch. In großen Umgebungen sollten Sie das Monitoring all Ihrer Systeme auf einer Plattform zentralisieren, visualisieren und Alarme einrichten. Nur dann fallen Angriffe zeitnah auf.

☑ Mit Besuch rechnen

Ein per IPv4-Adresse 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 IP-Adressen des Internets durchprobieren und wird Ihre vermeintlich geheime Seite finden. Sichern Sie vertrauliche Informationen deshalb immer mit einem Kennwort. Auch wenn Sie Ihren Server nur per IPv6 zugänglich machen, wo die Wahrscheinlichkeit, zufällig entdeckt zu werden, wirklich gering ist, gehört ein Kennwort vor Ihre Server-Dienste. Welches Protokoll Sie auch für Ihre Dienste verwenden: Transportverschlüsselung (TLS 1.2 oder 1.3) ist Pflicht. TLS 1.0 und 1.1 sind unsicher und gehören abgeschaltet.

Konfigurationsanleitungen
ct.de/wwd8

☑ Passwörter hashen

Wenn Sie einen eigenen Dienst entwickeln, speichern Sie niemals Klartextpasswörter Ihrer Nutzer. Nutzen Sie stattdessen ein modernes Hash-Verfahren wie PBKDF2 und legen Sie nur die (gesalzenen) Hashes in Ihrer Datenbank ab. Speichern Sie darüber hinaus so wenig Daten wie möglich über Ihre Nutzer. Setzen Sie verbreitete Krypto-Bibliotheken ein, die von einer großen Community entwickelt wurden. Wenn Ihre Webanwendung mit personalisierten Links arbeitet, achten Sie darauf, dass diese ausreichend lang und zufällig sind, damit ein Nutzer keine fremden Daten sehen kann, wenn er Teile der URL ändert. (jam) c't

Make:
KREATIV MIT TECHNIK

DAS KANNST DU AUCH!

2× Make testen und 6 € sparen!

Ihre Vorteile:
✓ GRATIS dazu: Arduino Nano
✓ Zugriff auf Online-Artikel-Archiv*
✓ NEU: Jetzt auch im Browser lesen!
✓ Zusätzlich digital über iOS oder Android lesen

Für nur 15,60 Euro statt 21,80 Euro.

* Für die Laufzeit des Angebotes.

Jetzt bestellen:
make-magazin.de/miniabo

GRATIS!

Europas sicherster Cloud-Speicher

pCloud wurde 2013 in der Schweiz gegründet mit dem Ziel, einen gleichermaßen sicheren und nutzerfreundlichen Cloud-Speicher zu schaffen. Heute wird der Dienst von über 14 Millionen Benutzern verwendet, die einen einfachen Zugriff auf Ihre Dateien überall und zu jeder Zeit haben, ohne dabei die Sicherheit zu beeinträchtigen.

Schweizer Gesetze
Mit Sitz in der Schweiz unterliegt pCloud den Schweizer Datenschutzgesetzen, die zu den strengsten in Bezug auf die Daten einer Person gehören.

ISO 27001:2013
pClouds Rechenzentren sind nach SSAE 18 SOC 2 Typ II & SSAE 16 SOC 2 Typ II zertifiziert und erfüllen die höchste Stufe von physischen und technischen Sicherheitsanwendungen.

TLS/SSL-Kanalschutz
Alle Dateien, die in pCloud gespeichert werden, sind während der Datenübertragung und auf den Servern mit einer 256-Bit-AES-Verschlüsselung gesichert. Um die Sicherheit der Dateien weiter zu gewährleisten, verwendet pCloud auch das TLS/SSL-Protokoll bei der Übertragung von und zu den Servern.

Clientseitige Verschlüsselung
Benutzer können die clientseitige Verschlüsselung für ihre vertraulichen Dateien aktivieren. pCloud Encryption ist eine zusätzliche Dateischutzschicht, die Dateien direkt auf dem lokalen Gerät verschlüsselt, bevor sie auf die pCloud-Server hochgeladen werden, wodurch die Möglichkeit von Datenlecks oder unbefugtem Zugriff verhindert wird.

GDPR
pCloud erfüllt alle Anforderungen der europäischen Datenschutzgrundverordnung (EU-DSGVO).

Zero-Knowledge-Protokoll
Weder pCloud als Dienstanbieter noch irgendeine Behörde oder ein Dienst werden jemals Zugang zu den verschlüsselten Dateien haben.

Scannen Sie diesen QR-Code und erhalten Sie 3 Monate pCloud Premium 500 GB kostenlos. Oder folgen Sie diesem Link:
www.pCloud.com/heise

pCloud

Fritzboxen sicher betreiben

Gescheiterte Anmeldeversuche am Webinterface der Fritzbox zeigen, dass Cyber-Schurken massenhaft versuchen, die Kontrolle über schlecht gesicherte AVM-Router zu übernehmen. Mit wenigen Handgriffen schützen Sie sich vor diesen und weiteren Angriffen.

Von **Ronald Eikenberg**

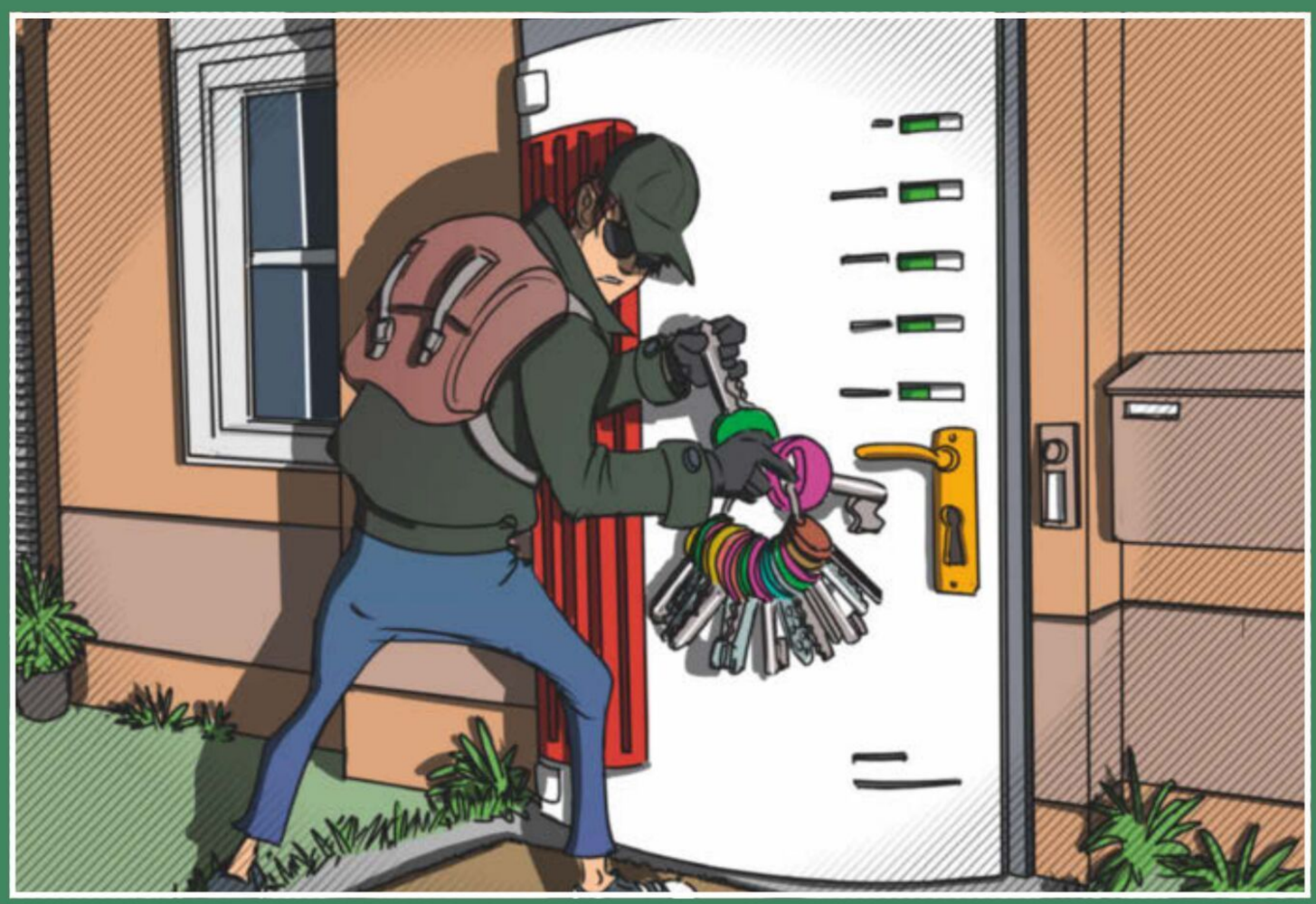


Bild: Thorsten Hübner

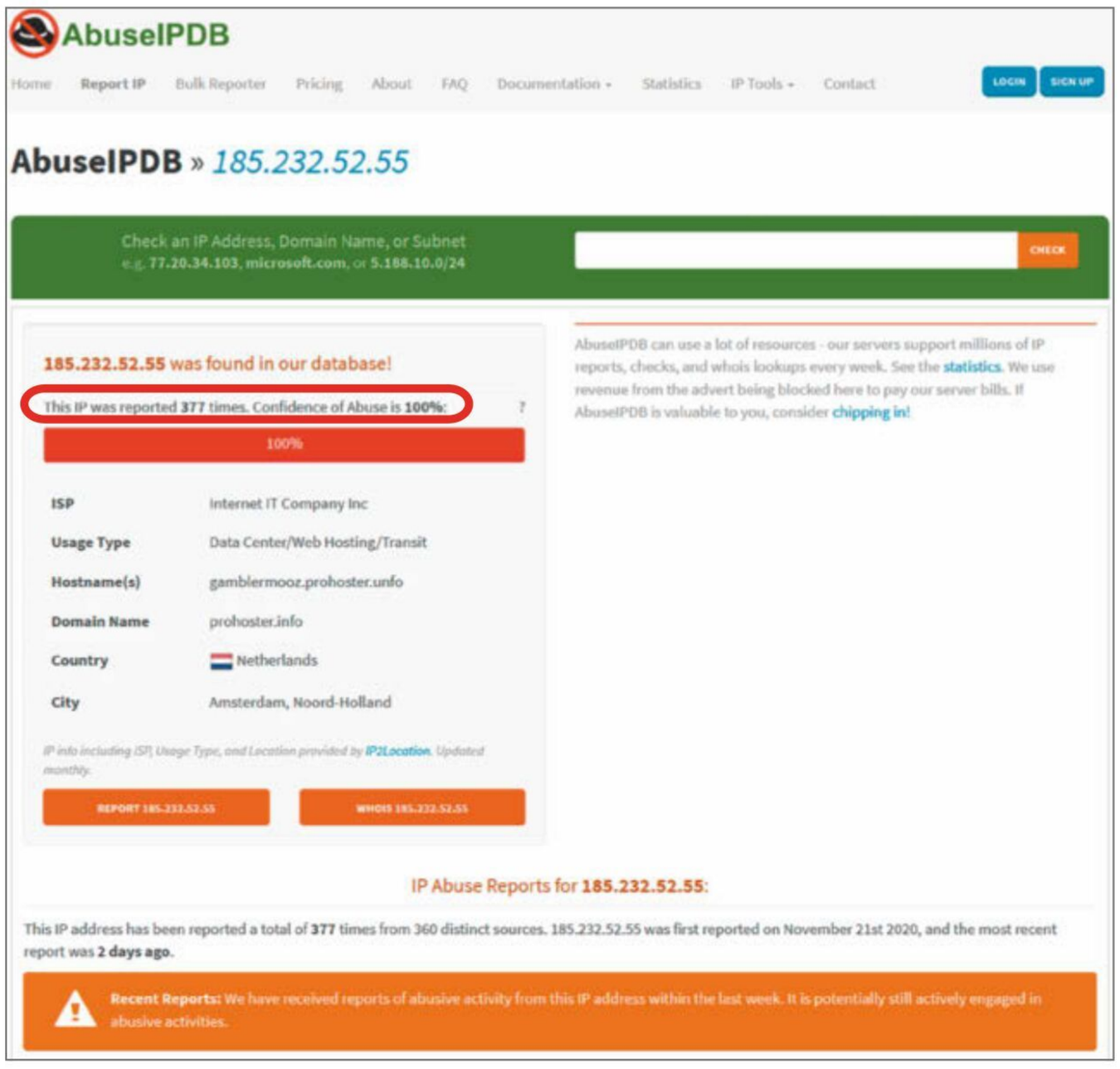
Fritzboxen sicher betreiben	34
NAS sicher betreiben	44
Netzwerkabklopfer	52
WLAN-Alarmanlage	54

Mit zunehmender Häufigkeit erreichen uns Zuschriften von Lesern, denen beunruhigende Aktivitäten im Ereignis-Log Ihrer Fritzboxen auffallen. Ein zufälliges ausgewähltes Beispiel: „Seit drei Tagen sind in der Logdatei meiner Fritzbox vermehrt Einbruchversuche von der IP-Adresse 185.232.52.55 zu verzeichnen. […] Auch wenn ich ein starkes Passwort einsetze, ist es doch ein komisches Gefühl.“ Unbekannte versuchen demnach, sich am Webinterface der Fritzboxen anzumelden – und das immer wieder, oft über einen langen Zeitraum. Häufig gehen diese Anmeldeversuche von der gleichen IP-Adresse aus, bei mehreren Lesern versuchte sich etwa ein Nutzer der IP-Adresse 185.232.52.55 etliche Male einzuloggen.

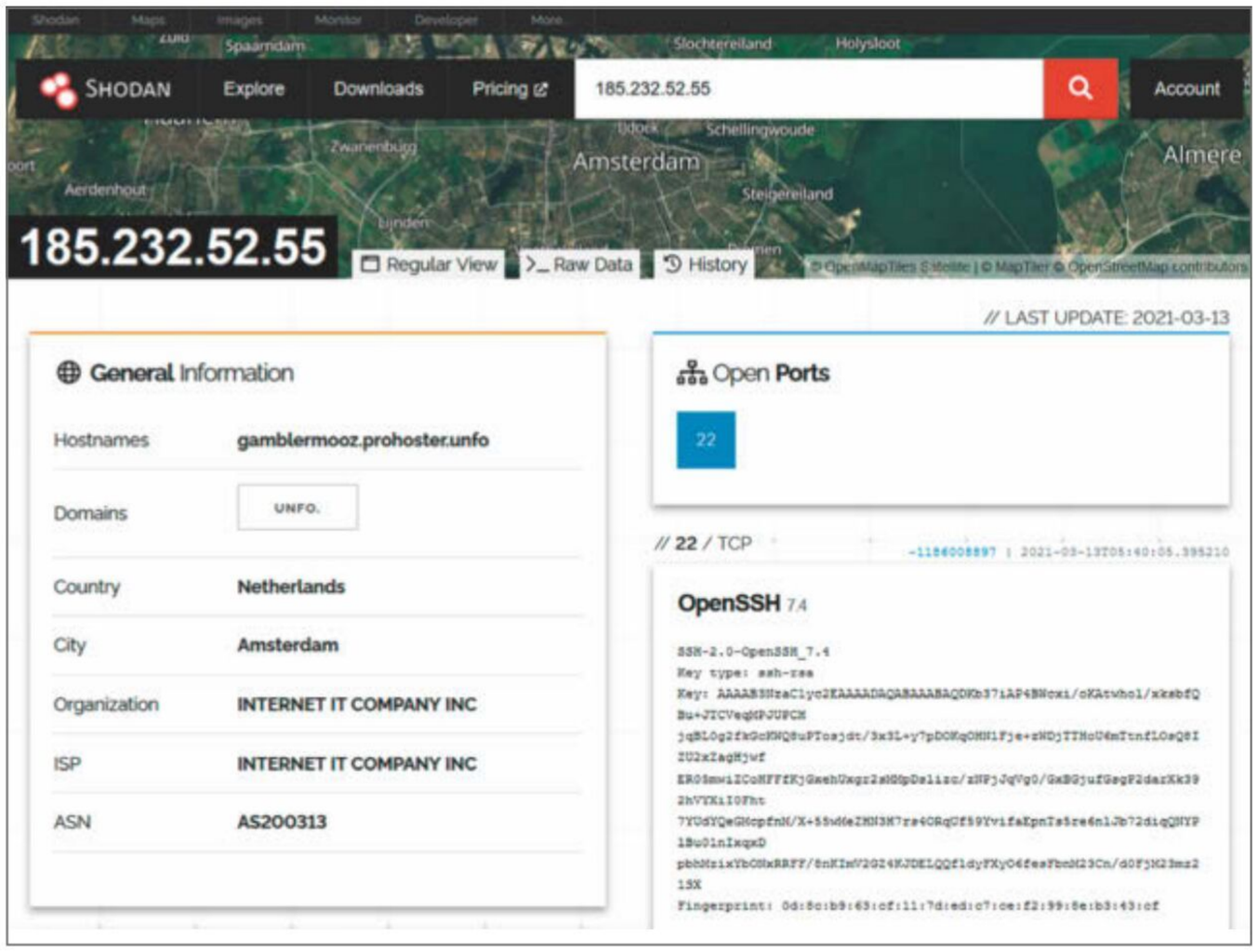
Gibt man diese Adresse bei Google ein, landet man schnell bei AbuseIPDB, einer Website, auf der man IP-Adressen melden kann, die sich auffällig verhalten. Zu 185.232.52.55 findet man dort bereits Hunderte Beschwerden. Die meisten kommen von Nutzern aus Deutschland und betreffen Vorkommnisse der Kategorien Hacking und Brute-Force. Zumeist wird die Fritzbox als Angriffsziel genannt. Recherchiert man weiter, zeigt sich auffälliges Verhalten, das von der IP-Adresse bereits seit Sommer 2020 ausgeht und AVM-Router zum Ziel hat.

Aber wer steckt dahinter? Laut einer Whois-Abfrage gehört die IP-Adresse zu einem Unternehmen namens „Internet IT Company Inc.“, das offenbar auf den Seychellen angemeldet wurde. Als Abuse-Kontakt ist eine Freemail-Adresse bei Yandex.ru angegeben – nicht gerade vertrauenerweckend. Etwas mehr verrät der Portscan-Dienst Shodan: Er verortet die Adresse in Amsterdam und ordnet ihr die Domain gamblermooz.prohoster.unfo zu.

Laut Shodan ist unter der IP-Adresse lediglich ein OpenSSH-Server erreichbar. Das spricht dafür, dass dahinter nicht etwa ein infizierter Desktop-Rechner steckt, sondern eher ein Serversystem in einem Rechenzentrum. Da die OpenSSH-Version mit 7.4 reichlich alt ist und Sicherheitslücken enthält, erscheint denkbar, dass es sich um einen vergessenen Server-



Ein Nutzer der IP-Adresse 185.232.52.55 versucht offenbar, sich in etliche Fritzboxen einzuloggen. Allein bei AbuseIPDB findet man Beschwerden Hunderter Fritzbox-Nutzer.



Der Internetscanner Shodan vermutet hinter den Angriffen einen Server aus Amsterdam.

Zombie handelt, der übernommen wurde und nun fremdgesteuert wird.

Wer auch immer dahintersteckt, man muss davon ausgehen, dass er keine redlichen Absichten hegt. Denn eine Fritzbox ist ein hochattraktives Angriffsziel. Die Täter gehen bei der Wahl ihrer potenziellen Opfer anscheinend wahllos vor; vermutlich scannen sie stumpf weite Teile des deutschen Internets nach Fritzboxen, deren Webinterface von außen erreichbar ist. Offenbar haben es die Angreifer vornehmlich auf den HTTPS-Standardport 443 abgesehen. Als Benutzernamen probieren sie unter anderem zahllose Mailadressen durch, meist mit .de-Endung. In einem uns bekannten Fall geht aus dem Ereignisbericht der Fritzbox hervor, dass eine Liste mit Mailadressen deutscher Kleinunternehmer zum Einsatz kam (kontakt@[domain].de). Unklar bleibt, ob die Adressen aus öffentlichen Quellen stammen oder irgendwo mit dazu passenden Passwörtern entwendet wurden.

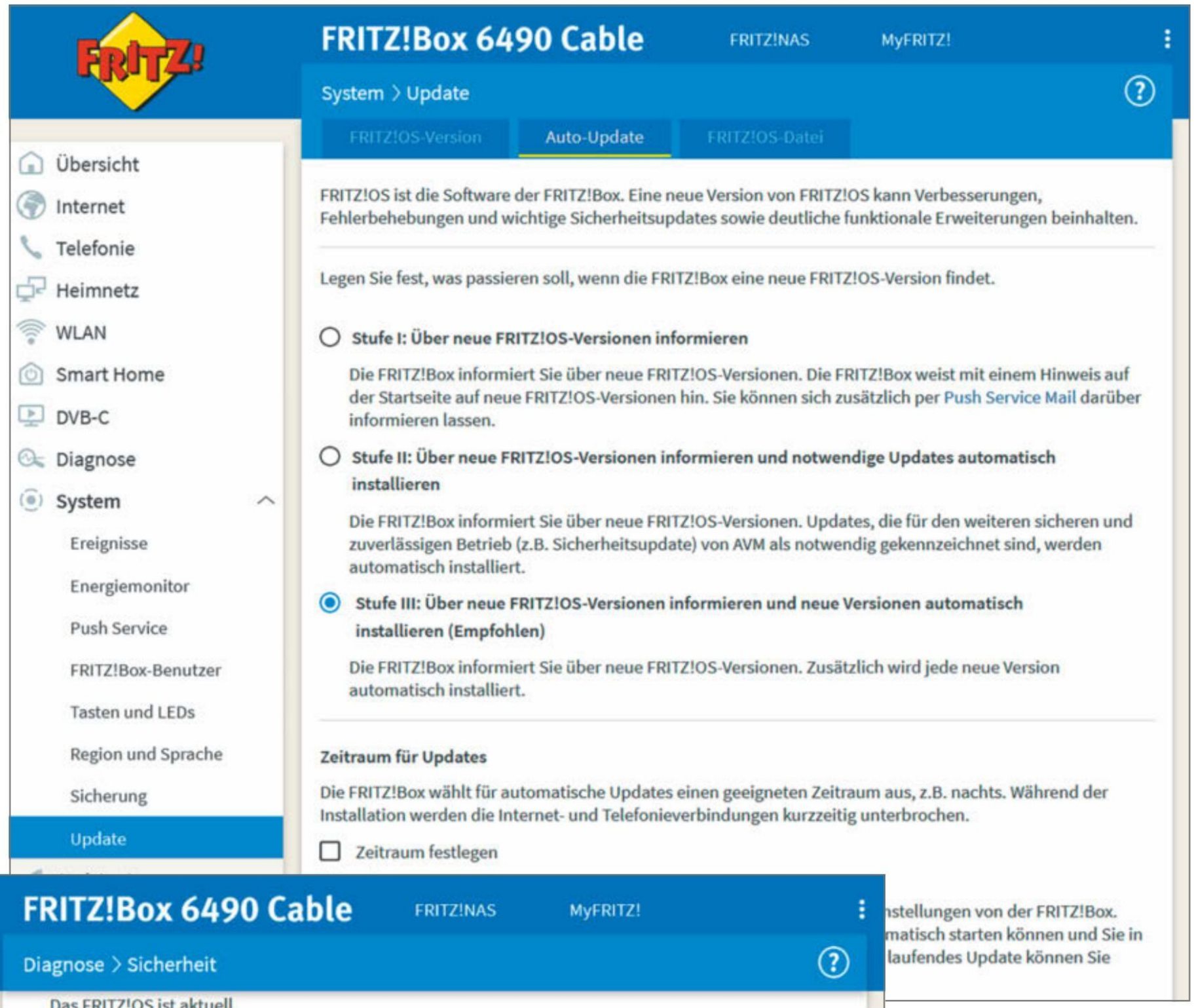
Wer solche Login-Versuche in seinem Fritzbox-Log entdeckt, sollte nicht gleich in Panik verfallen. Es handelt sich erst mal nur um gescheiterte Anmeldungen. Die Situation ist vergleichbar mit einem Einbruchsversuch, bei dem ein Angreifer vor Ihrer Haustür steht und auf gut Glück einen großen Bund mit Schlüsseln durchprobiert. Passt keiner der vielen Schlüssel, zieht der Möchtegern-Einbrecher unverrichteter Dinge weiter. Das ist ohne jede Frage unangenehm, doch noch nicht gefährlich – schließlich bleibt in diesem Fall die Haustür verschlossen.

Einbruchschutz

Damit das auch so bleibt, sollten Sie die Einbruchsversuche zum Anlass nehmen, Ihr Schutzkonzept zu überprüfen und zu verbessern. Denn spätestens, wenn der Einbrecher vor Ihrer Tür steht, kann man nicht mehr von einer theoretischen Gefahr sprechen. Sie ist sehr konkret. Im besten Fall sorgen Sie dafür, dass ein potenzieller Einbrecher das Login-Formular – und damit das gesamte Webinterface der Fritzbox – gar nicht erst erreichen kann. Wenn Sie ohnehin nicht von unterwegs auf Ihren Router oder dessen Dienste zugreifen, dann besteht kein Grund, ihn aus dem Internet erreichbar zu machen.

Bevor Sie mit dem Sicherheits-Check loslegen, sollten Sie sicherstellen, dass das Fundament stabil ist: Öffnen Sie die Weboberfläche des Routers, die Sie aus Ihrem Netz über http://fritz.box erreichen und stellen Sie im Menü System / Update sicher, dass die aktuelle Firmware (FritzOS) installiert ist. Klicken Sie unten rechts auf „Neues FRITZ!OS suchen“, um die Update-Suche anzustoßen. Falls es ein Update gibt, sollten Sie es gleich einspielen. Der Grund ist simpel: Firmware-Updates können nicht nur neue

Regelmäßige Firmware-Updates sind essenziell. Am besten lässt man sie automatisch einspielen.



Alles auf einen Blick: Im Menü Diagnose/ Sicherheit führt die Fritzbox viele sicherheitsrelevante Einstellungen auf. Dort finden Sie auch Dienste, die aus dem Internet erreichbar sind. Im Idealfall ist die Liste, so wie hier, leer.

Funktionen und Bugfixes mitbringen, sondern auch Sicherheits-Patches, die Schwachstellen im Router-Betriebssystem beheben.

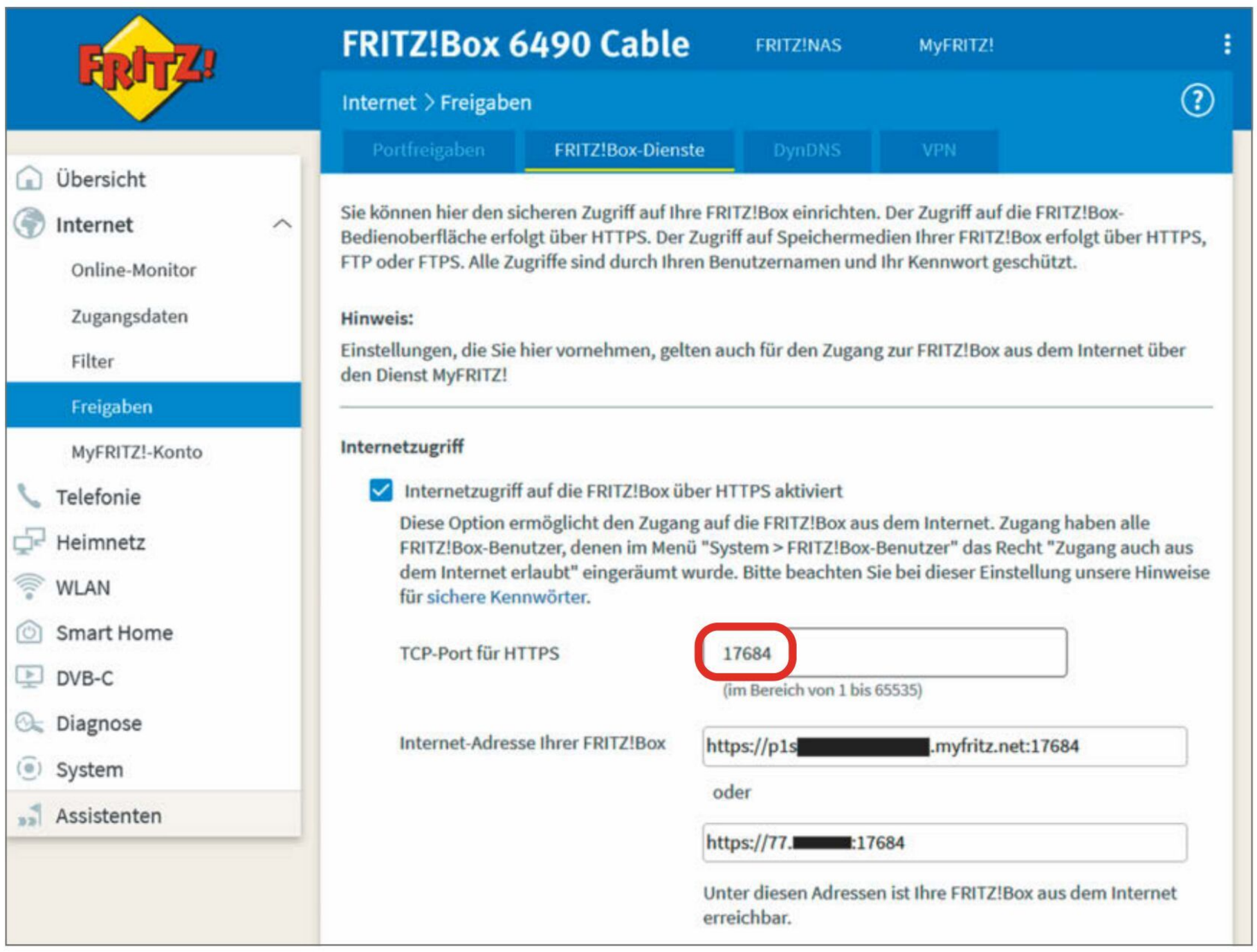
Statten Sie auch der Unterseite Auto-Update einen Besuch ab und aktivieren Sie mindestens die „Stufe II: Über neue FRITZ!OS-Versionen informieren und notwendige Updates automatisch installieren“, damit Ihr Router automatisch Updates einspielt, die der Hersteller als sicherheitsrelevant einstuft. Darunter können Sie bei „Zeitraum für Updates“ eine Startzeit für die automatischen Updates einstellen, um sicherzustellen, dass Sie von den Aktualisierungen nicht tagsüber aus dem Videocall mit dem Chef gerissen werden.

Eine Übersicht der Firmware-Versionen für die aktuellen Fritzbox-Modelle finden Sie unter ct.de/w25p. Falls Sie den AVM-Router von Ihrem Provider erhalten haben, dann können Sie Firmware-Updates möglicherweise nicht selbst installieren. Dies ist beispielsweise bei den Providern von Internet per TV-Kabel der Fall. In diesem Fall können Sie nur abwarten, bis Ihr Provider das Update einspielt.

Wenn Ihr Fritzbox-Modell nicht länger mit Firmware-Updates versorgt wird, dann ist es schon recht alt. Denken Sie in diesem Fall über eine Neuanschaffung nach. Eine moderne Fritzbox ist dank der aktuellen Firmware nicht nur sicherer, sondern durch die neuere Hardware auch flotter. Es muss nicht zwangsläufig das aktuelle und teure Spitzenmodell sein. Je nach Anforderungen reicht auch das gebrauchte Top-Modell von vor zwei Jahren für einige Zeit aus.

Fenster und Türen verschließen

Steht das Firmware-Fundament, dann können Sie sich einen Überblick über die allgemeine Sicherheitslage verschaffen. Öffnen Sie im Webinterface im Menü Diagnose / Sicherheit den Sicherheitsbericht, der die relevanten Einstellungen übersichtlich zusammenfasst. Die aus dem Internet erreichbaren



Ändert man die Ports der Fritzbox-Dienste auf hohe, zufällig gewählte, klopft ungebetener Besuch deutlich seltener an.

Dienste finden Sie gleich oben, etwa unter „1. Verbindung, Internet“: Bei FRITZ!Box-Dienste führt der Router eigene Dienste auf, die für Zugriffe aus dem Internet erreichbar sind und unter „Portfreigaben auf Heimnetzgeräte“ erfahren Sie, welche Dienste anderer Geräte im Heimnetz von außen zugänglich sind.

Im Idealfall sind beide Listen leer, denn jeder öffentlich erreichbare Dienst ist ein Angriffsziel. Sind Dienste direkt aus dem Internet zugänglich, werden sie zwielichtige Gestalten eher früher als später attackieren, um etwaige Zugangsbeschränkungen wie Passwortabfragen zu brechen oder Sicherheitslücken auszunutzen. Schlimmstenfalls hat der Angreifer anschließend nicht nur den attackierten Dienst im Griff, sondern Ihr gesamtes Heimnetz.

Wenn Sie von unterwegs auf Ihr Heimnetz zugreifen möchten, nutzen Sie stattdessen besser eine verschlüsselte VPN-Verbindung [1]. Falls Sie doch einmal Dienste direkt von außen erreichbar machen wollen oder müssen, dann sollten Sie darauf achten, dass diese auf dem aktuellen Software-Stand sind und zudem auf eine sichere Authentifizierung setzen: starke, lange Passwörter sowie Zwei-Faktor-Authentifizierung, wenn möglich.

Falls Sie überflüssige Dienstefreigaben im Sicherheitsbericht der Fritzbox entdecken, sollten Sie diese im Menü Internet / Freigaben deaktivieren. Im Bereich Portfreigaben finden Sie die Weiterleitungen ins interne Netz und unter FRITZ!Box-Dienste die öffentlich erreichbaren Dienste der Fritzbox. Wenn Ihnen die eingangs beschriebenen Zugriffsversuche im Ereignis-Log der Fritzbox (System / Ereignisse) aufgefallen sind, dann haben Sie das Webinterface und / oder den FTP-Dateiserver des Routers für Zugriffe aus dem Internet freigegeben. Falls das unbeabsichtigt geschah, dann machen Sie es rückgängig, indem Sie bei den Fritzbox-Diensten im Bereich Internetzugriff die Häkchen bei „Internetzugriff auf die FRITZ!Box über HTTPS aktiviert“ und „Internetzugriff auf Ihre Speichermedien über FTP / FTPS aktiviert“ entfernen und die Konfigurationsänderungen übernehmen.

Falls Sie auf einen oder beide Dienste nicht verzichten können, sollten Sie zumindest sicherstellen, dass nicht die Standardports 443 für HTTPS und 21 für FTP eingestellt sind. Damit verhindern Sie die unbefugten Zugriffsversuche zwar nicht, sie werden aber seltener, da Angreifer häufig nur die Standardports abklopfen – das aber bei sehr vielen IP-Adressen. Nur wenn es jemand wirklich auf Sie abgesehen hat, wird er sich die Mühe machen, andere Ports zu scannen, etwa solche im fünfstelligen Bereich.

Der Portbereich reicht bis 65535. Seit FritzOS 7.10 schlägt die Fritzbox automatisch einen zufälligen Port für HTTPS vor, wenn Sie den Fernzugriff aktivieren. Überprüfen Sie die Einstellung insbesondere dann, wenn die Funktion schon längere Zeit aktiv ist oder gar noch eine ältere FritzOS-Version läuft. Um Angreifern das Auffinden offener Ports nicht leichter als nötig zu machen, sollten Sie in Internet / Filter / Listen / Globale Filtereinstellungen die Option „Firewall im Stealth Mode“ einschalten. Das erschwert den Angreifern die erforderlichen Portscans sehr, weil die Fritzbox nun nicht mehr mit einem Lebenszeichen reagiert (Zugriff verweigert), sondern stumm bleibt.

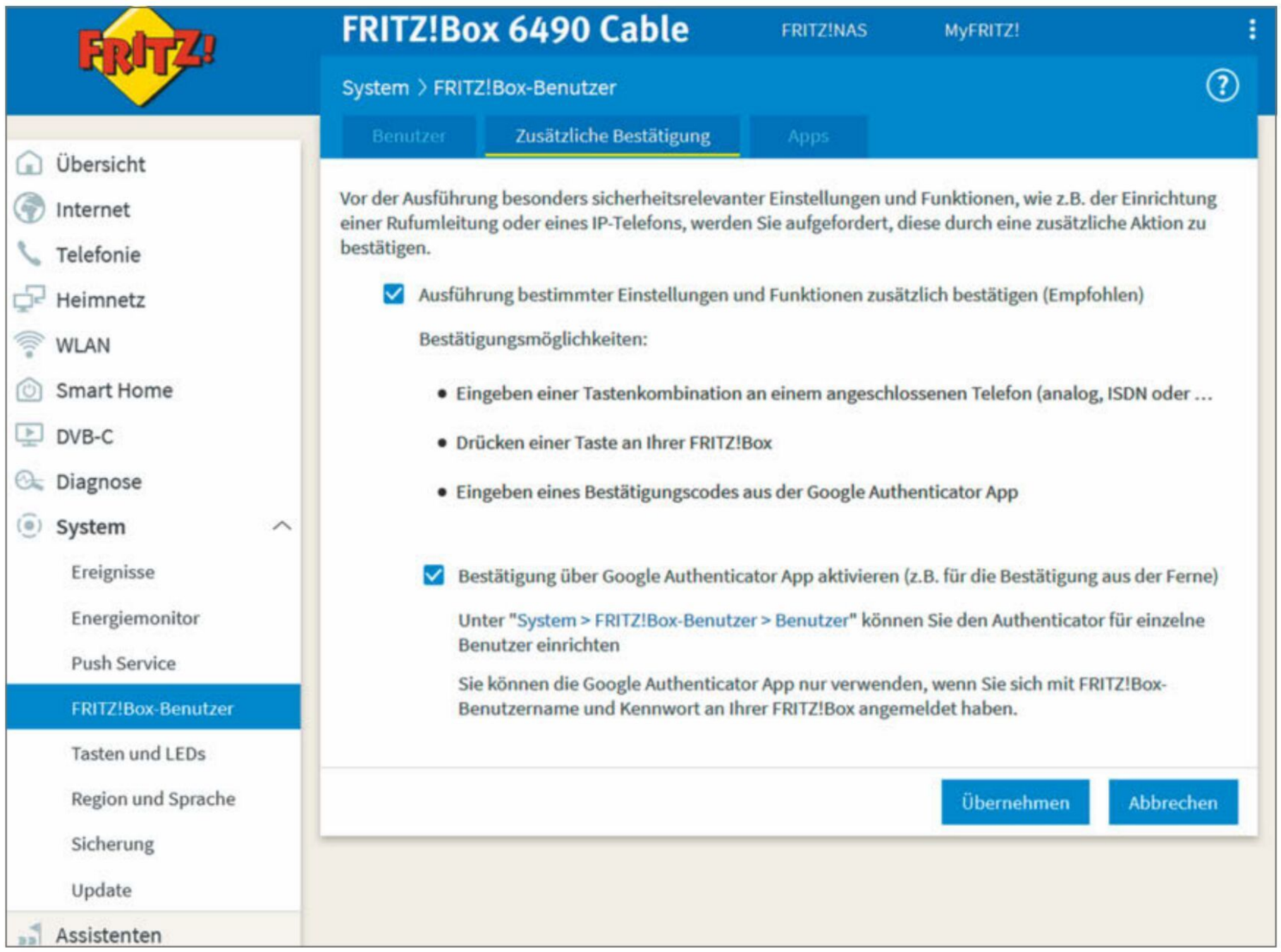
Sicherheitsschloss installieren

Falls ein Angreifer das Webinterface auf dem exotischen Port entdeckt, wird er mit einem Login-Dialog konfrontiert, in das er einen Benutzernamen und ein Passwort eingeben muss. Nur wenn beide Angaben stimmen, bekommt er Zugang zur Fritzbox. Machen Sie es ihm so schwer wie möglich, indem Sie sowohl einen individuellen, schwer zu erratenden Usernamen als auch ein sicheres Passwort einstellen. Wechseln Sie hierzu in das Menü System / FRITZ!Box-Benutzer. Anschließend können Sie einen Benutzereintrag ändern oder einen neuen anlegen. Sowohl beim Benutzernamen als auch beim Kennwort können Sie Ihrer Kreativität freien Lauf lassen – je länger, desto besser. Wichtig ist nur, dass Sie die korrekte Zeichenfolge beim späteren Fernzugriff auf die Fritzbox parat haben. Der Einsatz einer Gedächtnisstütze ist ratsam, etwa in Form eines Passwortmanagers oder eines Zettels im Portemonnaie.

Gehen Sie alle angelegten Benutzer durch und misten Sie gründlich aus. Das Häkchen bei „Zugang auch aus dem Internet erlaubt“ sollte, wenn überhaupt, nur bei Konten mit individuellem Benutzernamen und starkem Passwort gesetzt sein. Bei dieser Gelegenheit sollten Sie auch die Berechtigungen überprüfen. Es ist eine gute Idee, den Nutzern nur jene Berechtigungen zu erteilen, die sie wirklich brauchen und alle übrigen Rechte zu entziehen. Sinnvoll ist auch, mit mehreren Konten für verschiedene Zwecke zu arbeiten: So muss etwa der Nutzereintrag, mit dem Sie auf den Netzwerkspeicher der Fritzbox zugreifen, nicht gleichzeitig die Router-Einstellungen ändern dürfen.

Stellen Sie auf der Unterseite „Zusätzliche Bestätigung“ sicher, dass die Option „Ausführung

Hinter dem Push-Service Änderungsnotiz verbirgt sich eine äußerst nützliche Benachrichtigungsfunktion, die den Fritzbox-Besitzer per Mail über sicherheitsrelevante Änderungen an den Einstellungen sowie über Anmeldungen an der Bedienoberfläche informiert.



Zum Ändern wichtiger Einstellungen, etwa von Rufumleitungen, sollte eine zusätzliche Bestätigung erforderlich sein – etwa durch das Drücken einer Taste am Router oder per OTP-App.

bestimmter Einstellungen und Funktionen zusätzlich bestätigen (Empfohlen)“ eingeschaltet ist. Dann müssen Sie beim Ändern folgenreicher Einstellungen gesondert bestätigen, dass Sie vor Ort und somit wahrscheinlich dazu berechtigt sind. Hierzu drücken Sie einfach eine Taste am Router oder tippen einen vorgegebenen Code ins Festnetztelefon ein.

Recht neu ist die Möglichkeit, wichtige Änderungen aus der Ferne zu bestätigen. Das ist sehr nützlich, wenn Sie die Router-Konfiguration von unterwegs ändern möchten. Hierzu setzt AVM auf das bewährte OTP-Verfahren (One Time Password): Sie verknüpfen einen OTP-Generator wie die Google-Authenticator-App oder andOTP per QR-Code-Scan mit der Fritzbox und können anschließend kurz gültige Einmalcodes generieren, mit denen Sie sicherheitskritische Einstellungen aus der Ferne ändern dürfen. Der Einmalcode ersetzt den Knopfdruck am Router. Leider ist es noch nicht möglich, schon das Einloggen am Webinterface der Fritzbox mit diesem Zweitfaktor zu schützen.

Wenn Sie schon mal den Bereich FRITZ!Box-Benutzer offen haben, sollten Sie dort im Bereich Apps nicht länger genutzten Anwendungen die Zugriffsrechte entziehen. Klicken Sie dazu neben einem Eintrag auf das rote X.

Alarmanlage scharfschalten

Um über verdächtige Aktivitäten auf dem Laufenden zu bleiben, sollten Sie von Zeit zu Zeit das Ereignis-Log im Menü System / Ereignisse kontrollieren. Setzen Sie den Filter oben auf System, um Anmeldeversuche an den Fritzbox-Diensten zu inspizieren; mit dem Filter Alle bekommen Sie unter anderem auch WLAN-Anmeldeversuche mit.

Über System / Push Service kann die Fritzbox per Mail über diverse Ereignisse informieren. Sie müssen zunächst unter Absender ein Mailkonto konfigurieren, das die Fritzbox zum Versand nutzen soll. Legen Sie für diesen Zweck am besten ein separates Konto an, damit Sie nicht das Kennwort Ihres primär genutzten Mailzugangs in der Fritzbox hinterlegen müssen. Schalten Sie dann den Push-Service Änderungsnotiz ein und abonnieren Sie „Über Anmeldungen an der Benutzeroberfläche informieren“, um keine erfolgreiche Anmeldung zu verpassen. Stöbern Sie nach weiteren Ereignissen, die Sie interessieren – Ihre Fritzbox kann Sie per Mail zum Beispiel auch über die Verfügbarkeit neuer Firmware benachrichtigen.

Netzwerkcheck

Um den Erfolg der getroffenen Schutzmaßnahmen zu überprüfen, können Sie zum Beispiel den Netzwerkcheck von heise Security benutzen (siehe ct.de/w25p): Er scannt Ihre aktuelle Internet-IPv4-Adresse nach offenen Standard-Ports und warnt, sollte er fündig werden. Damit versetzen Sie sich in die Perspektive eines Angreifers, der nach Schlupflöchern sucht. Wenn Sie alle Dienste nach außen gekappt haben, sollte der Netzwerkcheck keine oder nur sehr wenige Ports entdecken. Es gibt wenige Ports, die die Fritzbox selbstständig nach außen offenhält, damit Router-eigene Dienste wie die VoIP-Telefonie laufen. Laut AVM-Dokumentation sind dies: TCP-Port 21 (FTP/FTPS), TCP-Port 443 (Fernzugriff auf Weboberfläche, wenn mit alter FritzOS-Version aktiviert), UDP-Port 500 und 4500 (VPN), TCP- und UDP-Port 5060 (VoIP), UDP-Port 7078-7109 (VoIP) sowie TCP-Port 8089 (TR-069).

Sollten diese Ports in den Ergebnissen des Netzwerkchecks stehen, gibt es dafür also einen guten Grund. Die ersten Ports für FTP(S), Weboberfläche und VPN stehen dort nur, wenn Sie die zugehörigen Fritzbox-Funktionen aktiviert haben, die Telefonie-Ports nur, wenn VoIP eingerichtet ist. Beachten Sie, dass der Netzwerkcheck von heise Security derzeit nur IPv4-Adressen abklappert. Bei Fritzboxen darf man davon ausgehen, dass die Ergebnisse auch für deren aktuelle globale IPv6-Adresse gelten.

Ungebetene Besucher aus dem Internet sind nicht nur eine Gefahr, vor der Sie Ihren Router schützen müssen. Auch die Funkstrecke muss abgesichert werden, damit sich Ihre Nachbarn nicht in Ihrem Heimnetz umschauen oder ungefragt über Ihren Anschluss surfen und Dinge tun, für die später Sie den Kopf hinhalten müssen.

Die gute Nachricht ist, dass Sie damit nur wenig Arbeit haben. Stellen Sie unter WLAN / Sicherheit / WPA-Verschlüsselung am besten „WPA 2 + WPA3“ (WPA3-Mixed-Mode) ein, damit moderne Geräte, die bereits WPA3 verwenden, die bestmögliche Verschlüsselung einsetzen. Ältere Geräte wählen dann automatisch die WPA2-Verschlüsselung, die weiterhin ausreichend sicher ist. Wenn Sie diesen Modus wählen, sollte unter „Weitere Sicherheitseinstellungen“ die Option „Unterstützung für geschützte Anmeldungen von WLAN-Geräten (PMF) aktivieren“ aktiv sein. Einen ausführlichen Hintergrundartikel über die Vor- und Nachteile von WPA3 finden Sie im Sonderheft c’t Fritzbox [2].

Perspektivwechsel: Mit dem Netzwerkcheck von heise Security begeben Sie sich in die Rolle eines Angreifers und überprüfen, ob Dienste über Ihre IPv4-Adresse auf den Standardports erreichbar sind.

Einige alte Geräte haben im WPA3-Mixed-Mode möglicherweise Probleme mit dem Verbindungsaufbau, zum Beispiel alte iPads, die Apple seit Jahren nicht mehr mit iOS-Updates versorgt. Statt für solche Problemfälle die Sicherheit Ihres Haupt-WLANs und damit aller Geräte zu reduzieren, können Sie einfach das Gastnetz der Fritzbox mit der Verschlüsselung WPA2 (CCMP) aufspannen und die betroffenen Geräte dort einbuchen. Sie finden es unter WLAN / Gastzugang. Das vom Hauptnetz separierte Gastnetz ist auch der richtige Ort für alle Clients, denen Sie nicht über den Weg trauen sowie für Ihre Gäste, denen Sie zwar Internetzugriff spendieren möchten, die aber nicht aufs Heimnetz zugreifen sollen.

Falls Sie das WLAN-Passwort aushändigen, sollten Sie es von Zeit zu Zeit ändern, um die Kontrolle über die Nutzung zu behalten. Unter „Weitere Einstellungen“ können Sie noch etwas Feintuning betreiben: Aktivieren Sie zum Beispiel den Push-Service, um ein Protokoll über die An- und Abmeldungen am Gastnetz per Mail zu erhalten. Unter „Geräte im Gastzugang oder Hotspot“ sollte die Option „WLAN-Geräte dürfen untereinander kommunizieren“ ausgeschaltet und „Internetanwendungen beschränken“ eingeschaltet sein, damit Ihre Gäste nur surfen und mailen können.

Nutzen Sie für Ihre Funknetze möglichst lange Passwörter (WLAN-Netzwerkschlüssel), um es Angreifern schwer zu machen. Das voreingestellte Passwort sollten Sie ändern, da es lediglich aus Ziffern besteht. Nutzen Sie einen mindestens 16 Zeichen langen Mix aus Groß- und Kleinbuchstaben sowie Ziffern. Durch den Einsatz von Sonderzeichen können Sie die Komplexität erhöhen.

Achten Sie jedoch darauf, dass Sie das Passwort auf allen Geräten gut eintippen können – auch mit der Fernbedienung des Smart-TV und dem Controller der Spielekonsole. Auf allzu exotische Sonderzeichen sollten Sie deshalb besser verzichten, machen Sie das Passwort stattdessen lieber etwas länger. Auch sich optisch ähnelnde Zeichen wie 1, l und I sowie 0 und O erhöhen lediglich das Frustrationspotenzial.

Das Gastnetz sollten Sie unbedingt mit einem anderen Passwort schützen als Ihr Hauptnetz. Darüber hinaus sollten Sie in WLAN / Sicherheit / WPS-Schnellverbindung die Komfortfunktion WPS (Wi-Fi Protected Setup) abschalten, da sich Ihre Gäste ansonsten einfach per Knopfdruck am Router mit Ihrem Hauptnetz verbinden und sogar dessen WLAN-Passwort einsehen können. Sie können die Funktion bei Bedarf vorübergehend wieder aktivieren, etwa wenn Sie neue Geräte mit dem Router

Literatur

[1] Urs Mansmann, **Tunnel durchs Internet**, Mobile Geräte mit VPN sicher ins Netz bringen, c’t 3/2016, S. 126

[2] Dr. Alfred Arnold, Ernst Ahlers, **Extrasicheres WLAN** mit WPA3, c’t Fritzbox 2021, S. 60

Firmware-Versionen & Netzwerkcheck

ct.de/w25p

verbinden möchten, ohne immer wieder das Passwort eingeben zu müssen.

Hintertüren absichern

Damit Ihr Schutzwall nicht gleich wieder eingerissen wird, sollten Sie abschließend noch einen Blick auf UPnP werfen: Über das UPnP-Protokoll können Geräte in Ihrem Heimnetz Ihre Fritzbox nicht nur finden, sondern auch umkonfigurieren. Das kann gefährlich werden: Wenn es ganz schlecht läuft, dann ist die neue WLAN-Kamera von Discounter nicht nur unsicher vorkonfiguriert, sie richtet sich über UPnP auch noch eine Portweiterleitung im Router ein. Dann ist sie fortan für die ganze Welt erreichbar und mit Pech auch noch als DDoS-Server und andere Angriffe dienstbar – ganz ohne Ihr Zutun.

In Heimnetz / Netzwerk / Netzwerkverbindungen spüren Sie Geräte auf, die via UPnP an der Fritzbox-Konfiguration schrauben dürfen. Klicken Sie bei Ihren Geräten auf das Stift-Symbol, um die jeweiligen Einstellungen zu öffnen. Hier sollte die Funktion „Selbstständige Portfreigaben für dieses Gerät erlauben“ ausgeschaltet sein, damit die Geräte nicht eigenmächtig Port-Weiterleitungen im Router einrichten. Unter Internet / Freigaben / Portfreigaben können Sie ganz unten über den Deaktivieren-Knopf die selbstständige Portfreigabe zudem für alle Geräte deaktivieren, die bisher keine Freigaben angelegt haben.

Falls Sie Ihre Fritzbox ausschließlich über das Webinterface konfigurieren und zudem keine AVM-Apps wie FRITZ!App Fon nutzen, können Sie unter „Heimnetz / Netzwerk / Netzwerkeinstellungen / weitere Einstellungen“ die Funktion „Zugriff für Anwendungen zulassen“ abschalten. Damit verhindern Sie, dass Ihre Fritzbox über das TR-064-Protokoll gesteuert wird. Da TR-064 eine Authentifizierung voraussetzt, ist das davon ausgehende Sicherheitsrisiko allerdings überschaubar, sofern Sie Ihre Fritzbox-Accounts mit starken Passwörtern schützen. Beachten Sie, dass Sie damit auch einige Drittanbieter-Apps und Skripte aussperren, welche die Box über TR-064 steuern. (rei) c't

c't Fotografie

Das Magazin von Fotografen für Fotografen

Porträtfotograf und c't Fotografie-Autor

Tilo Gockel, Fotografiert u. a. für Spiegel-Online, Vogue.it, Pablo-Magazin, DIGIT

„Porträts? Sind hart und stressig... und damit die interessanteste Art von Aufnahmen! :-)“

Tilo Gockel, Fotopraxis.net

+

2 × c't Fotografie testen

- **2 Ausgaben** kompaktes Profiwissen für 14,30 €
- 35 % Rabatt gegenüber Einzelheftkauf
- Inkl. Geschenk nach Wahl

Jetzt bestellen:

www.ct-foto.de/miniabo

www.ct-foto.de/miniabo +49 541/80 009 120 leserservice@heise.de

Bild: Andreas Martini

NAS sicher betreiben

Ein rätselhafter Fall: Statt seiner Daten fand unser Leser Gunther J. nur noch ein Erpresserschreiben auf seinem NAS. Er ahnte noch nicht, dass sich der Netzwerkspeicher sein eigenes Datengrab geschaufelt hatte. So kam es dazu – und so schützen Sie sich.

Von **Ronald Eikenberg**

Als c't-Leser Gunther J. seine Urlaubsfotos durchstöbern wollte, erlebte er eine unangenehme Überraschung: Alle Dateien auf dem ansonsten zuverlässigen NAS waren gelöscht. Stattdessen entdeckte er eine Datei namens „DATA RECOVERY ! ! !!.txt“, die wie folgt beginnt: „YOUR REMOTE STORAGE WAS COMPROMISED. YOUR FILES ARE IN OUR POSSESSION.“ J. war offenbar Opfer einer Cyber-Gang geworden, die sich an seinen Urlaubsfotos zu schaffen gemacht hatte.

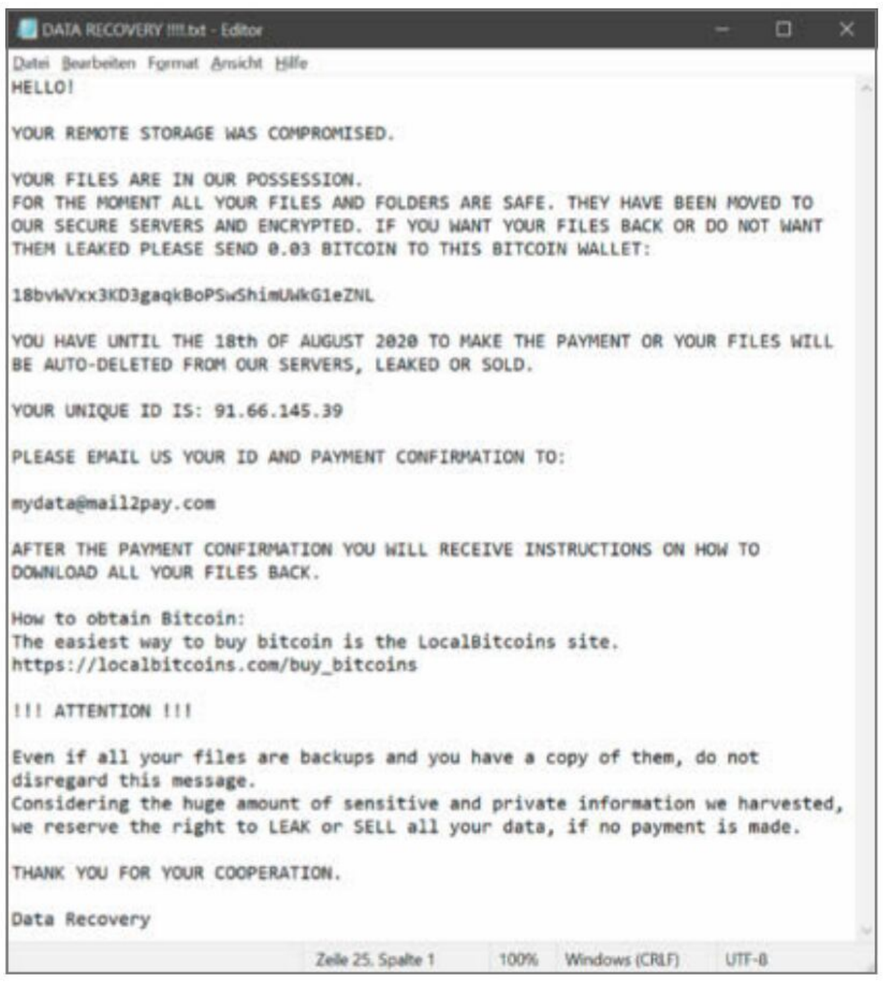
Die Täter behaupteten, die Dateien seien in Sicherheit, verschlüsselt auf einem Server. Um die Urlaubsfotos aus der digitalen Geiselhaft zu befreien, solle J. 0,03 Bitcoin an die Adresse 18bvW-

Vxx3KD3gaqkBoPSwShimUWkG1eZNL überweisen, umgerechnet rund 400 Euro. Doch da gab es zwei Probleme: Zum einen war die Frist der Erpressergruppe, die sich selbst ironischerweise „Data Recovery“ nennt, längst abgelaufen – J. hatte die Misere erst nach zwei Monaten entdeckt. Zum anderen ist es immer eine schlechte Idee, mit Erpressern zu verhandeln.

Gemeinsam mit seiner Frau suchte Gunther J. nach einem Weg, die Urlaubsfotos zu retten. Dann hatte sie eine Idee, die kurz darauf auch in die Tat umgesetzt wurde: Die beiden riefen in der c’t-Redaktion an. Bei uns melden sich häufig Opfer von Cyber-Erpressern, doch dieser Fall machte uns besonders neugierig. Denn es war völlig rätselhaft, wie die Täter auf das NAS zugreifen konnten. Es war schnell klar, dass der Anrufer sein Heimnetz mit Bedacht aufgebaut und konfiguriert hatte.

Meist gelingen solche Angriffe, weil ein NAS unzureichend abgesichert und über eine Port-Weiterleitung im Router von außen zugänglich gemacht wurde. Doch das war anscheinend nicht der Fall, J. griff nur von zu Hause auf seinen Netzwerkspeicher mit den Urlaubsfotos zu und hatte auch keine Port-Weiterleitung eingerichtet. Theoretisch kann die Attacke auch von einem infizierten Rechner im lokalen Netz ausgegangen sein, doch auch diese These schien unwahrscheinlich: J. hatte sämtliche Rechner bereits vor seinem Anruf mit Desinfec’t auf Virenbefall untersucht – keine Funde, alles war sauber.

Dennoch war es den Cyber-Erpressern offensichtlich gelungen, auf sein NAS zuzugreifen und die Urlaubsfotos zu löschen. J. erzählte, dass er vor dem Vorfall seine Fritzbox, an der das NAS hing, durch den Standard-Router seines Providers Vodafone ersetzt hatte, ein Gerät des Typs CBN CH6640E. Zwar machte dieses Modell schon in der Vergangenheit durch haarsträubende Sicherheitslücken Schlagzeilen. Vodafone hat die Probleme jedoch längst mit einem automatisch verteilten Firmware-Update gelöst. Wir baten J., uns weitere Informationen zu mailen, und gaben ihm den Tipp, die beiden NAS-Festplatten in einen Rechner einzubauen und sie dort mit dem in Desinfec’t enthaltenen Datenrettungs-Tool photorec zu untersuchen – in der Hoffnung, dass sich die Urlaubsfotos doch noch wiederherstellen lassen.

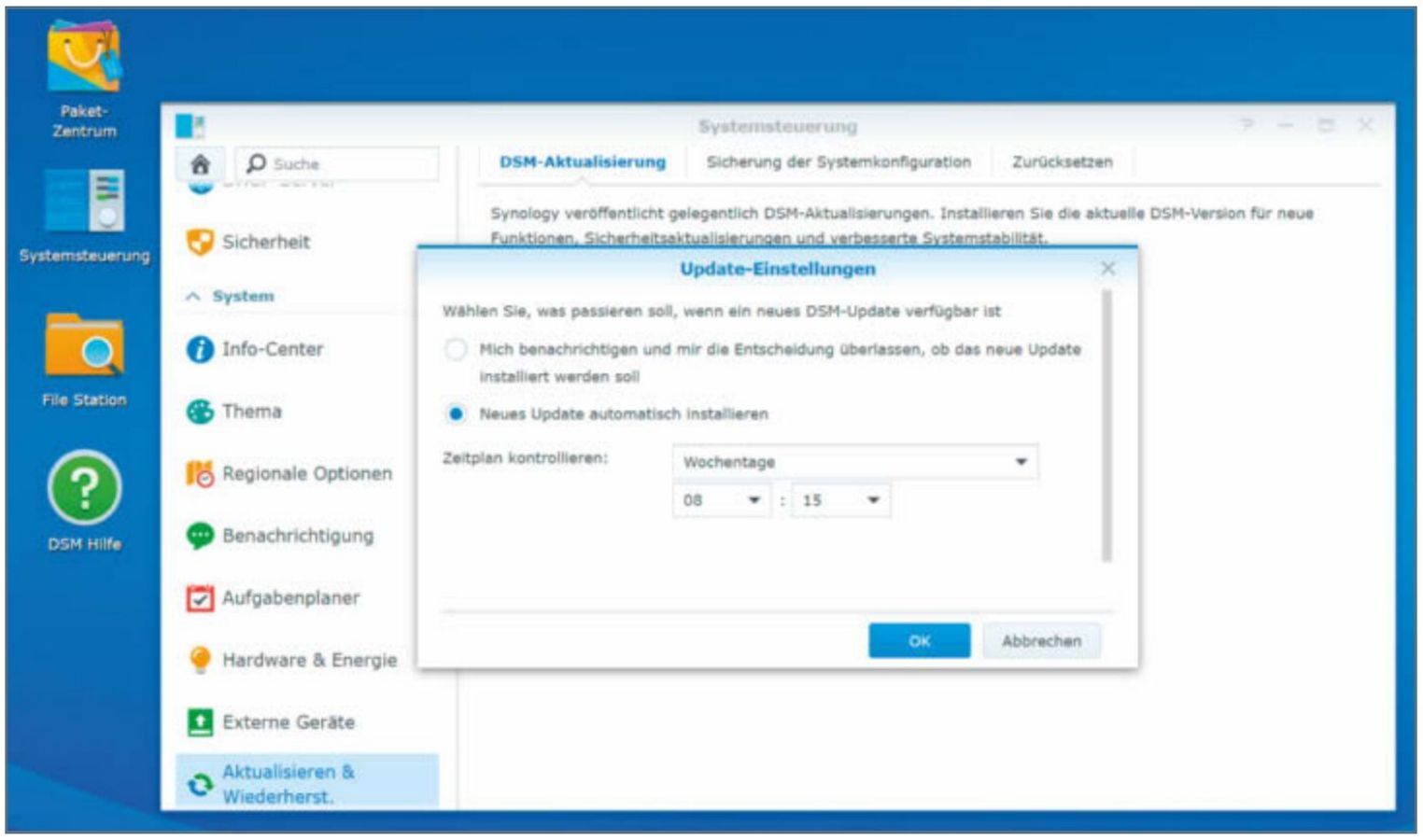


Das ist alles, was die Cyber-Erpresser auf dem NAS hinterließen: einen Erpresserbrief, in dem sie 0,03 Bitcoin (etwa 400 Euro) Lösegeld fordern.

Erpresserbrief statt Urlaubsfotos

Gunther J. schickte uns unter anderem das Erpresserschreiben, das er auf seinem NAS entdeckt hatte. Zu der darin angegebenen Bitcoin-Adresse lieferte Google interessante Details: Sein NAS ist offenbar einer größeren Angriffswelle zum Opfer gefallen, die auf bestimmte NAS-Modelle des Herstellers Lenovo-EMC (früher Iomega) abzielt. Tatsächlich hat unser Leser ein solches NAS im Einsatz, nämlich ein Iomega StorCenter ix2-200. Über blockchain.com fanden wir heraus, dass auf der Bitcoin-Adresse der Täter immerhin gut 0.13 BTC eingegangen waren, umgerechnet über 1700 Euro. Weitere Recherchen ergaben, dass die Angreifer vermutlich eine Sicherheitslücke in der Iomega-Firmware ausnutzten. Durch ein ungeschütztes API ist es möglich, ohne Authentifizierung auf das Dateisystem des NAS zuzugreifen (CVE-2019-6160). Im August 2019 hatte Lenovo auf seiner Website vor diesem akuten Sicherheitsproblem gewarnt und ein Firmware-Update zur Verfügung gestellt. Das war unserem Leser offenbar entgangen. Eine Rückfrage ergab, dass die von ihm eingesetzte Firmware älter war.

Doch der Fall war noch längst nicht gelöst, denn auch ein ungeschütztes API ist erstmal nicht für Angreifer aus dem Internet erreichbar – und eine Port-Weiterleitung im Router hatte J. ja nicht ein-



Firmware-Updates sorgen für Sicherheit. Im Idealfall kümmert sich das NAS automatisch darum.

gerichtet. Den letzten Teil des Rätsels löste unser Leser selbst: Er entdeckte, dass in dem Vodafone-Router sehr wohl eine Weiterleitung aufs NAS eingerichtet war. Aber wer hatte die angelegt, wenn nicht J.? Der Übeltäter war das verwundbare Iomega-NAS selbst: Gut versteckt auf Seite 92 des Handbuchs findet sich der folgende Hinweis: „Router-Port-Weiterleitung: Einige Router haben eine UPnP-Option. Bei einem UPnP-Router kann die Software des Iomega-Geräts bei Aktivierung automatisch die richtigen Weiterleitungs-Ports konfigurieren."

J. hatte vergessen, nach einem Werksreset des Routers die UPnP-Funktion abzuschalten. Das NAS hat dies bemerkt, selbstständig ein Port-Forwarding anlegt – und sich damit sein eigenes Datengrab geschaufelt. Die Täter hatten noch am Tag des Router-Resets zugeschlagen. Doch auch diese Geschichte hat ein Happy End: Nachdem der Datenretter photorec durchgelaufen war, konnte unser Leser wieder auf seine Urlaubsfotos zugreifen. Einzig die Sortierung der zahlreichen Dateien war durcheinander geraten, doch das war schnell behoben.

Jetzt sind Sie dran!

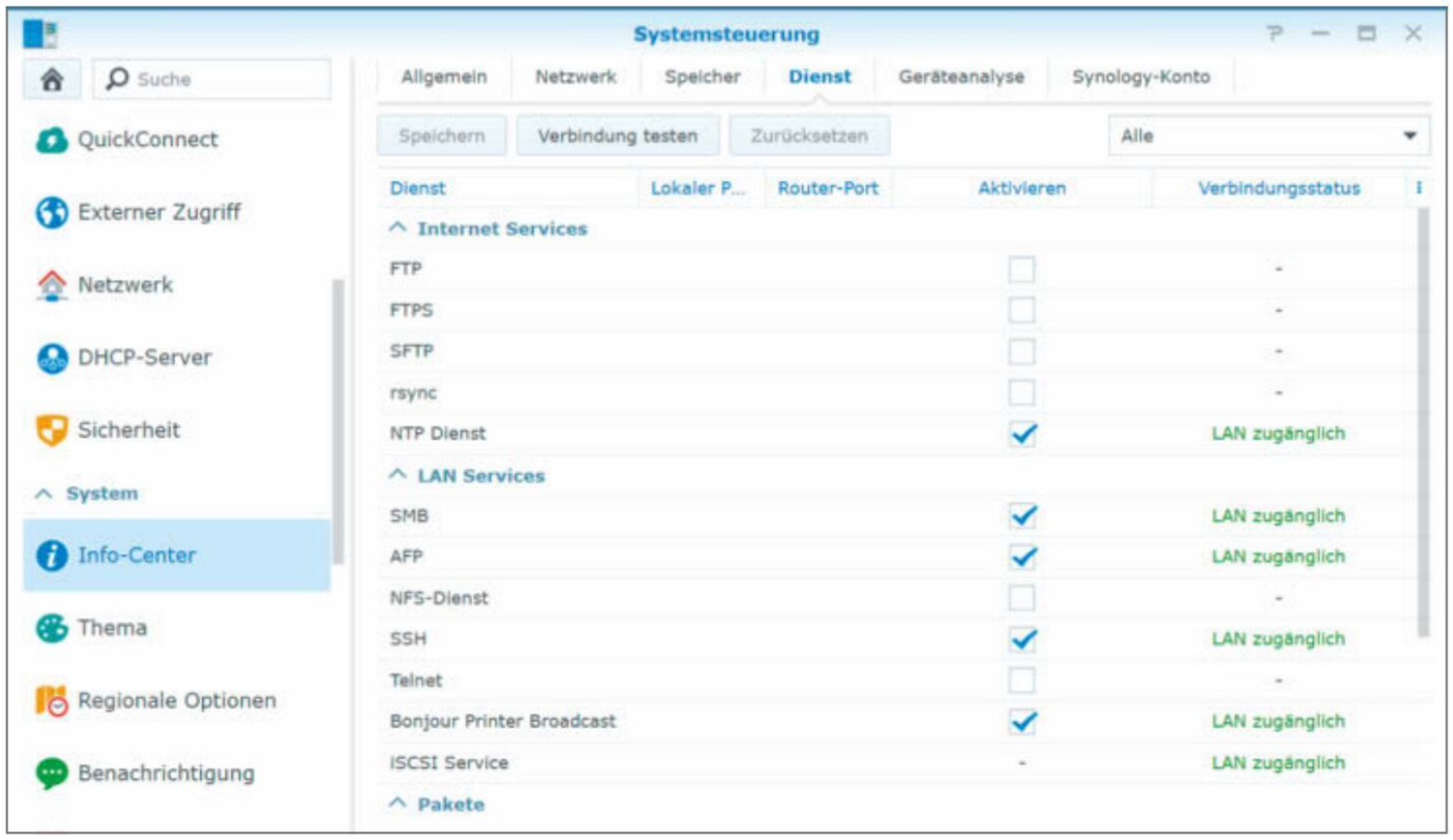
Der Fall demonstriert, wie schwierig es ist, Geräte im lokalen Netz vor Hackern zu schützen – selbst wenn man die Gefahren kennt. Damit es Ihnen nicht ähnlich ergeht, fassen wir die wichtigsten Handgriffe zum Absichern eines NAS am Beispiel eines Synology-Geräts in diesem Artikel zusammen. Die Tipps gelten sinngemäß für alle anderen Marken. So können Sie Ihre Daten nicht nur vor Cyber-Angriffen schützen, sondern auch vor anderen Arten des Datenverlustes.

Firmware-Updates

Um ein NAS sicher zu betreiben, muss sein Besitzer die Firmware aktuell halten. Firmware-Updates schließen häufig Sicherheitslücken, durch die Angreifer auf Ihre Daten zugreifen können. Im Idealfall kümmert sich das NAS selbsttätig darum: Es installiert verfügbare Updates automatisch oder informiert den Nutzer zumindest, damit dieser die Installation anstoßen kann. Wenn Ihr NAS einen Auto-Update-Mechanismus hat, schalten Sie ihn ein. Falls das NAS Sie über Updates benachrichtigen kann, etwa per Push-Nachricht oder Mail, aktivieren Sie auch diese Funktion.

Öffnen Sie die Konfigurationsoberfläche im Browser und loggen Sie sich ein. Anschließend klicken Sie auf „Systemsteuerung/Aktualisieren & Wiederherst.", um zu erfahren, ob die installierte Firmware (Synology spricht von DSM, Disk Station Manager) auf dem aktuellen Stand ist. Falls nicht, können Sie die Aktualisierung direkt anstoßen. Anschließend klicken Sie auf den Button „Update-Einstellungen", um die automatische Update-Installation einzuschalten. Aktivieren Sie hier die Einstellung „Neues Update automatisch installieren". Sie können dort

Weniger ist mehr: Schalten Sie alle nicht benötigten NAS-Dienste ab, um die Angriffsfläche zu reduzieren.



außerdem den Zeitplan für die Installation verändern, um zu verhindern, dass Ihr NAS werktags während der Arbeit im Homeoffice ausfällt, weil es Updates einspielt. Übernehmen Sie die neue Einstellung anschließend mit „OK“.

Um auf dem Laufenden zu bleiben, sollten Sie in der Systemsteuerung des NAS unter „Benachrichtigung“ einstellen, dass Sie Ihr NAS über Firmware-Updates und weitere sicherheitsrelevante Ereignisse per Mail oder Push-Benachrichtigung informiert. Für die Mailbenachrichtigung können Sie entweder unter „E-Mail“ einen eigenen Mail-Account eines beliebigen Anbieters hinterlegen oder Sie nutzen den Maildienst von Synology, den Sie unter „Push-Dienst“ finden. Unter „Erweitert“ legen Sie fest, über welche Ereignisse Sie das NAS informieren soll. Ereignisse zur Aktualisierung der Firmware finden Sie unter „System“, weitere Berichte kann Ihnen der „Sicherheitsberater“ schicken, etwa wenn das System ein Schadprogramm auf dem NAS entdeckt hat.

Wenn Sie bei Ihrem NAS weder Auto-Updates noch Update-Benachrichtigungen einstellen können, dann setzen Sie sich am besten einen wiederkehrenden Kalendereintrag, der Sie daran erinnert, regelmäßig auf der Hersteller-Website nach Firmware-Updates zu schauen; zum Beispiel alle vier Wochen, mindestens aber alle drei Monate. Überprüfen Sie, ob der NAS-Hersteller Ihr Modell überhaupt noch mit Firmware-Updates versorgt. Falls Sie hierzu keine Informationen auf der Herstellerseite finden, können Sie per Mail beim Hersteller nachfragen. Liegt das letzte Update bereits mehrere Jahre zurück, dann hat der Hersteller den Support höchstwahrscheinlich eingestellt. In diesem Fall sollten Sie darüber nachdenken, auf ein modernes Gerät umzusteigen. Wenn dies nicht infrage kommt, dann stellen Sie zumindest sicher, dass Ihr NAS unter keinen Umständen aus dem Internet erreichbar ist (siehe „Router konfigurieren“).

Dienste einstellen

Ein NAS ist inzwischen viel mehr als ein Datenlager im LAN: Die Hersteller statten die Geräte mit allerlei Zusatzfunktionen aus, die teilweise bereits im Auslieferungszustand aktiv sind. Solche Funktionen reichen vom Medien- bis hin zum Mailserver. Allerdings bieten sie Angreifern mit jedem aktiven Dienst eine weitere Angriffsmöglichkeit. Halten Sie die Angriffsfläche so klein wie möglich, indem Sie alle nicht benötigten Dienste deaktivieren. Nutzen Sie Ihr NAS am besten nur als Netzwerkspeicher, alle weiteren Dienste sind auf einem anderen System, etwa einem Raspberry Pi, besser aufgehoben.

Bei den Synology-NAS finden Sie eine Übersicht über die laufenden Dienste in der Systemsteuerung unter „Info-Center/Dienst“. Dort können Sie bei nicht länger benötigten Diensten das Häkchen bei „Aktivieren“ entfernen. Klicken Sie anschließend auf „Speichern“, um die Änderungen zu übernehmen. Schauen Sie im Paket-Zentrum unter „Installiert“

Räumen Sie bei den Portfreigaben gründlich auf. Insbesondere der hier gezeigte SMB-Port 445 sollte unter keinen Umständen in der Liste auftauchen.

nach nicht verwendeten Apps und deinstallieren Sie diese.

Sehen Sie davon ab, NAS-Dienste direkt aus dem Internet erreichbar zu machen. Wenn Sie Ihr NAS aus der Ferne erreichen können, dann können das auch Hacker. Falls Sie von unterwegs auf Ihre Dateien zugreifen möchten, dann nutzen Sie besser einen VPN-Tunnel ins Heimnetz. Als VPN-Server können Sie zum Beispiel viele Router (Fritzbox, Speedport & Co.) oder einen Raspberry Pi einsetzen. Wenn möglich, sollten Sie das flinke und stabile WireGuard-Protokoll (siehe ct.de/watx) nutzen.

UPnP abdrehen

Deaktivieren Sie im NAS die UPnP-Funktion zur Konfiguration des Routers, sofern vorhanden. Mit der Funktion könnte der Netzwerkspeicher selbstständig Port-Weiterleitungen im Router einrichten, was schwerwiegende Folgen haben kann (siehe Fall oben). Bei Synologys DSM steckt UPnP in der Systemsteuerung unter „Externen Zugriff/Routerkonfiguration“. Falls aktiv, schalten Sie diese Komfortfunktion aus.

Deaktivieren Sie UPnP auch im Router, damit auch keine anderen Geräte im lokalen Netz ohne Ihr Zutun Port-Weiterleitungen anlegen (siehe „Router konfigurieren“). Um sicherzustellen, dass Ihr NAS tatsächlich nicht aus dem Internet ansprechbar ist, können Sie den Netzwerkcheck von heise Security nutzen (siehe ct.de/watx). Dieser kostenlose Dienst überprüft, welche Ports bei Ihrem Anschluss über das Internet erreichbar sind. Im Idealfall sind es keine. Wenn es welche gibt, sollten Sie im Netz recherchieren, was es damit auf sich hat, damit Sie geeignete Maßnahmen treffen können (etwa, indem Sie die Weiterleitung der Ports im Router abschalten). Häufig ist der Port 5060 von außen erreichbar, dafür gibt es jedoch oft einen guten Grund: Router wie die Fritzbox öffnen ihn für eingehende VoIP-Telefonate. Lassen Sie ihn also in Ruhe. Der SMB-Port 445 für Windows-Dateifreigaben hingegen hat im Internet nichts verloren.

Sichere Passwörter

Sie haben es sicher schon oft gehört, dennoch muss es erwähnt werden: Nutzen Sie sichere Passwörter. Sicher bedeutet: individuell und möglichst lang. Ein sicheres Passwort funktioniert nur bei einem Dienst, wählen Sie also für jeden Zweck ein anderes. Geht es um lokale Verschlüsselung, zum Beispiel um die Festplatten Ihres NAS zu verschlüsseln, dann können Sie durch den Einsatz möglichst langer Kennwörter dafür sorgen, dass sich Angreifer möglichst lange die Zähne daran ausbeißen. Durch den Hersteller voreingestellte Kennwörter sollten Sie stets ändern.

Für weiteren Schutz sorgt die sogenannte Zwei-Faktor-Authentifizierung (2FA), die Sie bei einigen Diensten aktivieren können. Dann ist zum Einloggen nicht nur das Passwort nötig, sondern auch ein

zweiter Faktor, etwa in Form eines USB-Sicherheitsschlüssels oder eines einmalig gültigen Codes, den eine Authenticator-App generiert. 2FA schützt effektiv vor Angriffen, weil ein Hacker, der das Passwort erbeutet hat, in aller Regel keinen Zugriff auf den zweiten Faktor hat. Bei Synology-NAS schalten Sie 2FA über die Systemsteuerung und „Benutzer/Erweitert/2-Stufen Verifizierung“ für Admins oder alle Nutzer scharf.

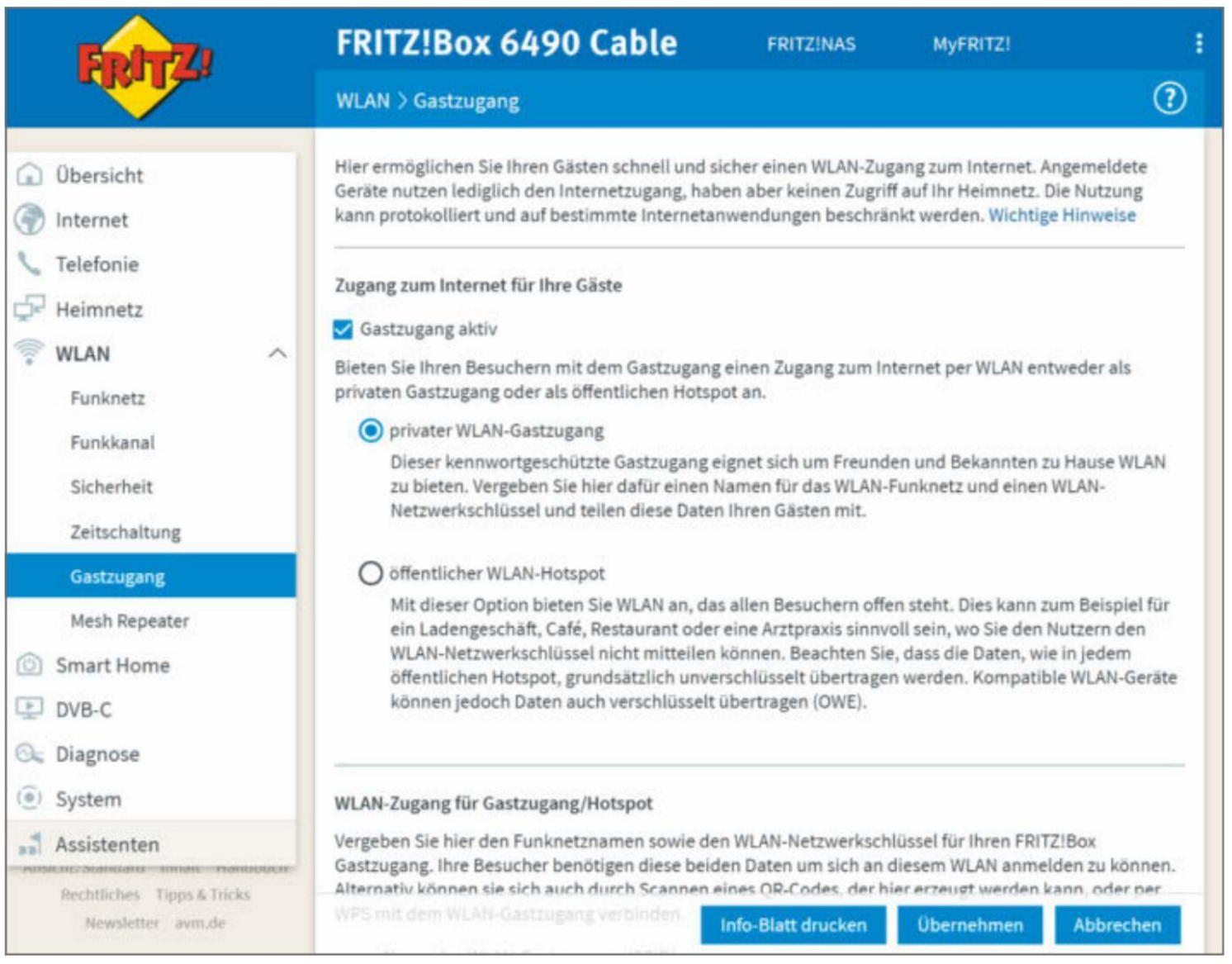
Wenn es eine Nutzerverwaltung mit unterschiedlichen Zugriffsrechten gibt, machen Sie davon Gebrauch. Jeder Nutzer sollte so wenig Rechte wie möglich haben: Sinnvoll sind etwa ein Admin-Account zur Konfiguration des Geräts und weitere Konten ohne Admin-Rechte, die jeweils nur auf genau die Daten und Funktionen zugreifen dürfen, die sie etwas angehen.

Seien Sie Ihr eigener Gast und versetzen Sie sich in die Lage eines Besuchers, der zum Beispiel über das WLAN auf das Internet zugreifen darf. Probieren Sie, als Gast auf das NAS zuzugreifen, um herauszufinden, welche Bereiche für jeden einsehbar sind. Unter Umständen möchten Sie zwar gewisse Bereiche für Gäste öffnen, aber etwa Ihre Urlaubsfotos und Dokumente privat halten.

Router konfigurieren

Sie müssen sich nicht nur um Ihr NAS kümmern, sondern auch um Ihren Router. Er ist die einzige Barriere zwischen Angreifern aus dem Internet und Ihrem Netzwerkspeicher. Die meisten der Empfehlungen aus diesem Artikel lassen sich auch auf den Router übertragen: Nutzen Sie sichere, individuelle Passwörter. Das WLAN-Passwort (WPA-Passphrase) darf nicht zugleich die Konfigurationsoberfläche (Webinterface) entsperren und so weiter. Voreingestellte Standardpasswörter sollten Sie auch beim Router ändern. Als WLAN-Verschlüsselung sollte mindestens WPA2 eingestellt sein, besser ist das aktuelle WPA3-Verfahren [1], das jedoch noch nicht von allen Geräten unterstützt wird. Bei der Fritzbox sorgt die Einstellung „WPA2 + WPA3“ dafür, dass beide Verschlüsselungsverfahren parallel aktiv sind.

Auch die Sicherheit Ihres Routers steht und fällt mit der Aktualität der Firmware. Prüfen Sie wie beim NAS also regelmäßig, ob die aktuelle Firmware installiert ist, und aktivieren Sie Mechanismen, die neue Updates automatisch einstellen oder zumindest eine Benachrichtigung auslösen, wenn es etwas Neues gibt. Bei den verbreiteten Fritzboxen



Gäste gehören ins Gastnetz. Dort können sie aufs Internet zugreifen, nicht aber auf Ihre Urlaubsfotosammlung, die auf dem NAS lagert.

aktivieren Sie die automatischen Updates wie folgt: Öffnen Sie das Webinterface des Routers im Browser (http://fritz.box) und klicken Sie nach dem Einloggen auf „System/Update/Auto-Update“. Wählen Sie die Option „Stufe III: Über neue FRITZ!OS-Versionen informieren und neue Versionen automatisch installieren (Empfohlen)“. Unter „Zeitraum für Updates“ können Sie eine Tageszeit für die automatische Update-Installation vorgeben. Vergessen Sie nicht, die Änderungen mit einem Klick auf „Übernehmen“ zu speichern.

Öffnen Sie abschließend die Unterseite „FRITZ!OS-Version“ und klicken Sie dort auf „Neues FRITZ!OS suchen“, um verfügbare Updates sofort zu finden und zu installieren. Falls Sie Ihre Fritzbox vom Provider gemietet haben, dann kann es sein, dass sich dieser um die Aktualität der Firmware kümmert und Sie die Installation nicht beeinflussen können. Dies ist auch bei Mietroutern anderer Hersteller häufig der Fall.

Kontrollieren Sie im Webinterface des Routers, welche Port-Weiterleitungen eingerichtet sind, und entfernen Sie alle nicht verwendeten. Bei der Fritzbox finden Sie die Weiterleitungen unter „Internet/Freigaben“. Deaktivieren Sie zudem die Konfigurierbarkeit des Routers über UPnP. Bei der Fritzbox klicken Sie hierzu auf den Button „Deaktivieren“, der sich unter dem Text „Sie können die Einstellung Selbstständige Portfreigabe für alle Geräte deaktivieren, die bisher keine Portfreigabe angefordert haben“ befindet. Suchen Sie unter „Heimnetz/Netzwerk“ zudem nach Geräten, bei denen unter Eigenschaften „selbst. Portfreigabe erlaubt“ angezeigt wird. Klicken Sie dort auf den Stift, um den Eintrag zu ändern, und deaktivieren Sie „Selbstständige Portfreigaben für dieses Gerät erlauben“.

Spannen Sie, wenn möglich, ein Gastnetz für Ihre Besucher auf, das keine Zugriffe auf das Heimnetz erlaubt (bei der Fritzbox unter „WLAN/Gastzugang“). So verhindern Sie, dass sich Ihre Gäste auf dem NAS umsehen. In dieses Netz können Sie auch Geräte sperren, denen Sie nicht vertrauen – zum Beispiel neue Smart-Home-Geräte, die Sie erstmal ausprobieren und beobachten möchten. Falls Sie Gästen das WLAN-Passwort fürs interne Netz ausgehändigt haben, ändern Sie es nach einer Weile, um unerwünschte Zugriffe aufs Heimnetz zu unterbinden.

NAS ≠ Backup

Ein NAS ist ohne Frage als Backup-Speicher prädestiniert, allerdings sollten Sie sich nicht allein darauf verlassen. Wie der Fall unseres Lesers zeigt, ist auch das NAS nicht vor Datenverlust gefeit. Für den Daten-GAU müssen nicht mal Hacker im Spiel sein, auch NAS-Festplatten und -SSDs werden irgendwann durch einen Hardwaredefekt ausfallen. Sie sollten daher auch den NAS-Inhalt per Backup sichern und dieses regelmäßig aktualisieren – zumindest dann, wenn die Daten unersetzlich sind. Worauf Sie dieses Backup speichern, ist fast egal. Der Datenträger sollte allerdings möglichst langlebig [2] und nicht dauerhaft mit Computer oder NAS verbunden sein.

Viele Krypto-Trojaner nehmen nämlich nicht nur die Dateien des infizierten Systems in Geiselhaft, sondern befallen auch externe Datenträger und Netzwerkfreigaben. Geeignet ist zum Beispiel eine externe USB-Platte, die nur während des Backups mit dem System verbunden ist. Auch ein verschlüsseltes Backup in die Cloud [3] kann sinnvoll sein: Bei vielen Cloud-Speichern können Sie frühere Versionen Ihrer Dateien wiederherstellen, etwa nachdem ein Krypto-Trojaner zugeschlagen hat. Bewährt hat sich die 3-2-1-Regel: Bewahren Sie drei Kopien Ihrer Daten (das Original zählt mit) auf zwei unterschiedlichen Datenträgertypen auf, eine davon außer Haus. Dann sind Sie selbst dann noch auf der sicheren Seite, wenn das Haus abbrennt – zumindest, was Ihre Daten betrifft.

Security-Checkup

Machen Sie regelmäßig ein Security-Check-up, um sicherzustellen, dass Ihr NAS weiterhin geschützt ist. Manchmal sorgen Konfigurationsänderungen dafür, dass ein Sicherheitsleck entsteht. Oder man probiert eine neue Funktion aus, ohne sich über die Konsequenzen bewusst zu sein. Auch Firmware-Updates können unerwartete Änderungen an der Konfiguration oder neue Funktionen mitbringen, welche die Sicherheit gefährden. Daher ist es nicht damit getan, NAS und Router genau ein Mal sicher einzurichten.

Hilfreich beim Absichern von NAS, Router, Smartphone & Co. sind auch unsere Security-Checklisten auf den Seiten 6 bis 31. Wenn Sie diese durcharbeiten, ist Ihr digitaler Fuhrpark vor den häufigsten Cyberangriffen geschützt. Die wichtigsten Punkte haben wir in einem begleitenden PDF-Booklet zusammengefasst, das Sie unter **ct.de/check2022** herunterladen können. Diese kompakte Variante eignet sich auch hervorragend zum Weiterverschicken an Kollegen, Freunde und Verwandte. (rei) c't

Literatur

[1] Dr. Alfred Arnold und Ernst Ahlers, **Extrasicher funken**, WPA3 schützt das WLAN, nicht nur an Fritzboxen, c't 22/2020, S. 26

[2] Lutz Labs, **Stabile Magnetpartikelchen**, Langzeitarchivierung mit Festplatten, c't 22/2020, S. 64

[3] Holger Bleich, **Auf Eis gelegt**, Daten langfristig in der Cloud sichern, c't 22/2020, S. 72

Netzwerkcheck, Security-Checklisten und weitere Infos

ct.de/watx

Verteidigen Sie Ihre Privatsphäre!

shop.heise.de/ct-datenschuetzen

Heft + PDF mit 29 % Rabatt

shop.heise.de/ct-datenschuetzen

In dieser neuen Auflage des c't-Sonderhefts „Daten schützen" erfahren Sie detailliert, wie Sie Ihre Privatsphäre vor Übergriffen bewahren können. **Darum geht's im Heft:**

- E-Mails und Telefone absichern
- Welche Messenger verschlüsseln wirksam
- Welche Angriffe bedrohen Ihre Privatsphäre on- und offline
- Passwörter für alle Systeme sicher verwalten
- Für Abonnenten portofrei
- Auch im Set mit Reiner SCT Authenticator zum Sonderpreis

Heft für 14,90 € • PDF für 12,99 € • Bundle Heft + PDF 19,90 €

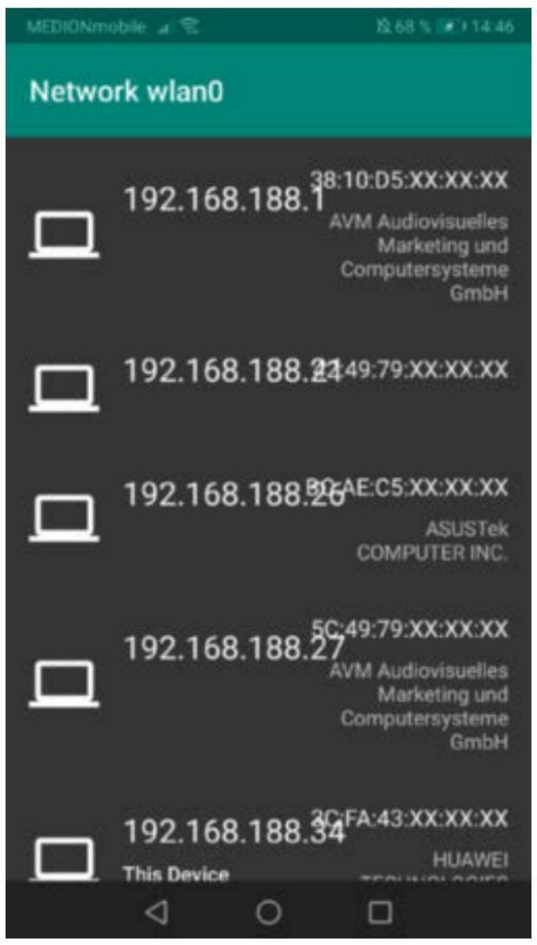
Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 €.
Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

heise Shop

Netzwerk-Abklopfer

Der Open-Source-Netzwerkscanner Ning spürt Geräte im lokalen Netz auf. Außerdem entdeckt er offene Dienste durch einen Portscan.

Von **Wilhelm Drehling**



Bei Ning handelt es sich um einen stark vereinfachten Netzwerkscanner, der nach Clients im lokalen Netz sucht und diese übersichtlich anzeigt. So verschafft man sich schnell einen Überblick über die Teilnehmer im Netzwerk und spürt längst vergessene Geräte auf. Auch der Nachbar, der vor Jahren nach dem WLAN-Passwort gefragt hat und seitdem auf fremde Kosten surft, fliegt durch einen Scan mit Ning auf. Zudem führt die Android-App einen Portscan aus, der verrät, auf welchen Ports ein gefundenes Gerät lauscht. So findet man zum Beispiel heraus, dass die preiswerte IP-Kamera vom Discounter auch über einen ungesicherten Telnet-Zugang auf Befehle wartet.

Ning kann man aus der Play-Store-Alternative F-Droid herunterladen (siehe ct.de/we3p). Alternativ geht das auch über die F-Droid-Website als APK-Installationsdatei, diese wäre jedoch dann eine fixe Version ohne automatische Updates. Daher wird, obwohl es sich um eine ältere Version handelt, ein Download via F-Droid-App empfohlen.

Als Inspiration diente dem Entwickler die Netzwerkscanner-App Fing. Doch die beiden Apps könnten unterschiedlicher kaum sein: Während einen beim Öffnen von Fing zunächst etliche Zusatzfunktionen anspringen, macht Ning kurzen Prozess und zeigt direkt alle Geräte im gleichen Netzwerk an. Im Überblick zeigt die App die MAC-Adresse und den Netzwerknamen und sortiert die jeweiligen Geräte nach der IP-Adresse. Anders als Fing versucht die Alternative nicht, den Gerätetyp (zum Beispiel Smartphone oder TV) zu erkennen.

Auf dem Hauptbildschirm der Ning-App kann man mit einem Wisch von links nach rechts die Einstellung zum Verstecken der MAC-Adressen sowie den Namen des aktuellen WLAN anzeigen. Ein kleiner Bug sorgt dafür, dass Scans manchmal die Geräte ohne MAC-Adresse auflisten. Dann hilft nur das Löschen der App-Daten. Wer einen der gefundenen Clients anklickt, startet automatisch einen Portscan und kann das Ergebnis in Echtzeit verfolgen. Klickt man beispielsweise beim Router (meistens die IP-Adresse, die auf .1 endet) auf einen der Ports für HTTP (80) oder HTTPS (443), öffnet sich dessen Weboberfläche im Browser.

Im direkten Vergleich erkannte das Vorbild im Test zwar meistens mehr Ports und konnte auch detailliertere Informationen aus der MAC-Adresse gewinnen. Die Open-Source-Alternative muss sich aber trotzdem nicht verstecken: Mit über 6020 individuell abgefragten Ports prüft Ning den Großteil aller relevanten Ports. Der Netzwerkscanner ist quelloffen und kommt, im Unterschied zu Fing, ohne Zugriffsberechtigungen und ohne Werbetracker aus.

Wer auf tiefgreifende Funktionen verzichten kann, wird mit Ning mehr als ausreichend bedient sein. Die einfache App ist ein zuverlässig funktionierender Netzwerkscanner. Ning benötigt noch etwas Arbeit, um mithalten zu können, befindet sich aber auf dem richtigen Weg. (wid) c't

Ning

Netzwerkscanner	
Anbieter	Carsten Csiky
Systemvoraussetzungen	Android 6.0
Preis	**kostenlos** (LGPL V3)

Mehr Komfort im cleveren Zuhause!

Heft + PDF
mit 29 % Rabatt

Bauen Sie Ihre Fritzbox zur Smart-Home-Zentrale aus. Im 2. Sonderheft von **heise online** lesen Sie wie's geht:

- ► Fritzbox einrichten, steuern und erweitern
- ► Smart Home von Ikea
- ► Praxis- und Tuningtipps für Ihr System
- ► **Auch im Set mit Heizkörperthermostat zum Sonderpreis**

Heft für 14,90 € • PDF für 12,99 € • Bundle Heft + PDF 19,90 €

shop.heise.de/ho-smarthome21

Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 €.
Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

heise Shop

Bild: Sven Hauth

WLAN-Alarmanlage

WLAN ist praktisch, birgt aber auch viele Risiken: Jeder in Funkreichweite kann Router und Clients attackieren – und zwar weitgehend unbemerkt. Ein Raspi mit Nzyme schlägt Alarm, wenn sich jemand an Ihrem Netz zu schaffen macht.

Von **Tomas Jakobs**

Drahtlose Netzwerke sind vielen Gefahren ausgesetzt: Mittels Deauthentication können Angreifer WLAN-Clients beispielsweise zwingen, die Verbindung zur Basisstation zu trennen. Das geschieht entweder aus Spielerei oder um sie zu einer Verbindung mit einem Zugangspunkt unter Kontrolle der Angreifer zu animieren, der das WLAN-Netz der ursprünglichen Basisstation imitiert. Das Ziel ist, den Datenverkehr auszulesen oder zu manipulieren (Man-in-the-middle-Attacke). All das ist längst kein Hexenwerk mehr, es gibt sogar einsatzfertige Hacking-Gadgets, die Standardangriffe auf Knopfdruck ausführen [1].

Normalerweise bekommt man von WLAN-Attacken bestenfalls etwas mit, wenn die Angreifer längst ins Netzwerk eingestiegen sind. Doch Sie können vorbeugen und mit Nzyme aktiv nach auffälligen WLAN-Aktivitäten scannen. So bekommen Sie schnell mit, wenn etwa ein neues Netz in der Umgebung auftaucht, das Ihrem verdächtig ähnelt oder Ihre Geräte fremdgesteuert angewiesen werden, die Verbindung zu kappen. Die nötige Hardware kostet nur ein paar Euro und einen passenden Raspi haben Sie vielleicht sogar schon in der Schublade.

Das Open-Source-Projekt Nzyme fungiert als Wireless Intrusion Detection System (WIDS), also als Alarmanlage für Drahtlosnetzwerke. Gerade erschien die Version 1.1.1, welche die gröbsten Kinderkrankheiten hinter sich gelassen hat. Das Release bietet eine gute Gelegenheit zu erklären, wie Sie Nzyme in Betrieb nehmen und das eigene WLAN vor neugierigen Augen schützen. Entdeckt Nzyme Anomalien im Funkverkehr, warnt es in der Weboberfläche und versendet auf Wunsch E-Mails an den Administrator.

Frame-Sammler

Nzyme arbeitet im Hintergrund als Sniffer für die sogenannten WLAN-Management-Frames. Drahtlosgeräte senden Management-Frames meist unverschlüsselt, um Informationen auszutauschen. Sie machen so beispielsweise auf sich aufmerksam oder bereiten einen WPA-Handshake vor. Der Unterschied zu den bekannten Sniffern aus Pentesting-Werkzeugsammlungen liegt in der konsequenten Ausrichtung auf automatisiertes Schnüffeln und Warnen. Im Idealfall wird Nzyme stationär auf die Lauer gelegt und sich selbst überlassen. Fachkenntnisse über den Aufbau von WLAN-Paketen sind für den Betrieb von Nzyme nicht nötig. Die Software überwachte für diesen Artikel über einen Monat das heimische Netzwerk des Autors und konnte die eigenen Hackingversuche erfolgreich aufspüren.

Der Nzyme-Entwickler Lennart Koopmann hat das Tool für den Raspi konzipiert. Der Dokumentation zufolge reicht bereits ein Raspi 3 für kleine Heimnetze. Für diesen Artikel diente ein Raspi 4 mit 4 GByte Arbeitsspeicher als Testgerät. Bei Mesh-Drahtlosnetzwerken in Unternehmen empfehlen sich mehrere Raspis mit Nzyme für eine bessere Abdeckung der größeren Fläche. Diese können ihre Daten zur Auswertung an einen zentralen Log-Server im internen Netz schicken, beispielsweise an Graylog, das vom gleichen Entwickler stammt. So kann man kostengünstig auch große Netze scannen.

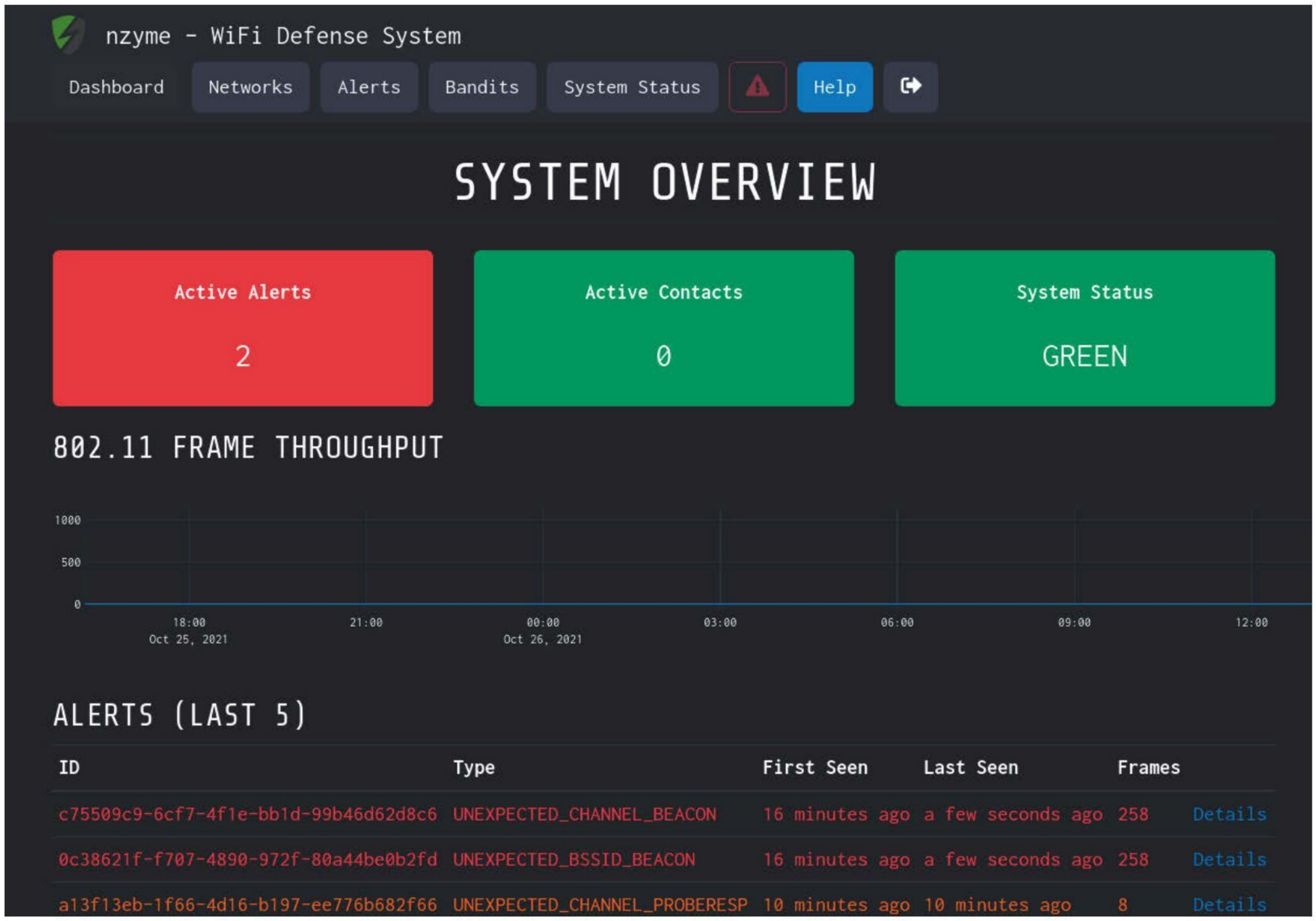
Für Nzyme genügt ein Raspberry Pi 3 oder neuer. Dazu brauchen Sie einen WLAN-USB-Stick, der den Monitor-Modus beherrscht.

Zur Überwachung der Funkfrequenzen ist ein WLAN-Modul nötig, das den sogenannten Monitor

WLAN-Management-Frames

Zur Überwachung des eigenen Netzes sammelt Nzyme WLAN-Management-Frames ein und meldet verdächtige Vorkommnisse, siehe dazu den Kasten „Verdächtige WLAN-Aktivitäten“ auf Seite 60. Neben Management-Frames gibt es auch weitere Arten von Frames, wie „control“, „extension“ und „data“, die für Nzyme nicht relevant sind. Management-Frames werden in der Regel unverschlüsselt gesendet und lassen sich in folgende Subtypen einteilen. Die Nzyme-Dokumentation (ct.de/wfrn) listet die sicherheitsrelevanten Management-Frames auf:

- **Authentication** ist der erste Schritt, um einem Drahtlosnetzwerk beizutreten. Je nach Verschlüsselungsverfahren (WEP, WPA) wird eine bestimmte Authentifizierungssequenz eingeleitet.
- Der **Association Request** folgt auf Authentication und fragt Ressourcen an der Basisstation an.
- Darauf folgt die **Association Response**. Wenn erfolgreich, dann darf das assoziierte Gerät weitere Frame-Arten senden, beispielsweise „data“ für Datenübertragung.
- Mit **Deauthentication** verlangt ein Drahtlosgerät die Trennung der Verbindung. Deauthentication muss von den anderen Geräten akzeptiert werden.
- **Beacon**: Basisstationen senden durchgängig solche Frames, um auf sich aufmerksam zu machen.
- **Probe Request**: Ein Drahtlosgerät sucht damit nach bekannten WLAN-Netzen.
- Zugangspunkte senden eine **Probe Response** als Antwort auf einen Probe Request und bestätigen ihre Anwesenheit.



In der intuitiv bedienbaren Weboberfläche ist das Dashboard die erste Anlaufstelle. Dort erfassen Sie auf einen Blick den Zustand des Systems. Verdächtige Aktivitäten springen direkt ins Auge.

Mode unterstützt. Ein preisgünstiger WLAN-USB-Stick, etwa mit Ralink-RT-Chipsatz, reicht schon aus. Wer nach einem Verwendungszweck für ältere, nicht mehr gebrauchte WLAN-Sticks sucht, kann mehrere davon an seinem Raspi für Nzyme nutzen. Das bringt mehr WLAN-Management-Frames in kleineren Zeitabständen und führt zu einem besseren Lagebild, da Nzyme auf mehreren Frequenzen parallel schnüffeln kann. Im Praxistest kamen ein älterer Panda-Wireless-USB-Adapter (PAU06) sowie ein etwas moderneres Handelsware-No-Name-Gerät mit RT5572-Chipsatz für gerade einmal 15 Euro zum Einsatz. Darüber hinaus sollte Nzyme via Ethernetkabel mit dem lokalen Netzwerk verbunden sein, um seine Weboberfläche bereitzustellen und vor Anomalien im Drahtlosnetzwerk zu warnen.

Installation

Nzyme installieren Sie wahlweise unter Debian, Ubuntu Server oder Raspberry Pi OS (ehemals Raspbian). Der Fokus liegt hier auf der Installation unter Debian 10 „Buster“. Mit Debian 11 „Bulleye“, das bei Redaktionsschluss kurz vor Veröffentlichung stand, kam es im Testlauf noch zu Problemen mit dem Channel-Hopping. Bei anderen Distributionen oder WLAN-Hardware können die einzelnen Installationsschritte abweichen und müssen angepasst werden. Grundkenntnisse und Transfervermögen im Umgang mit einem Linux-System werden vorausgesetzt. Debian-Images für den Raspberry Pi finden Sie im Downloadbereich der Debian-Webseite, die wir unter ct.de/wfrn verlinkt haben.

Nach der Debian-Grundinstallation und Sprachanpassungen bietet es sich an, den SSH-Server in Betrieb zu nehmen und von einem anderen Rechner aus mit dem Raspi zu arbeiten. Dazu sollten Sie unter Debian ein Passwort für root vergeben und in der Datei /etc/ssh/sshd_config den Login via Passphrase erlauben (PermitRootLogin yes), falls Sie sich nicht mit SSH-Schlüsseln authentifizieren. Für Raspberry Pi OS konfigurieren Sie den SSH-Zugang mit dem

Raspi-Imager-Tool vor [2]. Das Debian-Raspi-Image bringt nur den Nutzer root mit, unter Raspberry Pi OS setzen Sie „sudo“ vor die Befehle, um sie mit Systemverwalterrechten auszuführen. Besorgen Sie mit dem nachfolgenden Befehl zunächst die nötigen Abhängigkeiten und einige zusätzliche Pakete:

```
apt install libpcap0.8 sudo wget iwd \
openjdk-11-jre-headless \
wireless-tools \
postgresql-11 iw \
firmware-ralink apt-transport-https -y
```

Falls Sie einen anderen WLAN-Chipsatz anstelle des hier verwendeten Ralink-Chipsatzes nutzen, dann ersetzen Sie „firmware-ralink“ durch das Paket des Herstellers. Für Realtek wäre das beispielsweise „firmware-realtek“.

Stellen Sie im Anschluss sicher, dass das WLAN-Interface des Sticks, mit dem Sie scannen wollen, mit einem eindeutigen Namen ansprechbar ist. Einen Überblick über relevante Netzwerkinterfaces verschaffen Sie sich mit `iwconfig`. Tauchen in dessen Ausgabe die generischen Interface-Bezeichnungen wlan0 und wlan1 auf, dann müssen Sie Hand anlegen und feste Gerätenamen setzen. Vergeben Sie dazu zwei udev-Regeln im Verzeichnis /etc/udev/rules.d:

```
cat <<EOF >>/etc/udev/rules.d/\
70-persistent-net.rules
SUBSYSTEM=="net", ACTION=="add", \
DRIVERS=="?*", \
ATTR{address}=="XX:XX:XX:XX:XX:XX", \
ATTR{dev_id}=="0x0", \
ATTR{type}=="1", \
KERNEL=="wlan*", NAME="IDSWLAN"
EOF
```

Falls Sie Nzyme unter Raspberry Pi OS installieren, benötigen Sie die udev-Regeln nicht und es genügt, den Symlink `/etc/systemd/network/99-default.link` zu löschen und den Raspi neu zu starten. Das System generiert dann automatisch einen festen Namen mittels der MAC-Adresse des Adapters, beispielsweise „wlx00c0ca971201“. Ersetzen Sie unter Debian im vorigen Befehl die XX-Platzhalter durch die MAC-Adresse des eigenen WLAN-Sticks, die Sie mit `ip link show` ermitteln. Der Name des Gerätes sollte einmalig sein und nicht in Konflikt mit anderen Geräten stehen. Verwenden Sie einen Namen ohne Bindestriche, Unterstriche und andere Sonderzeichen, denn die stören Nzyme beim Kanalwechsel. Als Beispielname für das Interface dient hier der Name „IDSWLAN“, mit dem Sie auf der sicheren Seite sind.

Nachdem Sie die erste Regel gesetzt haben, starten Sie den Raspi neu und vergeben Sie im Anschluss die zweite Regel:

```
cat <<EOF >>/etc/udev/rules.d/\
75-persistent-net-generator.rules
KERNEL!="wlan*|ath*|msh*|ra*|sta*|\
ctc*|lcs*|hsi*", \
GOTO="persistent_net_generator_end"
EOF
```

Nach einem weiteren Neustart sollte das WLAN-Interface unter dem Namen „IDSWLAN“ ansprechbar sein.

Im Anschluss gilt es, die PostgreSQL-Datenbank einzurichten, die Nzyme benötigt. Legen Sie dazu eine Datenbank mit Namen „nzyme“ und den Datenbank-User „nzyme“ an. Die Sternchen ersetzen Sie durch ein eigenes Passwort, das Sie sicher aufbewahren sollten.

```
sudo -Hiu postgres psql -c ↵
↳"create database nzyme;"
sudo -Hiu postgres psql -c ↵
↳"create user nzyme with encrypted ↵
↳password '******';"
sudo -Hiu postgres psql ↵
↳-c "grant all privileges on ↵
↳database nzyme to nzyme;"
```

PostgreSQL bestätigt Ihnen die jeweilige Anweisung mit den Ausgaben „CREATE DATABASE“, „CREATE ROLE“ und „GRANT“. Als letzten Schritt vor der Installation des Nzyme-Paketes erstellen Sie mit dem Befehl `echo -n XXXXXX | sha256sum` ein Passwort-Hash zur späteren Anmeldung am Web-Interface. Ersetzen Sie `XXXXXX` durch das gewünschte Passwort. Legen Sie den Hash (ohne den Bindestrich am Ende) für späteres Copy & Paste in eine temporäre Datei im Home-Verzeichnis ab.

Laden Sie nun mittels `wget` das Debian-Paket der aktuellen Nzyme-Version herunter. Bei Redaktionsschluss war das die Version 1.1.1 „Cherry Bomb“:

```
wget https://assets.nzyme.org/\
releases/nzyme-1.1.1.deb
```

Gleichen Sie die SHA256-Prüfsumme des Pakets mit der Zahlenfolge auf der Nzyme-Projektseite ab (ct.

de/wfrn), um die Echtheit des Pakets zu prüfen. Fahren Sie mit der Installation via `dpkg` nur fort, wenn die Prüfsumme stimmt:

```
sha256sum nzyme-1.1.1.deb
dpkg -i nzyme-1.1.1.deb
```

Nyzme konfigurieren

Nzyme kommt mit einer kommentierten Konfigurationsvorlage, die Sie einfach übernehmen und als Grundlage nutzen können:

```
cp /etc/nzyme/nzyme.conf.example \
/etc/nzyme/nzyme.conf
```

Ersetzen Sie nun mit einem Texteditor Ihrer Wahl die Beispielwerte in der Datei /etc/nzyme/nzyme.conf durch Ihre eigenen.

```
general: {
  role: LEADER
  id: nzyme-node-01
  admin_password_hash:
  database_path: "postgresql://localh↵
↳ost:5432/nzyme?user=nzyme&password=↵
↳YOUR_PASSWORD"

  python {
    path: /usr/bin/python3.8
    script_directory: /tmp
    script_prefix: nzyme_
  }
```

Geben Sie im Abschnitt `general` Ihrer Nzyme-Instanz bei `id` einen eindeutigen Namen, der nur aus alphanumerischen Zeichen besteht. Tragen Sie bei `admin_password_hash` Ihren zuvor erstellten Password-Hash ein, den Sie in einer temporären Datei abgelegt haben. Der Punkt `database_path` zeigt den PostgreSQL-Verbindungsstring. Ersetzen Sie dahinter den Platzhalter YOURPASSWORD durch das eigene Datenbank-Passwort.

Gleichen Sie im Abschnitt `python` bei `path` die Vorgabe /usr/bin/phython3.8 mit Versionsnummer und Pfad der installierten Python-Version ab und korrigieren Sie falls nötig. Viele Distributionen setzen hier symbolische Verknüpfungen. Es ist ratsam, besser direkt auf das Python-Executable zu verweisen.

Den Abschnitt `alerting` mit den Angaben für E-Mail-Benachrichtigungen überspringen Sie zunächst. Bevor Nzyme bei jedem Alert Mails versendet, sollten Sie das System erstmal feintunen. Bei der ersten Inbetriebnahme kommt es üblicherweise zu vielen False-Positives.

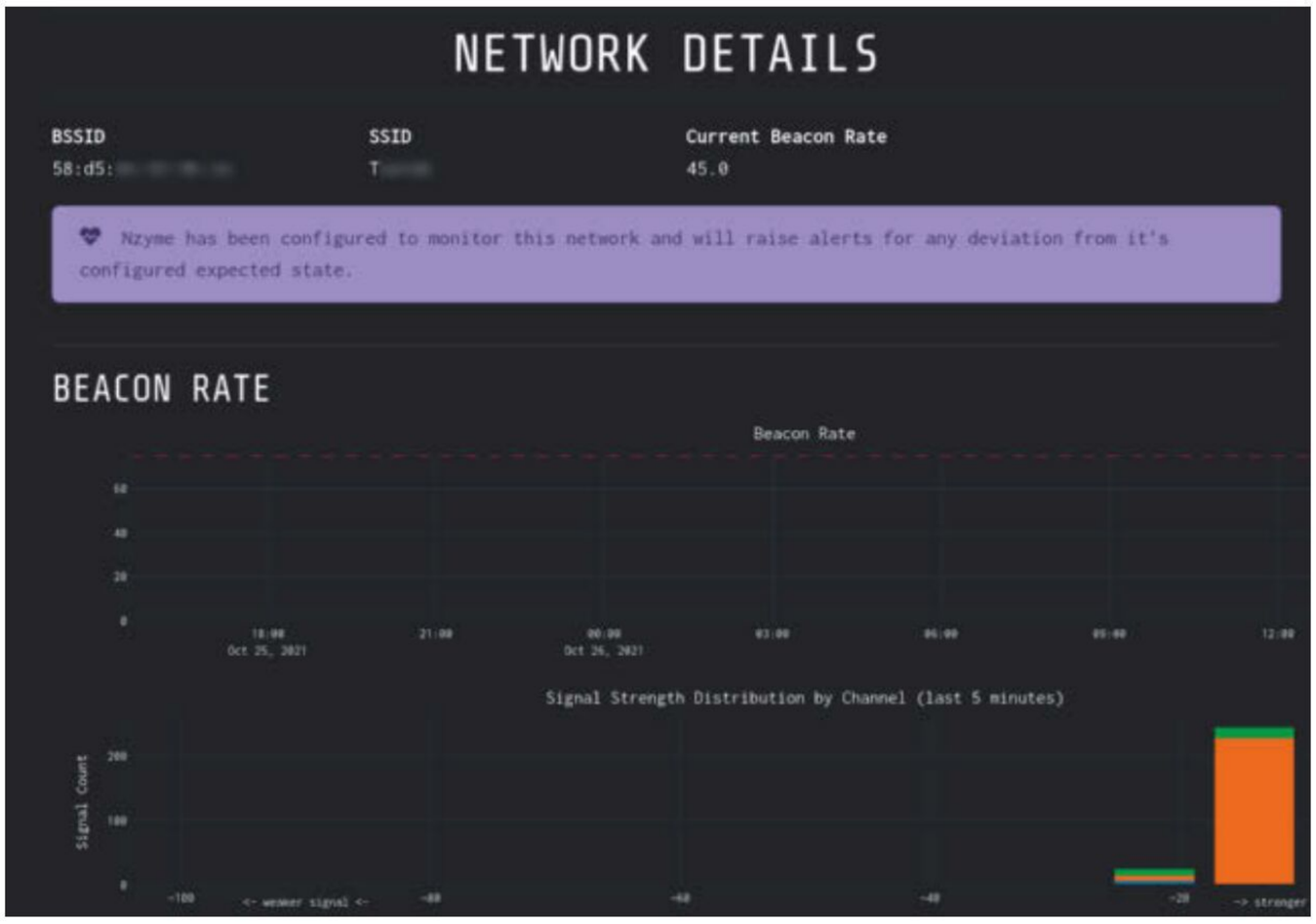
```
interfaces: {
  rest_listen_uri:↵
↳ "http://127.0.0.1:22900/"
  http_external_uri:↵
↳ "http://127.0.0.1:22900/"
}

802_11_monitors: [
  {
    device: wlx00c0ca971201
    channels:↵
↳ [1,2,3,4,5,6,7,8,9,10,11]
    channel_hop_command:↵
↳ "sudo /sbin/iwconfig {interface}↵
↳ channel {channel}"
    channel_hop_interval: 1
    skip_enable_monitor: false
  }
```

Ersetzen Sie im Abschnitt `interfaces` die Vorgabe `127.0.0.1` durch die IP-Adresse des Raspi-LAN-Interfaces, unter der er im lokalen Netz erreichbar ist. Prüfen Sie außerdem, ob der Raspi von einem DHCP-Server im Netzwerk eine fest zugewiesene IP-Adresse erhält. Von besonderem Interesse ist der Abschnitt `802_11_monitors`. Überschreiben Sie dort bei `devices` den Platzhalter „wlx00c0ca971201“ mit dem fest gesetzten Namen des Interfaces, beispielsweise „IDSWLAN“. Die Liste der abzusuchenden Kanäle steht kommasepariert unter `channels`. Für das 2,4-GHz-Band sind das zum Beispiel die Kanäle von 1 bis 14. Eine vollständige Liste aller verfügbaren Kanäle eines WLAN-USB-Sticks verschafft Ihnen der Befehl `iwlist channel`.

Zum Schluss machen Sie Nzyme systemd als Dienst bekannt und führen die Software aus. Zukünfig startet Nzyme nach einem Neustart des Raspi automatisch:

```
systemctl enable nzyme
systemctl start nzyme
```

Nach einer kurzen Wartezeit steht das Nzyme-Webinterface unter der IP-Adresse des Raspi und dem Port 22900 zur Verfügung. Die Anmeldung erfolgt mit dem Benutzernamen „admin“ und dem zuvor bestimmten Passwort. Falls Nzyme nicht star-



Der Menüpunkt „Network Details“ listet Informationen wie Beacon-Rate und Signalstärke auf. Wenn Sie von hier die Werte für SSID, BSSID, Beacon-Rate und Network-Fingerprint in die Nzyme-Konfigurationsdatei kopieren, beginnt Nzyme, das Netzwerk zu überwachen.

tet, besteht wahrscheinlich ein Problem mit der Konfigurationsdatei. Der Befehl `journalctl -xe` und ein Blick in die Logdatei /var/log/nzyme/nzyme.log helfen bei der Fehlersuche.

Nzyme auf das eigene Netzwerk ansetzen

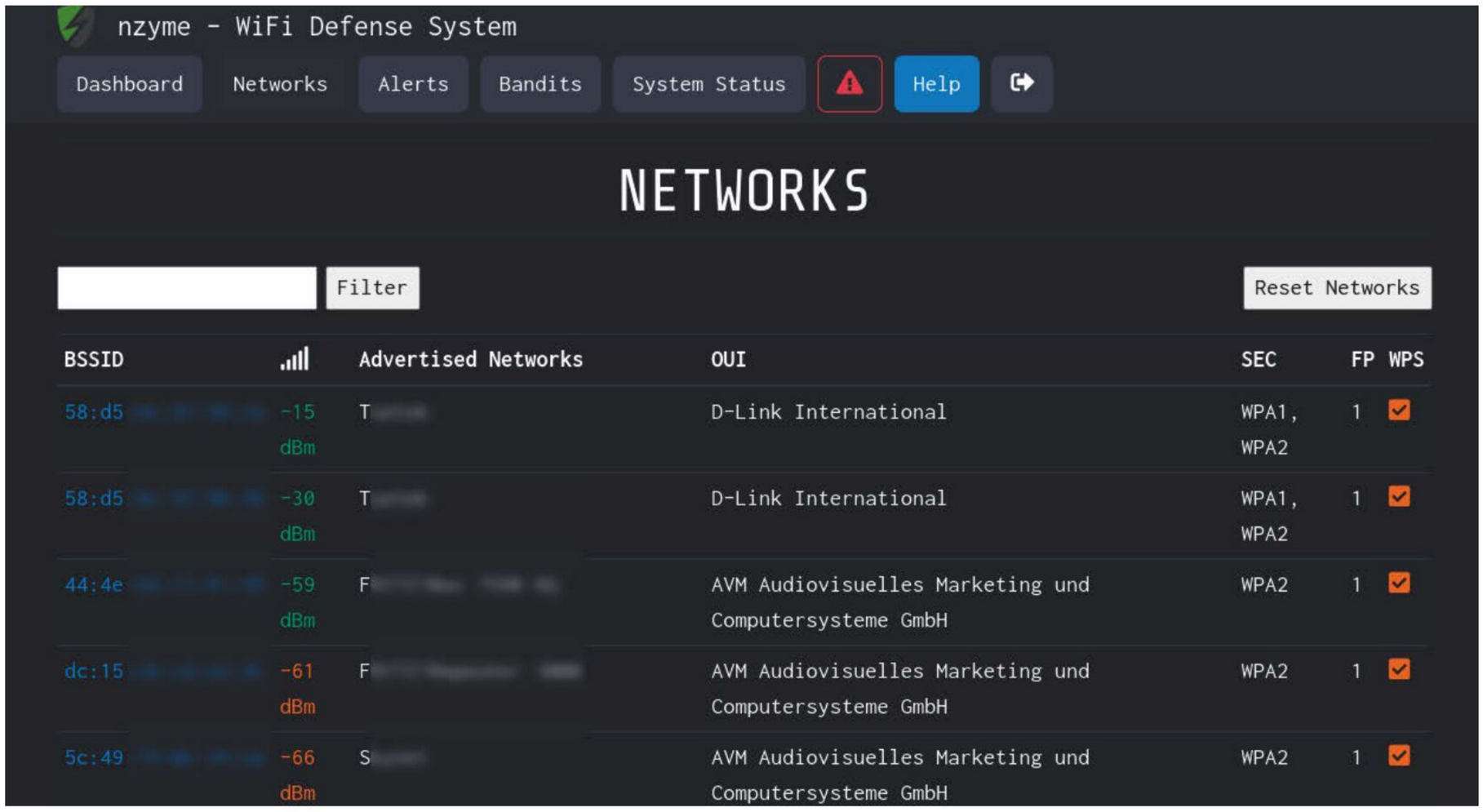
Nun gilt es, Nzyme mit dem eigenen Drahtlosnetzwerk bekannt zu machen, damit es überwacht werden kann. Wechseln Sie dazu nach der Anmeldung im Web-Interface zum Hauptmenüpunkt „Networks“ und öffnen dort die „Network Details“ für Ihre Drahtlosnetzwerke. Dort lesen Sie die Angaben wie SSID, BSSID, Beacon-Rate und Netzwerk-Fingerprint ab und speichern sie zwischen. Damit ergänzen Sie die Informationen in der Nzyme-Konfigurationsdatei im Abschnitt `802_11_networks`.

```
    ssid: mywifinetwork
    channels:↵
↳[1,2,3,4,5,6,7,8,9,10,11,12,13]
    security: [WPA2-PSK-CCMP]
    beacon_rate: 40
    bssids: [
      {
        address: "f0:9f:c2:dd:18:f6",
        fingerprints: [ 45933326ca0 ]
      }
    ]
```

Nach einem Neustart des Dienstes kennt Nzyme fortan ihr eigenes Netzwerk und dessen „Soll-Zustand“. Registriert Nzyme Abweichungen davon, zeichnet es diese auf und schlägt Alarm. Registriert Nzyme beispielsweise eine erhöhte Beacon-Rate, könnte dies darauf hindeuten, dass ein Angreifer versucht Ihren Access-Point zu imitieren (Spoofing). Zu jedem Alert informiert Nzyme über das mögliche Angriffsszenario, liefert aber zur besseren Einordnung auch Erklärungen für „natürliche Ursachen“ der Anomalie.

Alles im Blick

Das Dashboard ist die erste Anlaufstelle im Nzyme-Webinterface und zeigt den Status des Systems sowie mögliche Probleme an. Farbliche Statusanzeigen, Schnellübersichten der letzten Ereignisse und ein Graph über die vergangenen 24 Stunden verschaffen einen schnellen Situationsüberblick. Detailinformationen zu erkannten Drahtlosnetzwerken und Basisstationen finden Sie unter dem Hauptmenüpunkt „Networks“. Nzyme erstellt zum Unterscheiden einen möglichst eindeutigen Fingerprint. Dabei kann es vorkommen, dass einem Gerät meh-



Unter dem Menüpunkt „Networks“ listet Nzyme alle drahtlosen Netzwerke in Reichweite.

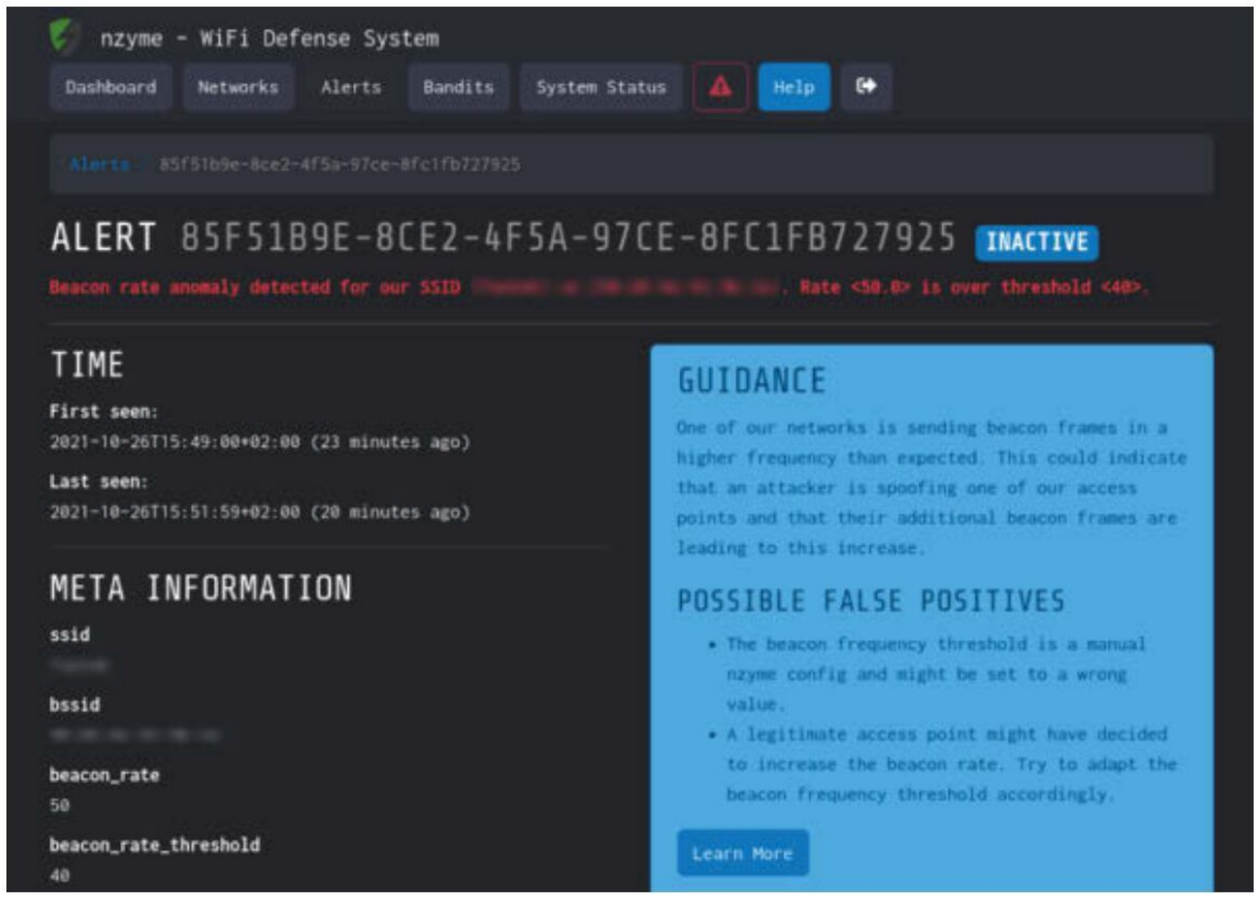
rere davon zuteil werden, je nachdem, auf welchen Kanälen es sendet oder für welche Drahtlosnetzwerke es verantwortlich ist.

Eine Gesamtübersicht aller von Nzyme registrierten „Alerts“ findet sich unter dem gleichnamigen Hauptmenüpunkt. Lassen Sie sich anfangs von den vielen Alarmmeldungen nicht verunsichern. Wie jedes Messinstrument braucht ein frisch installiertes Nzyme ein wenig Feinkalibrierung und Zeit, bis die Anzahl falsch positiver Alarme sinkt. Dazu passen Sie beispielsweise den Schwellenwert der Beacon-Rate, den Sie als üblich beobachtet haben, in der

Verdächtige WLAN-Aktivitäten

Nzyme behält die eigenen Drahtlosnetzwerke im Blick und sammelt möglichst viele WLAN-Management-Frames ein. Die folgenden Anomalien weisen auf einen möglichen Angriffsversuch hin:

- Neue Zugangspunkte, die legitime Access-Points nachahmen (Rogue-AP), fallen durch minimale Unterschiede in den Zeitstempeln auf.
- Nutzt das eigene Netzwerk plötzlich abweichende Kanäle, bricht die Verbindung ab oder ändert den Verschlüsselungsmodus, kann das auf einen aktuellen Angriff hindeuten.
- Durch die Organizationally Unique Identifier (OUI), die ersten Bytes der MAC-Hardware-Adresse, werden populäre Hacker-Werkzeuge wie Pineapples oder ESP8266-Deauther identifiziert.
- Deauth-Frames, die Endgeräte von Basisstationen trennen.
- Anomalien bei Signalstärken, etwa zusätzlich aufgestellte Access-Points oder physisch manipulierte Basisstationen, beispielsweise abmontierte Antennen.
- Unterschiedliche oder unerwartete Probe Responses bekannter Geräte.



Nyzme schlägt Alarm: Zu jedem Alert liefert die Software eine Erklärung, warum die Anomalie auf einen Angriff hindeutet. Zur besseren Einordnung gibt es auch einen Hinweis, warum es sich um einen False Positive handeln könnte.

Konfigurationsdatei entsprechend an. Mit etwas Herumprobieren sind die idealen Schwellenwerte für die Beacon-Rates der eigenen Basisstationen nach einigen Tagen gefunden, die naturgemäß etwas schwanken. Erst wenn die Werte sich etabliert haben und False-Positive-Alerts zurückgehen, sollten Sie die E-Mail-Benachrichtigungen einrichten, die Sie zuvor in der Konfigurationsdatei übersprungen haben.

Wanted: Hacking-Gadgets und andere Banditen

Als Banditen bezeichnet Nzyme Geräte, die anhand ihrer Hersteller-Identifikation als typische Hacker-Werkzeuge wie beispielsweise Wifi-Pineapple oder Deauther erkannt werden. Eine Reihe davon haben wir in c't bereits unter die Lupe genommen [1]. Neben der vorgefertigten Liste von Nzyme können Sie aber auch selbst Banditen definieren und nachverfolgen.

Bei der Kombination unterschiedlicher WLAN-USB-Sticks kann es zu Problemen bei dem automatischen Kanalwechsel und dem Versetzen in den Monitor-Mode kommen. Ist das bei Ihnen der Fall, meldet Nzyme dies sowohl im Log als auch im Web-Interface. Ein Wechsel des WLAN-Dienstes von wpa_supplicant zu iwd kann helfen. Die Dokumentation des Nzyme-Projektes, die wir unter ct.de/wfrn verlinkt haben, bietet Hilfestellung bei weiteren gängigen Problemen.

Weitere Anpassungen

Nzyme schützt Ihre Drahtlosnetzwerke, indem es verdächtige Aktivitäten aufspürt. Vergessen Sie jedoch nicht, auch Nzyme selbst zu schützen. Web-Interface und SSH-Zugang sollten nur aus einem verkabelten Management-Segment des Netzwerks erreichbar sein. Außerdem sollten Sie Transportverschlüsselung mittels TLS aktivieren. Dazu hinterlegen Sie die Pfade zu den Zertifikaten in der Konfigurationsdatei.

Je nach Größe und Struktur eines Drahtlosnetzwerkes lohnt es sich, zur großflächigen Abdeckung mehrere Nzyme-Raspis als Messpunkte aufzustellen, die ihre gesammelten Daten an ein zentrales Log-Management weiterleiten.

Fazit

Nzyme ist als Wifi-Intrusion-Detection-System (WIDS) eine sinnvolle Ergänzung zu bewährten IDS-Lösungen wie Snort oder Suricata. Es wird zum Auge und Ohr für jeden Admin von Drahtlosnetzwerken. Im Selbsttest konnte Nzyme sowohl einen simulierten Lauschangriff als auch die Imitation des eigenen Access-Point mittels SSID-Spoofing (Rogue-AP-Attacke durch WiFi Pineapple) erkennen und per Mail Alarm schlagen. Seine Stärke spielt Nzyme als automatisierte „Datenpumpe“ für eine zentrale Log-Auswertungssoftware wie Graylog aus, die nicht ganz ohne Zufall vom gleichen Entwickler stammt. (ndi) c't

Literatur

[1] Ronald Eikenberg und David Wischnjak, **Böse und billig**, Hacking-Gadgets, Gefahr durch angriffslustige Hardware, c't 18/2017, S. 64

[2] Ronald Eikenberg, **Raspi-Schnellstart**, Raspberry Pi superschnell einrichten durch Vorkonfiguration, c't 11/2021, S. 132

Nzyme-Projektseite, Dokumentation und Downloadbereich der Debian-Webseite

ct.de/wfrn

Logins absichern mit Authenticator

Um Zugänge bei Internetdiensten per Zwei-Faktor-Authentifizierung zu schützen, gibt es kostenlose Authenticator-Apps und erschwingliche Hardware. Damit erhöhen Sie das Sicherheitsniveau ganz erheblich, ohne sich bei Geräteverlust für immer auszusperren.

Von **Markus Montz**

Logins absichern mit Authenticator	62
2FA-Generator Reiner SCT Authenticator	66
Offener FIDO2-Schlüssel	69
Universal-Sicherheitsschlüssel TrustKey	70
FIDO2-Stick mit Fingerabdrucksensor	71
Dicekeys: Passwortgenerator mit Würfeln	72
Passwortmanager in Eigenregie hosten	76

Auch das beste Passwort (siehe S. 72) hat einen entscheidenden Nachteil: Errät oder erbeutet es ein Mensch mit sinistren Absichten, kann er sensible Daten ausspähen oder seinen Opfern direkt schaden, zum Beispiel finanziell oder sozial. Mit einer Zwei-Faktor-Authentifizierung (2FA) machen Sie Cyberkriminellen solche Einbrüche deutlich schwerer, denn zusätzlich zum Passwort müssen diese Zugang zu einem zweiten Kanal bekommen.

Der technisch eleganteste Ansatz ist ein zweiter Faktor auf einem Hardwarechip. So arbeiten FIDO2- oder U2F-Sticks (S. D30-D25). Ein kostenloser Weg ist ein dynamisch erzeugtes, zeitlich begrenzt gültiges Einmalpasswort – ein sogenanntes TOTP (Time-based One-Time Password). Idealerweise wird dieses auf einem getrennten Kanal generiert, etwa durch eine Software, die auf einem zweiten, vom ersten unabhängigen Gerät arbeitet. Doch selbst wenn beide Kanäle auf dem gleichen Gerät liegen, beispielsweise einem Smartphone, kann ein Angreifer zumindest nicht ohne Zugriff auf dieses Gerät zum Ziel kommen. Das bekannteste Beispiel für diesen Ansatz ist die TAN (Transaktionsnummer) im Onlinebanking: Mithilfe einer Smartphone-App oder eines dedizierten Gerätes, manchmal auch noch in Verbindung mit einer Chipkarte, müssen Sie Überweisungen oder Logins durch die zusätzliche Eingabe eines Zahlencodes absichern.

Nach dem gleichen Prinzip können Sie Mailkonten, Cloudzugänge, soziale Medien, einige Onlinehändler und etliche weitere Dienste besser vor unbefugtem Zugriff schützen. Gerade bei Ihren Mailkonten lohnt sich das: Wer die knackt, kann im schlimmsten Fall Ihre Passwörter bei Onlineshops, Messengern oder sozialen Medien zurücksetzen, Sie aussperren und reichlich Schindluder treiben.

Um eine TOTP-basierte 2FA einzurichten, bieten sich sogenannte Authenticator an. Diese gibt es als App für das Smartphone oder als dedizierte Hardware. Zwar ist auch die mitunter angebotene SMS als TOTP-Kanal besser als gar keine 2FA. Allerdings ist ihr Schutzniveau mangels Verschlüsselung und dem für Kriminelle relativ leichten Zugang zu Zweit-SIM-Karten (SIM-Swapping) niedriger. Ebenso können Sie Krypto-Sticks wie die auf Seite 70 oder die Yubikeys der 5er-Reihe zum Generieren der TOTP-Codes nutzen [1]. Das hat den Vorteil, dass die genutzten Geheimnisse auf einem geschützten Chip gespeichert werden. Dort sind sie nicht auslesbar und somit auch nicht duplizierbar.

Alternativ gibt es Hardware wie den Reiner SCT Authenticator (ab 32 Euro), den wir auf Seite 66 vorstellen. Der Vorteil der autarken Hardware ist, dass sie anders als ein Smartphone nicht aus dem Internet erreichbar und somit nicht angreifbar ist. Achten Sie darauf, das Gerät mit einer PIN zu schützen.

Alternativ zu einer Smartphone-App können Sie auch einen Hardware-Authenticator nutzen. Das Angebot an solchen Gadgets ist bisher aber überschaubar.

Einrichten und nutzen

Ein softwarebasiertes TOTP wird aus zwei Teilen erzeugt. Bei der Einrichtung der 2FA erhält die App oder Hardware zunächst vom Server des Dienstes ein Geheimnis (Shared Secret Key), das nur diese beiden Parteien kennen. Um daraus das TOTP zu generieren, fließt zusätzlich die aktuelle Unix-Zeit ein, also die seit 1. Januar 1970 um 0 Uhr UTC verstrichene Zeit in Sekunden. Daraus berechnen beide Seiten einen 30 Sekunden lang gültigen kryptografischen Hashwert, aus dem das TOTP destilliert wird. Das ist meist ein sechsstelliger Zahlencode [2].

Es gibt diverse kostenlose Authenticator-Apps, die allesamt diese Aufgabe erfüllen. Welche Sie nehmen, ist eine Frage des persönlichen Geschmacks. Am bekanntesten sind die Apps von Google und Microsoft sowie Authy von Twilio. Es gibt Open-Source Lösungen wie andOTP und Free OTP; KeePass-Nutzer können das darin enthaltene TOTP-Modul verwenden (Links unter ct.de/w4hx). Wichtig ist, dass sich Ihr Smartphone nur durch PIN, Passwort oder biometrisch entsperren lässt, sollte das Gerät einmal in die falschen Hände geraten – auch wenn manche Apps zusätzlich einen eigenen PIN- und Biometrie-

schutz bieten. Dies gilt insbesondere, wenn es sich um einen Passwort-Manager auf dem Smartphone handelt, der Passwörter *und* die dazu passenden TOTP-Codes ausspuckt.

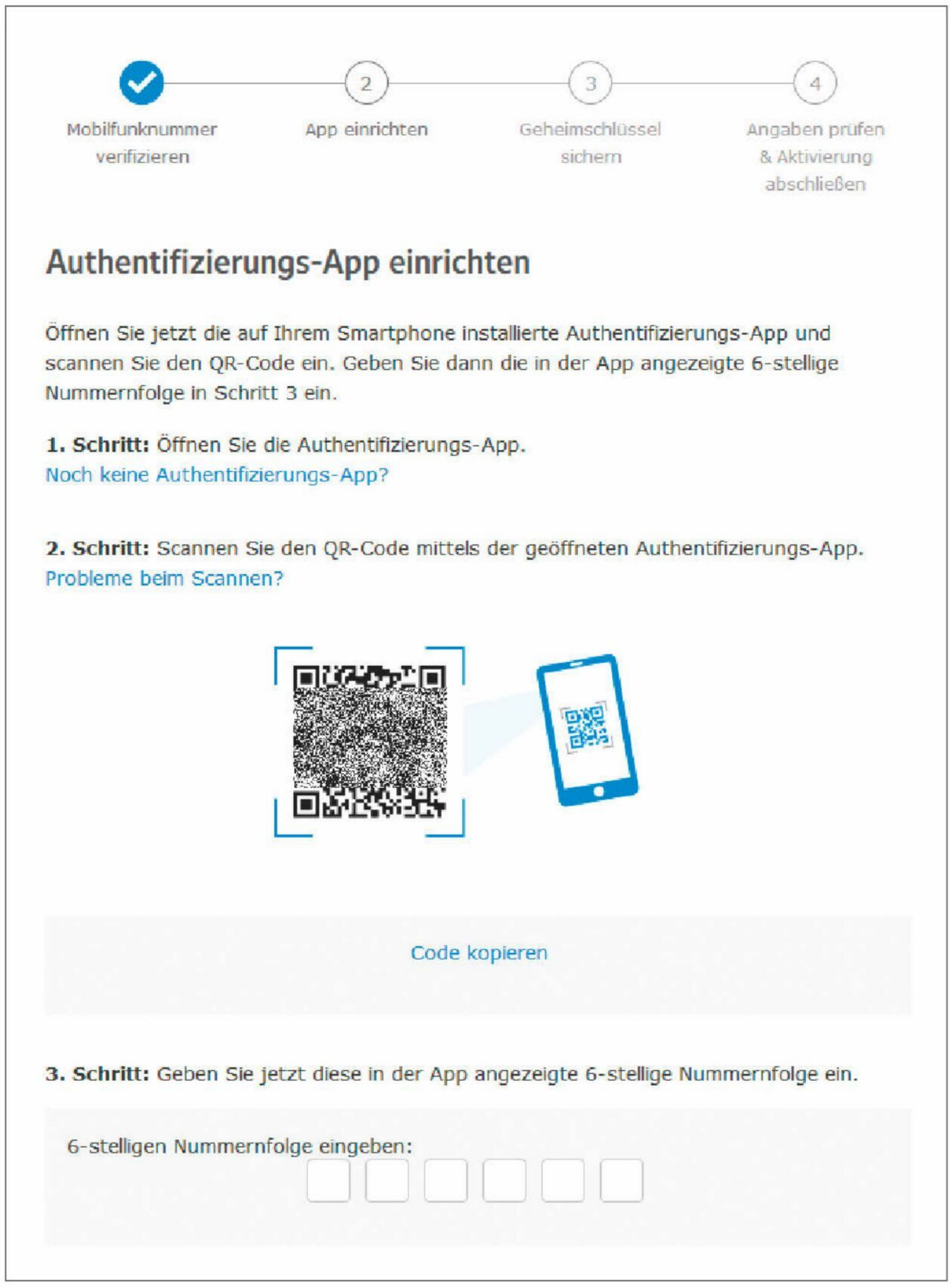
Eine 2FA per TOTP können Sie beispielsweise bei Google, Samsung und Microsoft, Maildiensten wie Posteo und GMX, sozialen Netzwerken wie Twitter und Facebook, Bezahldiensten und Shops wie PayPal und Amazon, diversen Webhostern sowie vielen Kryptobörsen einrichten. Einen gut sortierten Überblick finden Sie auf der englischsprachigen Seite 2FA Directory (siehe ct.de/w4hx); ein Haken bei „Software Token“ steht dort für Authenticator-Unterstützung. Die Einrichtung der 2FA bei den verschiedenen Diensten ist simpel und läuft relativ ähnlich ab. Oft finden Sie diese in den Einstellungen unter „Sicherheit“, „Login“ oder „Passwort“. Im Aktivierungsprozess zeigt Ihnen der Dienst dann einen QR-Code oder eine Zeichenkette für den Schlüsseltausch. In der App oder auf dem Gerät klicken Sie auf „Hinzufügen“ und können den QR-Code nun einscannen oder die Zeichenkette eintippen. Anschließend geben Sie zur Kontrolle erstmals das TOTP ein – fertig.

Fortan wird Ihnen das TOTP als sechsstelliger Zahlencode in der Liste der App oder des Gadgets angezeigt. Dieser wechselt alle 30 Sekunden, wobei er meist noch einige Sekunden länger gültig ist. Wollen Sie sich nun in den jeweiligen Dienst einloggen, müssen Sie ab sofort zusätzlich zum Passwort den gerade gültigen Code eingeben.

Wiederherstellung

Normalerweise können Sie nur ein Gerät pro Dienst für das TOTP nutzen. Ist dies ein Smartphone, sind Sie auf eine App beschränkt. Das bedeutet auch: Wird das Gerät gestohlen, geht verloren oder lässt sich die App nicht mehr starten, ist der zweite Faktor weg und Sie können Ihren Zugang oft nur noch mühselig wiederherstellen. Wie das geht, erklärt der Dienst meistens während des 2FA-Aktivierungsprozesses; schreiben Sie am besten mit und bringen Sie hinterlegte Daten wie Telefonnummern, Post- und Mailadressen zur Reaktivierung auf den aktuellen Stand.

Sie können sich allerdings viel Zeit und Mühe ersparen, wenn Sie bei der Einrichtung den QR-Code gleich mit mehreren Geräten scannen oder den Startwert sichern, den sogenannten Seed. Das ist das Geheimnis, das sich Authenticator und Server des Dienstes teilen. Der Seed steckt im QR-Code für die 2FA-Einrichtung. Viele (aber nicht alle) Dienste zeigen ihn aber auch als „Backup-Code“, „Secret“ und dergleichen genannte Zeichenkette an. Den Seed sollten Sie sich ganz altmodisch abschreiben oder ausdrucken und sicher verwahren. Wir raten davon ab, ihn auf dem Rechner oder in der Cloud zu speichern, weil dort im Fall der Fälle auch ein Hacker darauf zugreifen kann.



Um die Zwei-Faktor-Authentifizierung eines Dienstes im Authenticator zu aktivieren, müssen Sie meist einen QR-Code einscannen und anschließend zur Bestätigung das erste Einmalpasswort eingeben.

Komfort-Kompromisse

Wenn Sie bereit sind, zwischen maximaler Sicherheit und etwas mehr Komfort abzuwägen, können Sie sich das Leben erleichtern – und haben immer noch ein höheres Schutzniveau als mit einem Passwort allein. Die meisten Apps bieten Funktionen, um den Authenticator samt Seeds der hinterlegten Dienste auf ein neues Gerät umzuziehen oder auf ein weiteres Gerät zu übertragen. Authy enthält eigens zu diesem Zweck eine Synchronisationsfunktion, der Google Authenticator erzeugt zur Weitergabe einen QR-Code, den Sie mit der gleichen App auf einem anderen Gerät abscannen können. Nutzen Sie diese Funktionen aber mit Bedacht. Je mehr Geräte Sie für die 2FA aktivieren, desto mehr potenzielle Ziele haben auch Angreifer.

Auch bei der Eingabe des TOTP können Sie oftmals den Komfort erhöhen: Nach einmaliger 2FA lassen sich dort das beim Login verwendete Gerät und darauf befindliche Apps und Browser von der 2FA ausnehmen. Dazu wird ein vertrauenswürdiges Token hinterlegt. Meist können Sie diese Option in der Login-Maske auswählen. Trotz Ihres Komfortgewinns muss ein Angreifer, der über ein fremdes Gerät auf eines Ihrer Nutzerkonten zugreifen will, weiterhin eine 2FA durchführen. Geräte, auf denen Sie solch eine Komfortfunktion aktivieren, sollten Sie aber gut vor unbefugtem Zugriff schützen. Am besten aktivieren Sie auch etwaige Alarmfunktionen für Zugriffsversuche von unbekannten Geräten. Dann bekommen Sie beispielsweise eine Warnmail auf Ihr Zweit-Mailkonto bei einem anderen Dienst. Das geht unter anderem bei Google und GMX.

Sie können Ihre Nutzerkonten außerdem einfach auf zwei oder mehr Authenticatoren aufteilen. So lassen sich beispielsweise beruflich und privat genutzte Konten trennen oder besonders sensible Zugänge kompromisslos schützen, während Sie bei anderen gewisse Zugeständnisse an den Komfort machen.

Fazit

Wie stark Ihre Passwörter auch sind: Jede 2FA bietet prinzipbedingt mehr Schutz als ein Passwort allein. App-basierte Authenticator-Lösungen sind sogar kostenlos und einfach für viele Onlinedienste umzusetzen. Auch der Komfort muss darunter nicht signifikant leiden, wenn Sie kleinere Kompromisse in Sachen Sicherheit eingehen können und gut auf die beteiligten Geräte aufpassen. (mon) c't

Literatur

[1] Jan Mahn, FIDO2-Hardware einrichten und ausreizen, c't Security 2020, S. 130

[2] Jürgen Schmidt, **Doppelt genäht**, Zwei-Faktor-Authentifizierung schmerzfrei einsetzen, c't 24/2018, S. 178

Apps und Liste von Diensten mit 2FA-Option

ct.de/w4hx

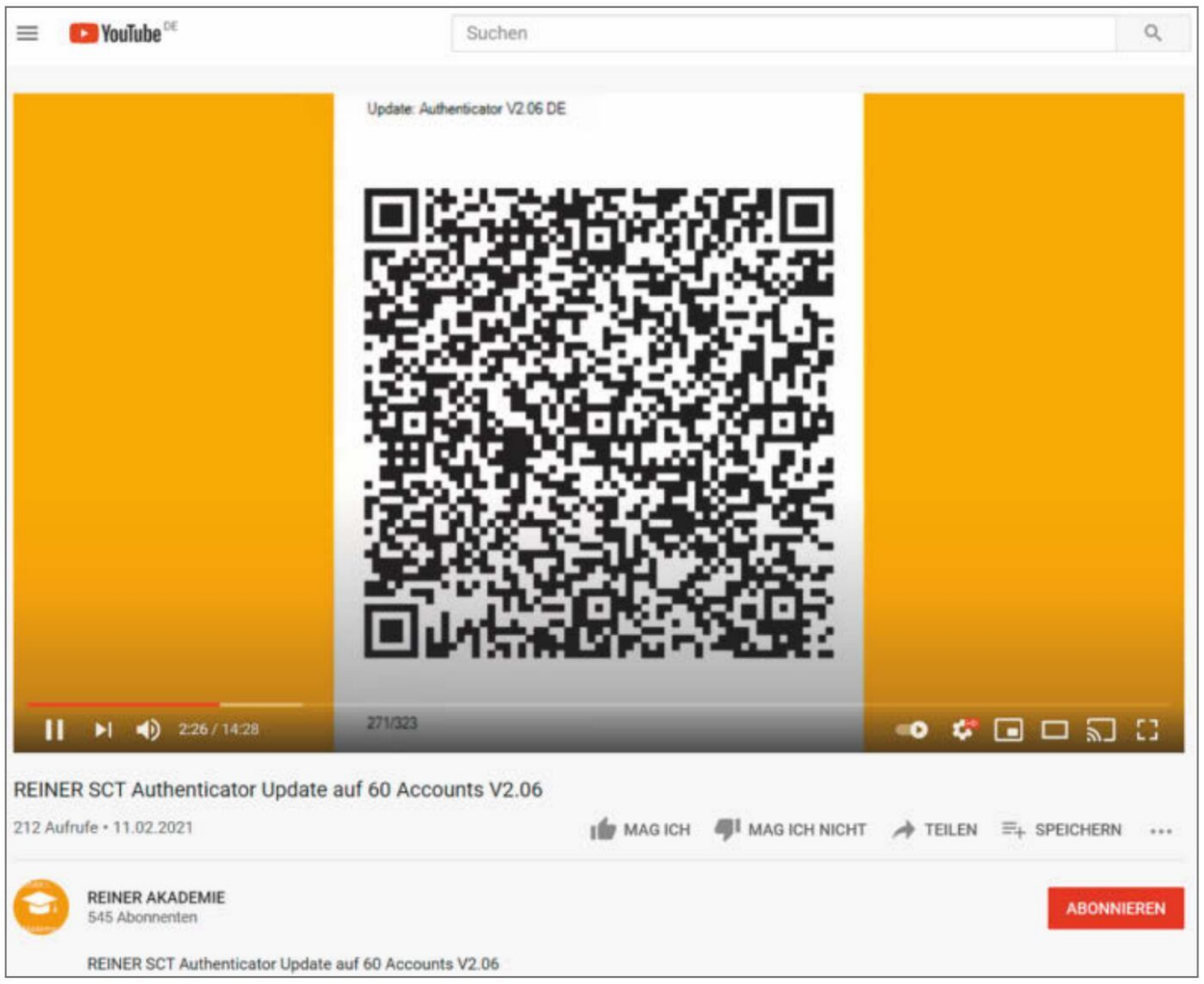
2FA-Generator Reiner SCT Authenticator

Der Reiner SCT Authenticator sichert Online-Accounts als zweiter Faktor ab. Das ist komfortabler und leichter verständlich als per Smartphone-App.

Von **Ronald Eikenberg**

Ein zweiter Faktor ist das Beste, was Ihren Online-Accounts passieren kann: Haben Sie die Zwei-Faktor-Authentifizierung (2FA) aktiviert, dann ist Ihr Account auch dann noch geschützt, wenn ein Hacker Ihr Passwort kennt. Der zweite Faktor ist zum Beispiel ein Einmalcode, den Ihnen der Dienst per SMS zuschickt oder den eine Authenticator-App generiert. Das Einloggen gelingt mit 2FA nur dann, wenn sowohl das Passwort als auch der aktuell gültige Einmalcode stimmen. Damit der Schutz wirksam ist, darf der Hacker nicht die Chance bekommen, den Einmalcode abzurufen oder zu generieren.

Würde der Code-Generator einfach nur als Software auf dem Rechner laufen, mit dem Sie sich einloggen, könnte ein Trojaner nicht nur das eingetipp-



Ungewöhnlich, aber effektiv: Der Reiner Authenticator zieht sein Firmware-Update, indem er ein YouTube-Video abfilmt. Die Update-Daten sind in die flimmernden QR-Codes kodiert.

te Passwort, sondern auch den Code-Generator mit allen Geheimnissen abgreifen. Daher ist es sinnvoll, den Code mit einer separaten Hardware zu generieren. Das kann im einfachsten Fall das Smartphone mit Authenticator-App sein, aber auch ein USB-Stick wie ein YubiKey oder TrustKey (siehe S. 70).

Der deutsche Kartenleser-Hersteller Reiner SCT setzt zu diesem Zweck nicht auf Hardware mit Kryptochips wie die auf Seite 69 bis 71 vorgestellten FIDO2- und U2F-Sticks und auch nicht auf Authenticator-Apps auf dem Smartphone. Er bietet stattdessen eine alternative Option an, die bei näherer Betrachtung durchaus sinnvoll ist: Der Reiner SCT Authenticator ist ein autarkes Gerät mit Zifferntastatur und Farbdisplay. Er besitzt keine Schnittstellen zur Außenwelt. Somit ist genau wie bei den Kryptosticks gewährleistet, dass ein Trojaner, der eventuell auf Ihrem Rechner oder Smartphone lauert, keinen Zugriff darauf hat und keine Einmalcodes generieren kann.

Der Authenticator arbeitet dazu mit demselben zeitbasierten TOTP-Verfahren (Time-based One-time Password), das die meisten Online-Dienste unterstützen, die Zwei-Faktor-Authentifizierung anbieten, darunter Google, Facebook und Twitter (S. 62). Das Gerät ist mit einem Display und einer Zifferntastatur ausgestattet und erinnert äußerlich an einen Taschenrechner. Neue Accounts fügt man jedoch nicht umständlich über die Zifferntasten hinzu, sondern über die kleine Kamera auf der Rückseite: Sie scannt das für TOTP nötige Krypto-Geheimnis einfach als QR-Code vom Webdienst.

PIN-Sperre mit Selbstzerstörung

Nach dem Einschalten drückt man zwei Mal auf den OK-Knopf, um das Gerät in den Scanmodus zu versetzen und den Code zu scannen. Das hat im Test zuverlässig funktioniert, das Scannen dauerte lediglich eine Sekunde. Anschließend generiert der Authenticator einen passenden TOTP-Code, wenn man den gewünschten Account in der Liste auswählt. Der Zugriff lässt sich durch eine bis zu 12-stellige PIN schützen. Ist der PIN-Schutz aktiv, führt das Gerät nach fünf Fehlversuchen einen Reset auf Werkseinstellungen durch.

Damit ist der Funktionsumfang auch schon fast erzählt. Über das zweckmäßige Menü kann man die

Auf der Rückseite des Authenticators befindet sich eine Kamera, mit der man QR-Codes fotografiert. So kann man Online-Accounts leicht mit dem Gerät verknüpfen.

PIN-Sperre konfigurieren, Account-Einträge umsortieren und löschen sowie Batteriestatus und Seriennummer abfragen. Hier lässt sich zudem eine Komfortansicht aktivieren, die sich jedoch kaum von der Standardansicht unterscheidet. Der Authenticator ist mit einer Uhr ausgestattet, die er benötigt, um die zeitbasierten OTP-Codes zu erzeugen. Sie kann über das Menü oder das Scannen eines QR-Codes gestellt werden. Eine Pufferbatterie sorgt dafür, dass man sich circa eine Minute mit dem Wechseln der vier AAA-Batterien Zeit lassen kann, ohne dass die eingestellte Uhrzeit verloren geht. Laut Hersteller halten die Batterien fünf Jahre, wenn pro Jahr 500 TOTP-Codes generiert werden.

Firmware-Update über YouTube

Ursprünglich konnte sich der Reiner SCT Authenticator lediglich zehn Accounts merken, inzwischen hat der Hersteller jedoch mit der Firmware-Version 2.06 auf 60 aufgestockt. Wer das Gerät mit der alten Firmware gekauft hat, kann das Update nachträglich installieren – das ist ziemlich interessant, weil der Authenticator keine der üblichen Datenschnittstellen wie USB hat. Der Hersteller hat dieses Problem kreativ gelöst: Das Update erfolgt per YouTube-Video. Im Video flimmern einige Minuten QR-Codes über den Bildschirm, in die das Firmware-Update kodiert ist. Versetzt man den Authenticator in den Scan-Modus und filmt den Bildschirm einige Minuten ab, während im Hintergrund beruhigende Musik läuft, ist das Gerät anschließend auf dem aktuellen Firmware-Stand. Das klingt seltsam, funktioniert aber. Der Hersteller empfiehlt, das Video mit der 360p-Auflösung abzuspielen, damit das Update reibungslos über die Bühne geht.

Im Alltagstest hat sich der Authenticator erstaunlich gut bewährt. Liegt das quietschgelbe Gerät neben der Tastatur, hat man den geforderten TOTP-Code schnell parat. Das geht schneller von der Hand, als etwa das Smartphone aus der Hosentasche zu ziehen, zu entsperren und den Google Authenticator zu starten. Wer bereits eine Authenticator-App mit allen Accounts eingerichtet hat, kann diese mit etwas Glück schnell auf den Reiner Authenticator übertragen: Mit der Android-App andOTP konnten wir einfach QR-Codes zu den hinterlegten Accounts anzeigen lassen, die sich mit dem Reiner-Gerät einlesen ließen. Der bei andOTP eingestellte „Aussteller“ wurde anschließend auf dem Reiner Authenticator als Dienstname angezeigt. Mit dem Google Authenticator klappte der Export jedoch nicht, das Gerät wusste mit den angezeigten QR-Codes nichts anzufangen. Es ist problemlos möglich, den von einem Webdienst angezeigten QR-Code mit mehreren Authentifikatoren zu scannen und das Reiner-Gerät parallel mit einer App zu nutzen.

Fazit

Die Zwei-Faktor-Authentifizierung ist mit dem Reiner SCT Authenticator zugänglicher als per Smartphone-App oder USB-Stick. Durch seinen reduzierten Funktionsumfang ist das Gerät intuitiv bedienbar, die Nutzung hat Parallelen zu TAN-Verfahren beim Online-Banking. Damit ist es auch für Personen verständlich, die mit der Nutzung einer Authenticator-App überfordert wären. (rei) c't

Reiner SCT Authenticator

OTP-Generator	
Hersteller	Reiner SCT, www.reiner-sct.de
Anschlüsse	–
OTP-Verfahren / Accounts	OATH-TOTP (SHA 1, SHA 256, SHA 512) / 60
Display / Auflösung	1,77"-TFT / 128 × 160 Pixel
Größe / Gewicht	102 mm × 62,5 mm × 19 mm / 80 g
Stromversorgung	4 × AAA-Batterien
Preis	40 €

Produktseite, Update-Video
ct.de/wwfs

Offener FIDO2-Schlüssel

Der Nitrokey FIDO2 sichert Online-Accounts ab und steht unter einer Open-Source-Lizenz.

Von **Ronald Eikenberg**

Das Authentifizierungsverfahren FIDO2 schützt Online-Accounts effektiv vor Hackern. Je nach Online-Dienst dient FIDO2 entweder als zweiter Faktor oder gar als Passwortersatz. Im c't Security 2020 ab S. 122 haben wir eine Reihe von FIDO2-Sticks detailliert vorgestellt und unter anderem erklärt, wie man sie bestmöglich nutzen kann. Mit dem Nitrokey FIDO2 ist jetzt ein Nachzügler erhältlich, der vieles richtig macht.

Während sich große Hersteller wie Yubico verschlossen zeigen und keine Einblicke in die Firmware gestatten, gibt sich Nitrokey erfreulich offen: Hard- und Software des Nitrokey FIDO2 sind Open Source. Wer will, kann mit den Daten aus dem GitHub-Repository des Herstellers die Funktion des Sticks komplett nachvollziehen. Theoretisch wäre es sogar möglich, den Stick selbst zu bauen und die Firmware zu kompilieren. Der Stick wird laut Hersteller komplett in Deutschland produziert, was das Risiko einer Manipulation auf dem Transportweg reduziert.

SoloKeys-Projekt als Basis

Die Firmware des FIDO2-Sticks basiert auf dem SoloKeys-Projekt, an dessen Entwicklung sich Nitrokey beteiligt hat. Dementsprechend funktionierte der Nitrokey FIDO2 in unserem Test genauso zuverlässig und problemlos wie die SoloKeys. Wir konnten auf Anhieb die gängigen FIDO2-kompatiblen Dienste wie Twitter mit dem Stick nutzen. Auch die Königsdisziplin, das Einloggen bei Microsoft.com ohne Passwort, brachte den Nitrokey nicht aus dem Konzept. Zudem konnten wir das Gerät als zweiten Faktor über das ältere U2F-Protokoll einsetzen. Wie auch bei den SoloKeys ist die Firmware des Nitrokey FIDO2 aktualisierbar, man kann also auf neue Funktionen hoffen. So befindet sich etwa eine OpenPGP-Anbindung in der Entwicklung, die den Stick als Smartcard nutzbar macht.

Das schwarze Kunststoffgehäuse des Nitrokey FIDO2 ist optisch unspektakulär, denn das spannendste Feature ist unsichtbar: Es gibt keinen Knopf, mit dem man die FIDO2-Prozesse bestätigt. Stattdessen berührt man das Gehäuse auf der Oberseite, um den kapazitiven Touch-Sensor auszulösen. Das hat den Vorteil, dass man keinen Druck auf die USB-Buchse ausübt. Dies hatten wir bei den SoloKeys bemängelt: Um deren Taster zu bestätigen, ist etwas Kraft nötig, die auf die USB-Schnittstelle übertragen wird.

Derzeit gibt es den Nitrokey FIDO2 nur mit USB-A, für die Zukunft hat der Hersteller eine Version mit USB-C und NFC in Aussicht gestellt. Bis dahin kann man sich mit einem USB-A-auf-C-Adapter behelfen, dem man für drei Euro im Herstellershop mitbestellen kann. Wer mit der Anschaffung eines FIDO2-Sticks liebäugelt und Wert auf Open Source legt, macht mit dem Nitrokey FIDO2 nichts verkehrt. (rei) c't

Nitrokey FIDO2

FIDO2-Sicherheitsschlüssel	
Hersteller	Nitrokey GmbH, www.nitrokey.com
Anschluss	USB-A
Preis	29 € (plus 4 € Versand)

Universal-Sicherheits-schlüssel TrustKey

Die TrustKey-Sicherheitsschlüssel beherrschen drei Verfahren zur Absicherung von Online-Accounts und sind damit vielseitig einsetzbar.

Von **Ronald Eikenberg**

Die beiden FIDO2-Sicherheitsschlüssel TrustKey T110 (USB-A) und T120 (USB-C) schützen Online-Accounts als zweiter Faktor oder Passwortersatz zuverlässig vor Zugriffen durch Hacker. Neben dem modernen FIDO2-Verfahren, das sogar sichere Logins ohne Passwort vorsieht, unterstützen die beiden TrustKey-Sticks wie die meisten FIDO2-Schlüssel auch das ältere U2F (FIDO1) sowie OTP (S. 62). Das macht sie vielseitig, denn nach wie vor ist die Anzahl der Online-Dienste überschaubar, bei denen man sich mit FIDO2 authentifizieren kann.

Um das OTP-Verfahren zu nutzen, installiert man den TrustKey Key Manager von der Herstellerwebsite. Aktuell gibt es ihn für Windows und macOS. Der Windows-Installer des Tools verwirrte uns im Test, da er nur kurz auf dem Bildschirm aufblitzte und uns nicht wie erwartet durch die Installation leitete. Anschließend ließ sich der Key Manager dennoch über das Startmenü ausführen. Der Funktionsumfang des Tools ist aufs Nötigste reduziert.

QR-Code-Scan

Zunächst muss man den Sicherheitsschlüssel mit einer PIN schützen, anschließend kann man Accounts mit ihm verknüpfen. Das Tool durchsucht den Bildschirm automatisch nach dem QR-Code, den die meisten Onlinedienste bei der Einrichtung von OTP anzeigen. Alternativ kann man auch einen Kryptoschlüssel in den Einrichtungsdialog des Key Managers kopieren. Den Kryptoschlüssel erhält man vom jeweiligen Onlinedienst während der Einrichtung. Anschließend erscheint ein Eintrag für den hinzugefügten Dienst im Hauptfenster des Key Managers. Ein Klick darauf erzeugt einen passenden Einmalcode.

Nur wer den TrustKey-Stick physisch besitzt, kann OTP-Codes damit generieren. Er ist nicht kopierbar. Die Sicherheitsschlüssel unterstützen die beiden gängigen Verfahren TOTP und HOTP. Die Authentifizierung mittels FIDO2 und U2F funktionierte im Test ebenso wie das Einloggen ohne Passwort auf Anhieb. Die beiden Sicherheitsschlüssel verhielten sich identisch. Einziger Unterschied: Der T110 ist mit dem weit verbreiteten USB-A-Anschluss ausgestattet, der T120 nimmt über das moderne USB-C Kontakt auf.

Fazit

Beide Modelle sind gut verarbeitet und wirken robust. Zur Bestätigung einer FIDO-Authentifizierung muss man die goldfarbene Kontaktfläche lediglich leicht berühren, wodurch der USB-Anschluss nicht mechanisch belastet wird. Zur Nutzung von OTP muss auf dem Sicherheitsschlüssel eine aktuelle Firmware laufen, die auf den derzeit vom deutschen Shop ausgelieferten Exemplaren bereits vorinstalliert ist. Nachträglich aktualisieren lässt sich die Firmware derzeit nicht. (rei) c't

TrustKey T110 & T120

FIDO2-Sicherheitsschlüssel		
Modell	T110	T120
USB-Anschluss	USB-A	USB-C
Resident Keys / U2F / OTP	✓ / ✓ / ✓	✓ / ✓ / ✓
Preis	28,56 € zzgl. 5,95 € Versand	30,34 € zzgl. 5,95 € Versand
Bezugsquelle	webshop.pointblank.de	webshop.pointblank.de
Bewertung		
Kompatibilität	⊕⊕	⊕⊕
Bedienung	⊕	⊕
Extras	⊕	⊕
Robustheit	⊕⊕	⊕⊕

⊕⊕ sehr gut ⊕ gut ✓ vorhanden – nicht vorhanden

FIDO2-Stick mit Fingerabdrucksensor

Der neue FIDO2-Stick mit Fingerabdrucksensor von Yubico gibt FIDO-Anmeldungen erst frei, wenn man sich per PIN oder Fingerdruck zu erkennen gibt. Entscheidend ist aber, was er nicht kann.

Von **Jan Mahn**

Den neuen FIDO2-Stick YubiKey Bio gibt es in zwei Varianten, mit USB-A- oder USB-C-Stecker. Äußerlich ist am YubiKey Bio nichts auszusetzen. Yubico schafft auch bei der USB-C-Variante das Kunststück, den schmalen Stecker so mit dem Rest des Sticks zu verbinden, dass er auch bei rohen Kräften nicht im geringsten wackelt, sodass einem Dauerbetrieb am Schlüsselbund nichts im Wege steht.

Der Fingerabdrucksensor reagiert sehr zügig. Dies ging im Test nicht auf Kosten der Genauigkeit: Auf eine Kopie des Fingerabdrucks aus einer dünnen Schicht Holzleim, die man erst aufträgt, trocknen lässt und dann verkehrt herum aufdrückt, fiel der YubiKey genau so wenig herein wie auf einen Streifen Klebefilm mit anhaftendem Abdruck.

Schon nach drei Fehlversuchen ist der Fingerabdrucksensor gesperrt und man muss die PIN eingeben. Die darf, weil man sie bestenfalls nur selten nutzt, durchaus kompliziert sein. Gibt der unberechtigte Finder auch die PIN achtmal falsch ein, kann man den Stick nur noch zurücksetzen. Er generiert dann ein neues Schlüsselpaar und man muss ihn neu bei den Diensten registrieren.

Zum Einrichten von PIN und Fingerabdruck kann man unter Windows die bordeigenen Werkzeuge in den Systemeinstellungen von Windows Hello nutzen. Unter macOS und Linux reicht ein Chrome-Browser, der beim ersten Registrierungsversuch die Einrichtung anbietet. Wer mehr als einen Finger anlernen will, braucht die kleine Desktop-App Yubico Authenticator, die es kostenlos für Windows, Linux und macOS gibt. Nach der Einrichtung brauchen Sie auf dem Computer, auf dem Sie sich mit FIDO2 anmelden wollen, keine zusätzliche Software. Die Unterstützung der Fingerabdruckfunktion in den Browsern ist in Ordnung – wenn auch noch nicht perfekt. Auf dem Mac funktionierte die Fingerabdruckfunktion nur unter Chrome und Firefox. Safari fragte nach dem Antippen mit dem richtigen Finger immer nach der PIN. Firefox war nicht in der Lage, bei falschen Fingern auf PIN-Eingabe umzuschalten.

Keine Extras

So praktisch der Sensor und die FIDO2-Anmeldung per Fingerdruck auch sind, so enttäuschend ist die weitere Ausstattung des YubiKey Bio: Außer U2F und FIDO2 bringt er keine Funktionen mit. Die YubiKeys aus der 5er-Reihe arbeiten zusätzlich noch als Smart-Card-Gerät, können OpenPGP-Schlüssel speichern und Einmalpasswörter (OTP) generieren (siehe S. 62). Letztere Funktion braucht man zum Beispiel, um eine Keepass-Datenbank mit dem Stick auf- und zuzuschließen. Auch eine NFC-Funktion, um den YubiKey kontaktlos an einem Mobiltelefon zu nutzen, fehlt.

Den Fingerabdrucksensor als komfortabler Ersatz für eine lange PIN lässt sich Yubico aber gut bezahlen: Für den happigen Preis von 95 Euro ist die Ausstattung spärlich, gibt es doch den YubiKey 5C NFC mit kryptografischer Vollausstattung schon für 53 Euro. Für denselben Preis gibt es bei Mitbewerbern schon FIDO2 mit biometrischer Sicherung – etwa den Trustkey G310. Wer gehofft hatte, auch seine Mails mit PGP per Fingerabdruck signieren zu können, muss darauf hoffen, dass Yubico den Sensor irgendwann in einen besser ausgestatteten Stick einbaut. (jam) c't

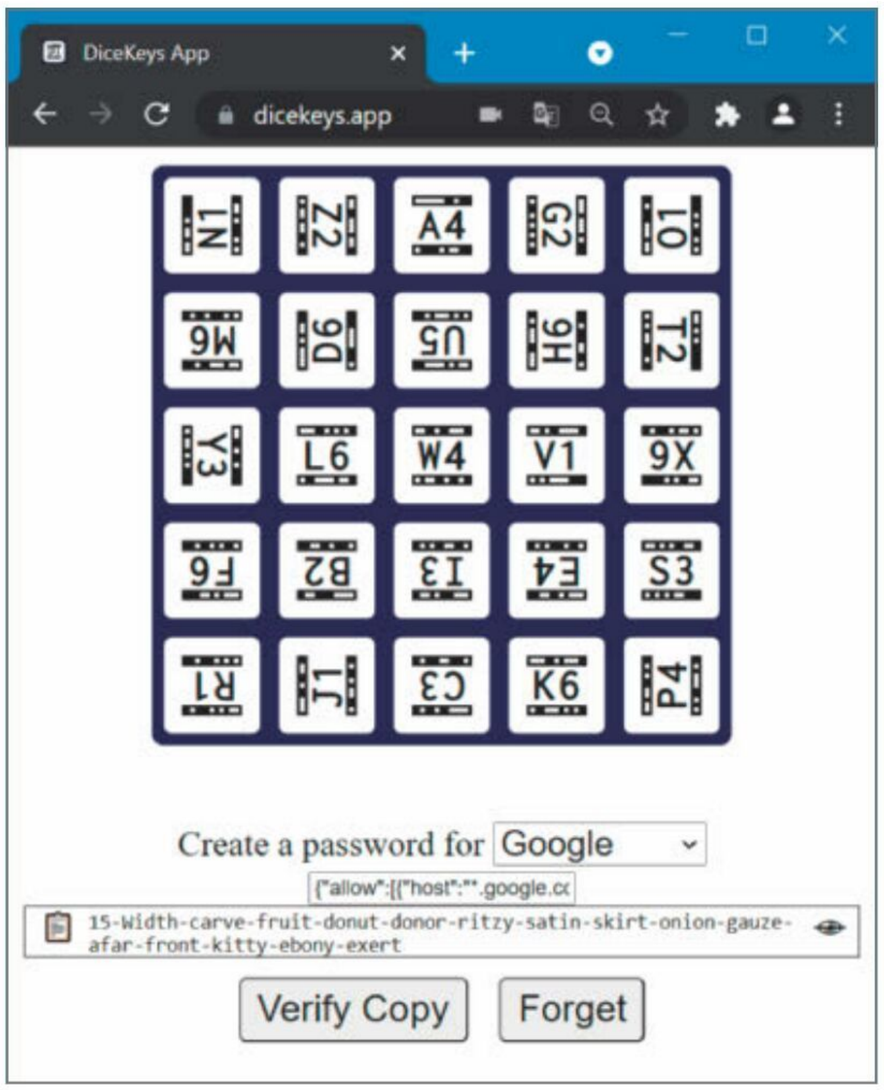
YubiKey Bio	
FIDO2-Stick mit biometrischer Sicherung	
Hersteller, URL	Yubico, yubico.com/de/store
Authentifizierungsfunktionen	U2F, FIDO2
Preis	95,20 €

DiceKeys: Passwort-generator mit Würfeln

Gute Passwörter sind lang und kommen nur bei einem Dienst zum Einsatz. Mit den DiceKeys und der dazugehörigen App erwürfelt man sie sich einfach.

Von **Ronald Eikenberg**

DiceKeys ist kein neues Würfelspiel für Nerds, sondern ein Passwortgenerator. Mit den 25 Plastikwürfeln erwürfelt man zunächst einen zufälligen Kryptoschlüssel (DiceKey), der als Grundlage für die Kennwörter dient. Jeder der sechsseitigen Würfel ist einzigartig und mit einem Buchstaben von A bis Z beschriftet. Zudem haben alle Seiten eines Würfels eine Zahl von 1 bis 6, damit klar ist, welche Seite oben liegt. Die gefallenen Würfel scannt man anschließend mit einer Smartphone-App, die damit



Über die Web-App kann man die DiceKeys mit jedem Betriebssystem im Browser nutzen und vor dem Kauf ausprobieren.

lange Passwörter für beliebige Onlinedienste und andere Zwecke generiert. Ein damit generiertes Kennwort für heise.de könnte etwa `15-Shown-groom-koala-flock-shale-wrath-sleep-henna-dance-dudes-grout-scam-patio-alias-jumbo` lauten. Solche Passphrasen gelten als sicher, weil die Zeichenanzahl ein effektiverer Stellhebel für die Passwortsicherheit ist als der Einsatz möglichst vieler Sonderzeichen. Da viele Onlinedienste die Passwortlänge unnötig begrenzen, kann die App aber auch kürzere Passwörter erzeugen.

Die Passphrasen generiert die DiceKeys-App nach einem dokumentierten Algorithmus, in den neben dem gewürfelten Kryptoschlüssel auch die URL des Dienstes einfließt, für den die Passphrase bestimmt ist (etwa https://heise.de). So kommt für jeden Dienst eine andere Passphrase heraus. Diese lässt sich zu jedem späteren Zeitpunkt reproduzieren, weshalb die generierten Passphrasen – anders als bei einem herkömmlichen Passwortmanager – nicht gespeichert werden müssen. Benötigt man die für heise.de genutzte Passphrase zum Einloggen, wird sie von der App ad hoc neu generiert. Wichtig ist bei diesem Konzept, dass der gewürfelte Kryptoschlüssel niemals verloren geht, sonst besteht keine Chance, die Passphrasen jemals wieder abzurufen.

Die Würfel sind gefallen

Deshalb würfelt man die 25 US-Dollar teuren DiceKeys nur ein Mal: Man lässt die Würfel in die blaue Box purzeln, in der sie zumeist von selbst einen Platz im Raster finden. Die Lücken werden anschließend mit den übrigen Würfeln gefüllt, die ihr Ziel verfehlt haben. Zu guter Letzt kommt das Oberteil der Box drauf, das fest einrastet und so konstruiert ist, dass sich die Box nicht mehr auseinandernehmen lässt. Die Würfel sind also gefallen – und für immer fixiert. Eine Klappe auf der Oberseite gibt den Blick auf die Würfel frei, etwa wenn man sie mit der für Android und iOS erhältlichen App etwa scannen möchte. Die Würfel sind nicht nur mit Buchstaben und Zahlen beschriftet, sondern auch mit einer optischen Codierung, wodurch das Einlesen so zuverlässig und flott über die Bühne geht wie bei einem QR-Code.

Auch das Einscannen ist nur einmalig nötig, da sich die App die Würfelkonstellation merken kann. In diesem Fall wird der gewürfelte Key verschlüsselt gespeichert und der Zugriff darauf per Fingerabdruck geschützt. In der App legt man Einträge für die Dienste an, die man mit DiceKeys nutzen möchte. Dies ist lediglich eine Komfortfunktion, die dafür sorgt, dass man die Dienste innerhalb der App bequem auswählen kann, um eine Passphrase abzurufen. Beim Anlegen fragt die App nach der URL des Dienstes, die in die Passwortgenerierung einfließt. Es muss sich nicht um eine gültige Webadresse handeln, eine beliebige Zeichenfolge genügt. Geht es um eine lokale Anwendung wie VeraCrypt, kann man also auch einfach „VeraCrypt“ eingeben. Darunter gibt es eine Sequenznummer, die ebenfalls in den Passwortalgorithmus fließt. Setzt man sie von 1 hoch, kommen weitere Passphrasen für den gleichen Dienst raus. Schließlich lässt sich noch die Passwortlänge begrenzen (6 bis 999 Zeichen).

Ein Button kopiert die generierten Passphrasen auf Wunsch in die Zwischenablage, sodass man sie nicht umständlich von Hand ins jeweilige Login-Formular eintippen muss. Eine Auto-Ausfüllen-Funktion gibt es jedoch nicht, ebenso wenig wie einen Sync-

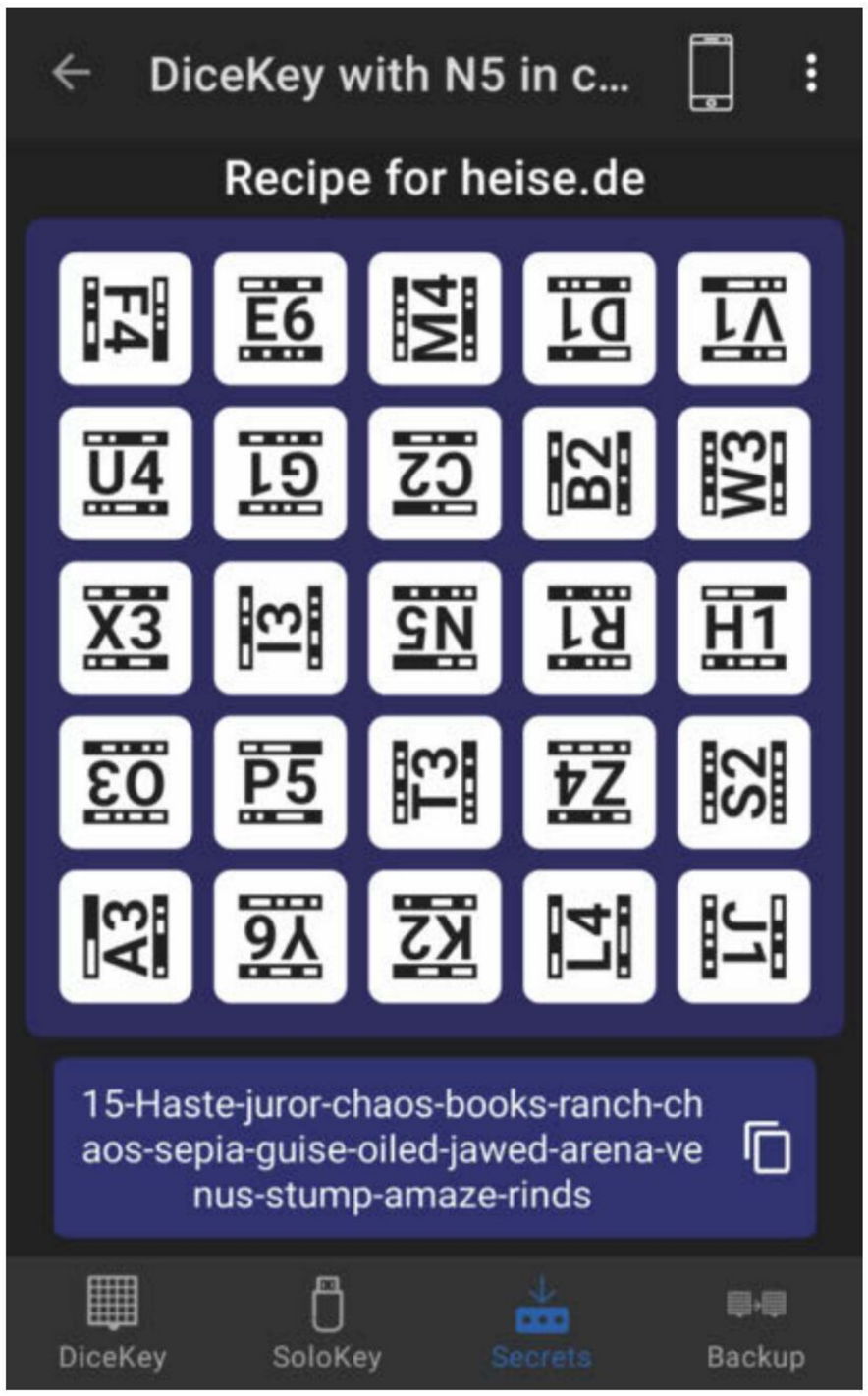
Mechanismus. Will man die DiceKeys mit mehreren Geräten nutzen, kann man sie zwar einfach mehrfach einscannen, die Diensteinträge muss man allerdings wieder von Hand eintippen. Die App gibt es auch für macOS, unter Windows und Linux kann man die DiceKeys über die Web-App https://dicekeys.app/ benutzen. Damit klappt sogar das Einscannen per Webcam tadellos.

Nachdem die Web-App vom Server geladen war, konnten wir keinen weiteren Netzwerkverkehr feststellen, sie wird also lokal im Browser ausgeführt. Wenn Sie neugierig geworden sind, können Sie das DiceKeys-Konzept damit auch ohne den Kauf der Würfel ausprobieren: Klicken Sie einfach auf „Create a Random DiceKey for Testing“, um die virtuellen Würfel fallen zu lassen. Derzeit befindet sich eine Electron-App in der Entwicklung, die lokal auf allen wichtigen Desktop-Betriebssystemen laufen dürfte. Die Apps sind Open Source (MIT-Lizenz), ihr Quellcode ist bei GitHub einsehbar (siehe ct.de/wzht).

Viele Möglichkeiten

Interessant ist auch die Mathematik hinter dem Konzept: Mit den insgesamt 25 unterschiedlichen Würfeln sind etliche Milliarden Kombinationen und damit ausreichend Entropie möglich. Jeder Würfel hat sechs Seiten, die oben liegen können und eine individuelle Position im Raster der Box. Zudem berücksichtigt der Algorithmus die Ausrichtung des Aufdrucks der Würfeloberseite. Laut dem DiceKeys-Erfinder Stuart Schechter entspricht dies einem Kryptoschlüssel mit einer Stärke von 192 Bit, was nach aktuellem Stand der Technik als sicher gilt. Grund, daran zu zweifeln, haben wir nicht: Dem Projekt stand Krypto-Papst Bruce Schneier beratend zur Seite.

Allerdings hat das System eine offensichtliche Schwäche an anderer Stelle: Die gewürfelten Schlüssel sind nicht vor der Vervielfältigung geschützt. Jeder, dem die blaue Box in die Hände fällt, kann den Schlüssel ablesen und ein Foto davon machen. Deshalb sollte man die Würfelbox nach dem Einscannen besser an einem sicheren Ort verwahren, zum Beispiel in einer abgeschlossenen Schreibtischschublade. Dafür sind Back-ups sehr einfach: Entweder schreibt man die Würfelpositionen per Hand auf oder man legt die Würfel in einer zweiten Box identisch zurecht. Hierbei ist die Back-up-Funktion der Smartphone-App behilflich: Sie leitet ihren Nutzer Schritt für Schritt an, wie die Würfel für die Kopie einer bereits gescannten Box zu platzieren sind.



Die DiceKeys-App generiert anhand der Würfel individuelle Passwörter für die verschiedenen Online-Dienste.

Über ein API lassen sich die Würfel prinzipiell auch für andere Projekte nutzen. Ein erstes Beispiel gibt es bereits: Wer einen FIDO2-Sicherheitsschlüssel von SoloKeys sein Eigen nennt, kann mit den DiceKeys das Kryptogeheimnis erwürfeln, das die Grundlage für die FIDO2-Authentifizierung ist. Dieses generiert normalerweise eine geschützte Funktion im Mikrocontroller, anschließend ist es aus Sicherheitsgründen nicht daraus auslesbar. Deshalb ist es nicht möglich, eine Kopie des FIDO2-Schlüssels als Backup anzufertigen. Wer einen zweiten FIDO2-Schlüssel als Ersatz bereithalten möchte – etwa für den Fall, dass

der erste verloren geht – muss also beide Schlüssel mit sämtlichen Online-Diensten verknüpfen. Hier kommen die DiceKeys ins Spiel: Die DiceKeys-App kann das gewürfelte Geheimnis auf mehrere SoloKeys kopieren, wodurch sich diese fortan absolut identisch verhalten und ein verlorener Sicherheitsschlüssel einfach durch eine 1:1-Kopie ersetzt werden kann. Eine solche Kopie kann man auch dann noch erstellen, wenn der ursprüngliche FIDO2-Schlüssel schon längst verloren oder ausgefallen ist.

Fazit

DiceKeys generiert Kryptoschlüssel offline und mit echtem Zufall – eine anschauliche Umsetzung eines Schlüsselgenerators. Die Idee dahinter ist charmant, vom Komfort eines modernen Passwort-Managers mit Auto-Ausfüllen und Sync-Funktion sind die Würfel jedoch weit entfernt. Die langen Passphrasen eignen sich gut als Master-Passwort für einen vollwertigen Passwortmanager.

Aktuell ist das Würfelset nur über die US-Crowdfunding-Plattform Crowd Supply und Mouser erhältlich. Zum Stückpreis von 25 US-Dollar kommen dort Versandkosten von 18 Dollar pro Bestellung hinzu. (rei) ct

DiceKeys

Passwortgenerator	
Hersteller	DiceKeys, LLC (Stuart Schechter)
Systemanf.	Android ab 6, iOS/iPadOS ab 14, macOS ab 11 oder Browser (Web-App)
Lieferumfang	25 Würfel, Aufbewahrungsbox, Transportbeutel
Preis	25 US-$ (zzgl. 18 US-$ Versand)

Apps & Bezugsmöglichkeit

ct.de/wzht

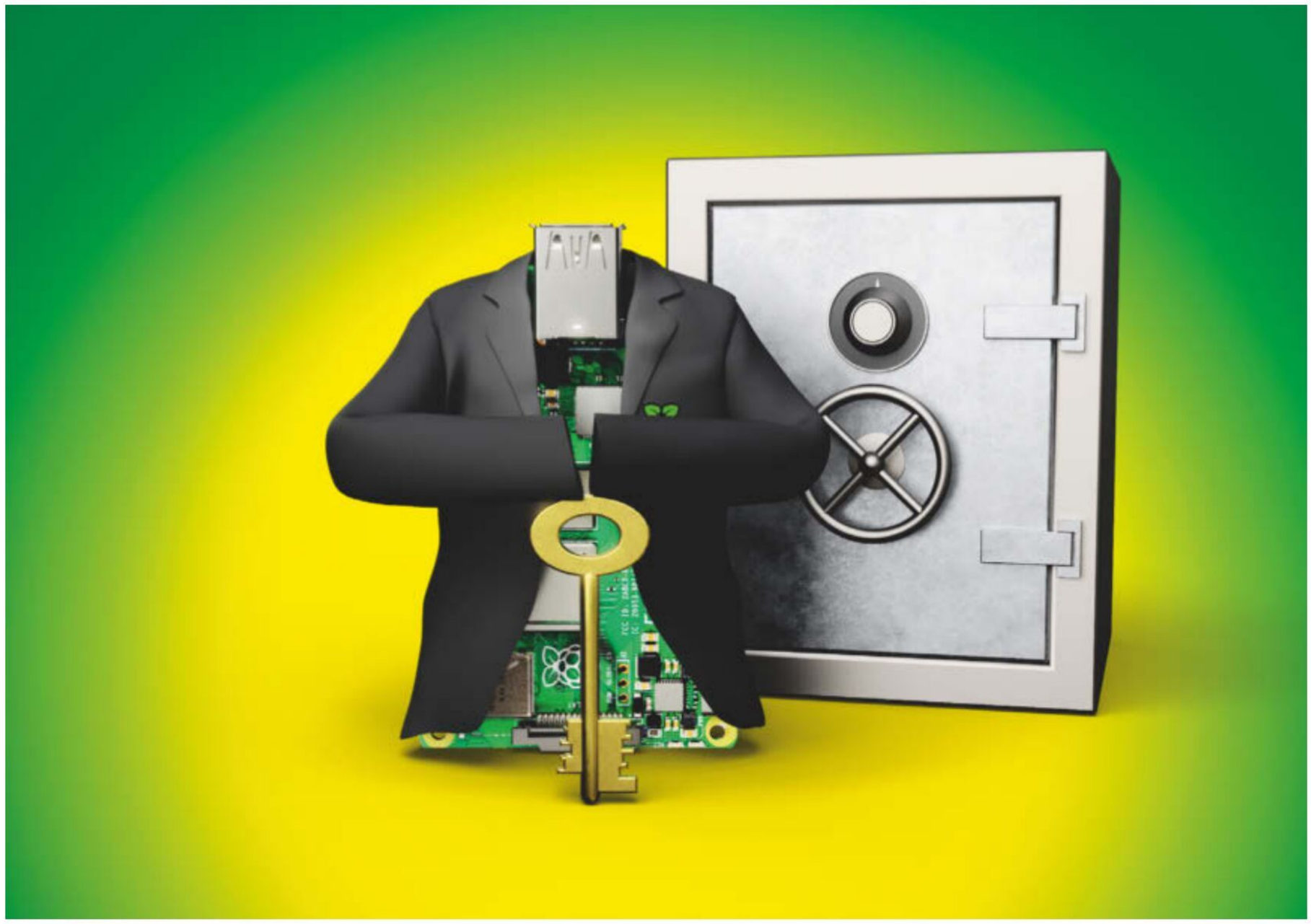


Bild: Andreas Martini

Passwortmanager in Eigenregie hosten

Mit Vaultwarden betreiben Sie Ihren eigenen Passwort-Tresor und -Server. Es synchronisiert Zugangsdaten zwischen mehreren Geräten, ohne Ihre Datenbank in fremde Hände zu geben. Das klappt auf einem (Heim-) Server oder mit dem Raspberry Pi.

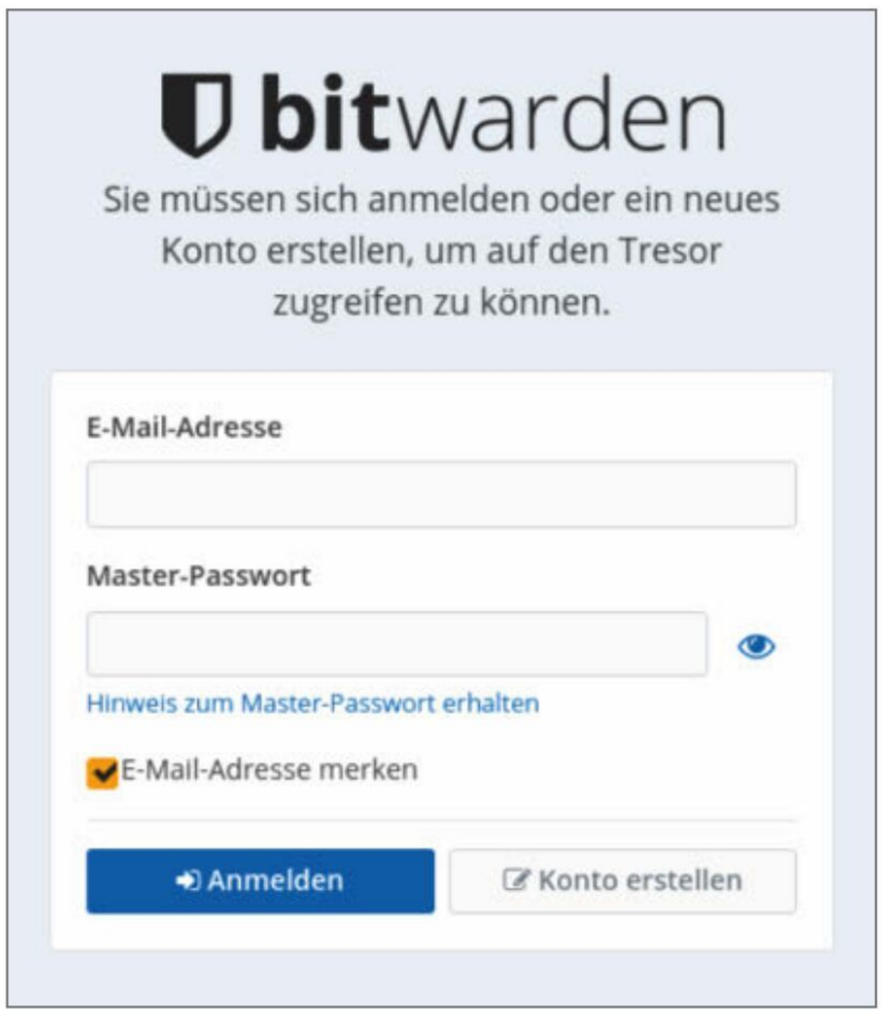
Von **Niklas Dierking**

Ein neues Kundenkonto hier, ein Social-Media-Login da. Bei vielen Internetnutzern türmen sich Zugangsdaten zu Portalen und Diensten zu einem bedrohlichen Haufen auf. Bei jeder Registrierung ein einzigartiges und sicheres Passwort zu überlegen und jedes einzelne zu merken, das ist eine schier unlösbare Aufgabe. Passwortmanager versprechen Abhilfe, aber sie hängen üblicherweise an der Cloud des Anbieters und synchronisieren die Passwortsammlung zwischen mehreren Geräten

nur, wenn man einen monatlichen Obolus zahlt. Außerdem brauchen Nutzer ein hohes Maß an Vertrauen in den Betreiber: Der virtuelle Schlüsselbund liegt immerhin in einem fremden Schließfach.

Den Open-Source-Passwortmanager Bitwarden können Sie in Eigenregie hosten. Bitwarden besteht aus zwei Teilen: dem Server, der Passwörter verwaltet und bereitstellt, und den Clients, die sie abrufen. Das Community-Projekt Vaultwarden hat eine schlankere Variante des offiziellen Bitwarden-Servers geschaffen, die das Bitwarden-API implementiert. Damit kann Ihr (Heim-)Server oder ein Raspberry Pi die Rolle des Passwort-Servers übernehmen, der zu den offiziellen Bitwarden-Anwendungen kompatibel bleibt. Nach der Installation können Sie mit mehreren Accounts über die offiziellen Bitwarden-Clients oder mittels Weboberfläche („Web-Vault“) auf den Server zugreifen. Die Lösung eignet sich damit auch für Familien, Freunde und kleine Teams.

Für Vaultwarden empfiehlt sich eine Docker-fähige Linux-Distribution, beispielsweise Ubuntu 20.04 LTS oder Raspberry Pi OS . Falls Sie den Passwort-Server auf dem Raspi aufsetzen, brauchen dazu mindestens einen Raspberry Pi 3. Ob Sie das System mit grafischer Oberfläche an einem Monitor mit Maus und Tastatur bedienen oder sich mittels SSH von einem anderen Gerät aufschalten, bleibt Ihnen überlassen.



Der Login-Bildschirm der Bitwarden-Weboberfläche („Web-Vault“). Nach der Installation von Vaultwarden genügt beispielsweise ein Browser, um jederzeit Zugriff auf Ihre Passwörter zu haben. Um den Passwortmanager zu benutzen, sind keine Spezialkenntnisse mehr nötig.

Für die Installation braucht es lediglich den Zugriff auf die Kommandozeile. Nach der Einrichtung können Sie Vaultwarden mit einem Web-Browser von einem beliebigen Gerät aus konfigurieren. Die Weboberfläche enthält eine Web-App („Vault“), in der Nutzer ihren Account verwalten, und stellt Werkzeuge zur Administration über ein Admin-Panel bereit. Die Entwickler von Vaultwarden empfehlen, den Server als Docker-Container aufzusetzen. Diese Lösung hat den Vorteil, dass der Passwortmanager anderen Diensten auf dem System nicht in die Quere kommt.

Als Zutaten für eine solche Installation haben sich die folgenden Komponenten bewährt: Ein Reverse-Proxy ist der bequemste Weg, die Weboberfläche und das API verschlüsselt ins Web zu bekommen. Der Proxy nimmt Anfragen entgegen und liefert die Daten über eine HTTPS-Seite aus. In den nachfolgenden Beispielen wird angenommen, dass die TCP-Ports 80 und 443 des Systems nicht bereits belegt sind. Für diesen Zweck eignet sich der containerisierte Edge-Router Traefik, der sich die nötigen TLS-Zertifikate selbst besorgt und diese automatisch erneuert.

Docker-Compose erspart lange `docker run`-Befehle. Die Konfigurationen der Container sind dabei in einer Compose-Datei zusammengefasst, die durch eine .env-Datei mit Umgebungsvariablen ergänzt wird. Beispieldateien stellen wir in einem GitHub-Repository zur Verfügung, das Sie über ct.de/w7gs einsehen können.

Wenn Sie Vaultwarden im Heimnetz betreiben und von außen erreichen wollen, benötigen Sie einen festen Hostnamen, der auf die WAN-IPv4-Adresse des Routers verweist. Hier hilft ein DynDNS-Dienst. Dieser leitet Anfragen, die beim konfigurierten DynDNS-Hostnamen eingehen, an die jeweils aktuelle WAN-IPv4-Adresse des Routers weiter. Eine Anleitung für den kostenlosen DynDNS-Anbieter FreeDNS finden Sie online im Artikel „Mit DDNS auf’s Heimnetzwerk zugreifen“ (ct.de/w7gs). Sie haben die Wahl, welchen DynDNS-Dienst Sie verwenden. In dieser Anleitung dient die Adresse bitwarden.example.com als Beispiel.

Das Betriebssystem vorbereiten

Im ersten Schritt bringen Sie das System auf den neuesten Stand und installieren mit einem Skript die Docker-Engine für die Container-Laufzeitumgebung. Wenn es sich um eine frische Raspberry-Pi-OS-Installation handelt, dann starten Sie das

System nach dem Einspielen der Updates neu, bevor Sie Docker installieren.

```
sudo apt update
sudo apt upgrade
sudo reboot
curl -fsSL https://get.docker.com \
-o get-docker.sh
sudo sh get-docker.sh
```

Falls auf Ihrem System die Apache2-Utilities und das Versionsverwaltungswerkzeug Git nicht vorhanden sind, dann installieren Sie die Pakete ebenfalls.

```
sudo apt install apache2-utils
sudo apt install git
```

Docker-Compose beziehen Sie am besten aus dem Python-Paketmanager „pip“.

```
sudo apt install python3-pip
sudo pip3 install docker-compose
```

Eine Einführung in die Funktionsweise von Docker-Compose finden Sie im Artikel „Container-Komponist“ [1]. Um mit dem Docker-Daemon zu interagieren, brauchen Sie Systemverwalterrechte. Wenn Sie Docker-Befehle ohne vorangestelltes `sudo` verwenden möchten, müssen Sie Ihren Benutzer zur Gruppe „docker“ hinzufügen und sich erneut einloggen.

```
sudo usermod -aG docker user
passwd
```

Die nötige Software ist jetzt installiert und Docker einsatzbereit. Bevor es jedoch an das Einrichten der Container geht, muss sichergestellt werden, dass ihr Server – und damit Weboberfläche sowie API – auch aus dem Internet erreichbar ist. Wenn Sie Vaultwarden auf einem angemieteten Server betreiben wollen, überspringen Sie den nächsten Schritt.

Netzwerkverkehr dirigieren

Damit Anfragen zuverlässig beim Passwort-Server und nicht bei einem anderen Netzwerkgerät landen, sollte eine feste IP-Adresse vergeben werden. Handelt es sich um einen Raspi, dann tragen Sie diese für das aktive Netzwerk-Interface in der Datei /etc/dhcpcd.conf ein. Wenn der Raspi via Ethernet mit dem Netzwerk verbunden ist, dann wählen Sie das Interface eth0 (bei WLAN entsprechend wlan0). Passen Sie in der Datei die folgenden vier Zeilen an Ihr lokales Netzwerk an, etwa so:

```
interface eth0
static ip_address=192.168.0.184/24
static routers=192.168.0.1
static domain_name_servers=192.168.0.1
```

Starten Sie das Systen mit `sudo reboot` im Anschluss neu, damit die Änderungen wirksam werden. Richten Sie nun im Web-Interface Ihres Routers eine Portfreigabe (Port-Forwarding) ein. Anfragen von außen, die an TCP-Port 80 oder 443 eingehen, sollen an den Server durchgereicht werden und beim Reverse-Proxy Traefik landen. Als Protokoll wählen Sie TCP und tragen Port 80 ein. Der Name, der für den Dienst vergeben wird, ist beliebig. Den gleichen Vorgang wiederholen Sie für den Port 443.

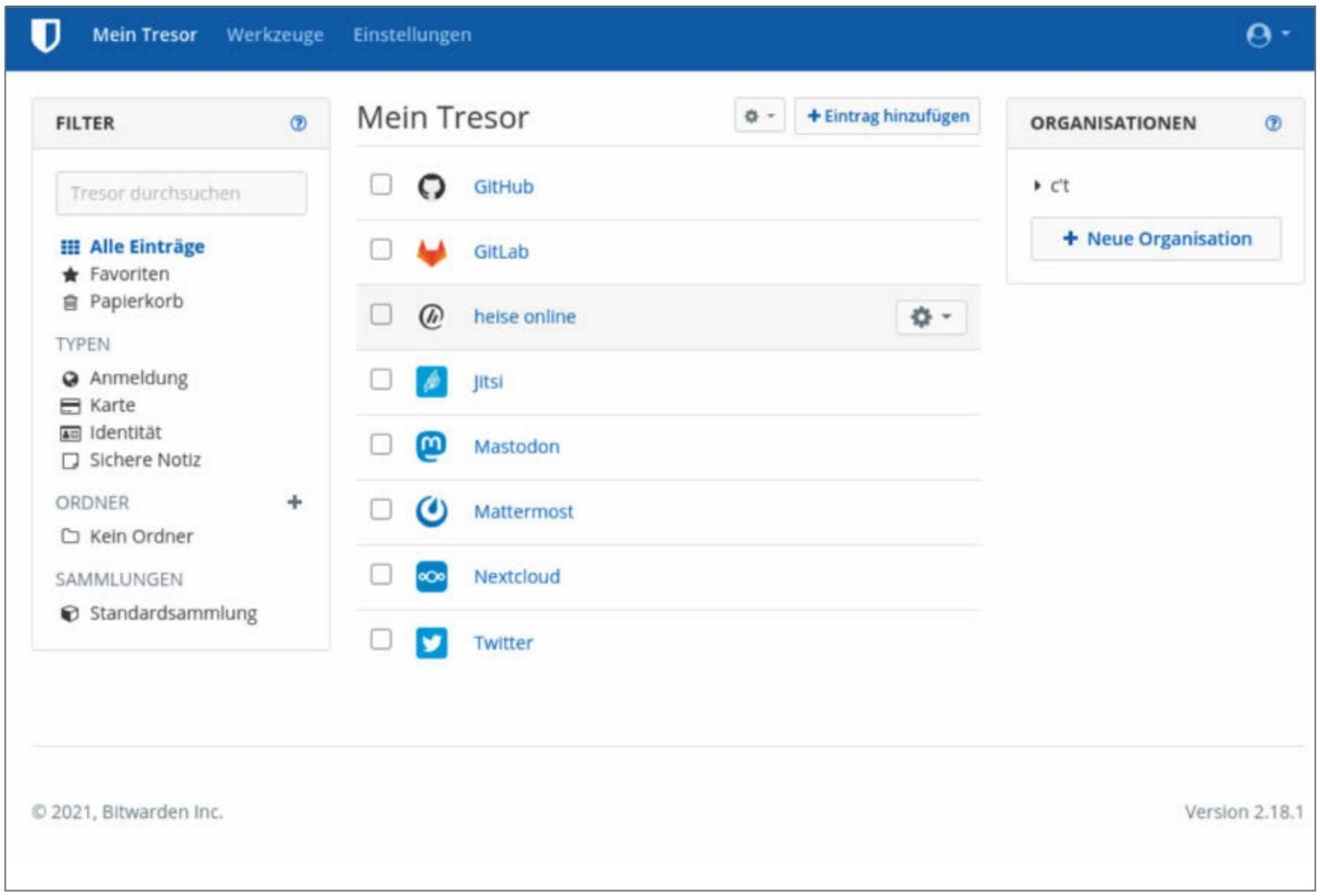
Damit der DynDNS-Dienst Ihrer Wahl in der Lage ist, auf die aktuelle WAN-IPv4-Adresse des Routers zu verweisen, benötigt er einen Gegenpart, der ihn mit dieser Information versorgt. Diese Aufgabe können die meisten modernen Router übernehmen. Die Konfiguration erledigen Sie ebenfalls im Webinterface des Routers. Wählen Sie im entsprechenden Menü den Anbieter aus und tragen Sie die abgefragten Daten, meist Login-Informationen und eine Update-URL, in die Maske ein. Wird Ihr DynDNS-Anbieter nicht gelistet, dann setzen Sie einen benutzerdefinierten Eintrag.

Transportverschlüsselung dank Traefik

Nach diesen Vorbereitungen geht es nun an die Container-Architektur. Als Speicherort für Container-Konfigurationen und Compose-Files auf dem Linux-Dateisystem hat sich das Verzeichnis /srv bewährt. Wenn Sie dort Dateien (be)schreiben wollen, müssen Sie mit `sudo` arbeiten oder sich Systemverwalterrechte einräumen. Klonen Sie das GitHub-Repository nach /srv und wechseln Sie danach in den Ordner.

```
sudo git clone \
https://github.com/ndi-ct/raspi-pwm \
/srv/raspi-pwm
cd /srv/raspi-pwm
```

Als Container-Blaupause steht im heruntergeladenen Repository eine YAML-Datei bereit. Die schreibt



Willkommen im Vault: In der Web-App können Sie Ihre Passwörter verwalten und Einstellungen vornehmen, beispielsweise Zwei-Faktor-Authentifizierung aktivieren.

fest, welche Container-Images aus dem Docker Hub geladen werden und wie diese konfiguriert sind. Umgebungsvariablen sind in die zugehörige .env-Datei ausgelagert. Diese wird standardmäßig nicht angezeigt. Bei Bedarf verschaffen Sie sich mit `ls -a` einen Überblick. Der Reverse-Proxy benötigt darüber hinaus noch die Dateien traefik.toml und dynamic.yml, die Anweisungen zur Beschaffung von Zertifikaten und zur Regelung des Netzwerkverkehrs geben. Diese finden Sie im Ordner config-files.

Öffnen Sie traefik.toml mit dem Texteditor Ihrer Wahl und tragen Sie in der Zeile `email = "mail@example.com"` eine gültige Mail-Adresse ein (die Anführungszeichen bleiben bestehen). An diese Adresse sendet Let's Encrypt Warnungen, falls es Probleme mit dem erteilten Zertifikat gibt. Traefik legt die Zertifikate, die es automatisiert mittels ACME-Protokoll besorgt, in der Datei acme.json ab. Diese darf nur für Root lesbar sein. Erstellen Sie im Ordner config-files eine leere Datei mit dem Namen acme.json und passen Sie die Rechte an.

```
sudo touch acme.json
sudo chmod 600 acme.json
```

Danach legen Sie ein virtuelles Netzwerk für den Reverse-Proxy an.

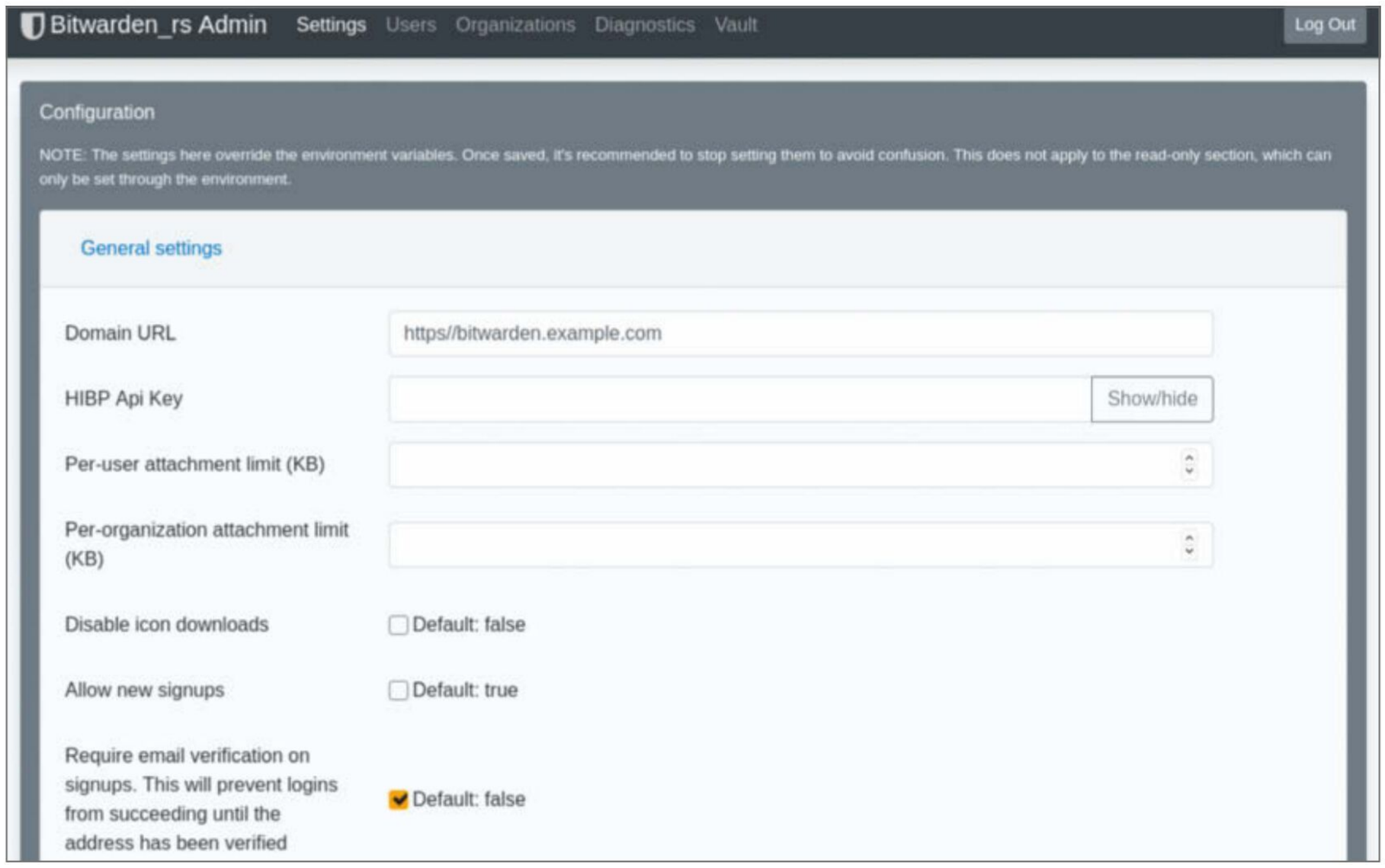
```
sudo docker network create \
traefik_reverse_proxy
```

Tresor aufstellen

Wechseln Sie jetzt in das Verzeichnis /srv/raspi-pwm. Um sich einen Überblick über den Container-Aufbau zu verschaffen, können Sie sich den Inhalt des Compose-File ausgeben lassen:

```
cat docker-compose.yaml
```

Die Images „vaultwarden/server“ und „traefik“ sind mit Versionsnummern versehen, um Ihnen unschöne Überraschungen zu ersparen. Ohne dieses Tag



Das Admin-Panel ist die Schaltzentrale von Vaultwarden. Hier haben Sie Zugriff auf wichtige Einstellungen und können die Nutzer verwalten.

lädt Docker stets das neueste Image vom Docker Hub herunter. Das kann dazu führen, dass der Container plötzlich nicht mehr startet, weil die neue Version Änderungen an den Konfigurationsdateien erfordert. Prüfen Sie regelmäßig, ob für Ihre Images (Sicherheits-)Updates vorliegen. Wenn das der Fall ist, dann ersetzen Sie das ausgediente Image durch ein neueres. Die verwendeten Images haben wir unter ct.de/w7gs verlinkt.

Der Parameter `restart: unless-stopped` sorgt dafür, dass die Container auch nach einem Neustart des Raspi wieder anlaufen, es sei denn, Sie haben zuvor einen Container manuell gestoppt. Der `volumes`-Abschnitt legt fest, wo der Bitwarden-Container persistente Daten speichert:

```
volumes:
  - /var/docker/bitwarden:/data
```

Das Verzeichnis /data im Container-Dateisystem entspricht /var/docker/bitwarden im Host-Dateisystem. Hier liegt auch die SQLite-Datenbankdatei db.sqlite3. Sie sollten das Verzeichnis /var/docker/bitwarden regelmäßig sichern.

Im Compose-File finden Sie die Variablen `${BITWARDEN_URL}`, `${WEBSOCKET_ENABLED}` und `${ADMIN_TOKEN}`. Die Werte holt Docker-Compose sich aus der .env-Datei. Öffnen Sie die Datei mit einem Texteditor.

```
BITWARDEN_URL=bitwarden.example.com
WEBSOCKET_ENABLED=true
ADMIN_TOKEN=
```

Tragen Sie hinter `BITWARDEN_URL=` Ihre DynDNS-Adresse ein. Die Adresse wird als Host an Traefik übergeben. Der Eintrag `WEBSOCKET_ENABLED=true` sorgt dafür, dass Passwörter und andere Einträge im Vault bei jeder Änderung synchronisiert werden, sofern der entsprechende Client dies unterstützt („Live-Sync“). Wir empfehlen, Vaultwarden über den Admin-Bereich der Weboberfläche zu konfigurieren. Zum Aktivieren des Admin-Panel setzen Sie hinter `ADMIN_TOKEN=` ein Token ein. Erzeugen Sie dazu auf der Kommandozeile einen langen String mit folgendem Befehl.

```
openssl rand -base64 48 | tr -d /=
```

Mit dem eingetragenen Token können Sie sich später im Admin-Panel der Weboberfläche authentifizieren. Es steht Ihnen frei, die Einstellungen, die das Admin-Panel bietet, manuell vorzunehmen, indem Sie in der .env-Datei weitere Umgebungsvariablen setzen und diese in der Datei docker-compose.yaml referenzieren. Die Entwickler von Vaultwarden stellen im GitHub-Wiki des Projektes eine umfangreiche Beispieldatei zur Verfügung, die Sie über ct.de/w7gs finden. Löschen Sie in diesem Fall die Zeile `ADMIN_TOKEN=` in der .env-Datei und die zugehörige Referenz aus dem Compose-File.

In unserem Beispiel haben wir das Admin-Panel zusätzlich mit einer Basisauthentifizierung, bestehend aus Username und Passwort, abgesichert. Dazu dient eine Middleware des Reverse-Proxy Traefik, die bereits in der Compose-Datei angelegt ist. Wer im Browser bitwarden.example.com/admin ansteuert, muss zunächst die Login-Daten eingeben, um die Seite zu sehen und kann sich erst im zweiten Schritt mit dem Token als Admin authentifizieren. Die nötigen Zugangsdaten erzeugen Sie mit folgendem Befehl:

```
htpasswd -nb user password\
 | sed -e s/\\$/\\$\\$/g
```

Dieser Befehl erzeugt das Zugangsdaten-Paar „user:password“, wobei „password“ als Hash ausgegeben wird. Ersetzen Sie „user“ und „password“ durch sichere Zugangsdaten. Öffnen Sie dann die Datei docker-compose.yaml mit einem Texteditor und ersetzen Sie in der folgenden Zeile „user:password“ durch die Ausgabe des Befehls.

```
- "traefik.http.middlewares.admin-auth.basicauth.
users=user:password"
```

Speichern Sie im Anschluss die Datei docker-compose.yaml und starten Sie die beiden Container:

```
sudo docker-compose up -d
```

Docker lädt nun zunächst die Images aus der Container-Registry. Der Reverse-Proxy kümmert sich um das Zertifikat von Let‘s Encrypt und liefert Web-Vault und Admin-Panel von Vaultwarden über die konfigurierte DynDNS-Adresse aus. Geben Sie den Containern dabei etwas Zeit zum Starten. Auf einem Raspberry Pi 4 mit 4 GByte Arbeitsspeicher nimmt der erste Startvorgang einige Minuten in Anspruch.

Den Status der Container können Sie mit dem Befehl `docker ps` einsehen. Sobald der Vaultwarden-Container den Status „up x minutes (healthy)“ ausgibt, können Sie das Web-Vault in einem Browser unter der Adresse bitwarden.example.com aufrufen. Für das Admin-Panel hängen Sie /admin an die URL an. Sollte Ihnen irgendwo ein Fehler unterlaufen sein, dann hilft der Befehl `docker logs` gefolgt vom Namen des Containers bei der Diagnose.

Tresortür abschließen

Registrieren Sie einen neuen Nutzer und vergeben Sie dabei ein sicheres Master-Passwort. Jetzt können Sie sich in das Web-Vault einloggen und Ihr Nutzerkonto einrichten. Wer zuvor einen anderen Passwortmanager genutzt hat, findet sich hier schnell zurecht. Die Kategorie „Mein Tresor“ listet Einträge wie gespeicherte Anmeldedaten und sichere Notizen auf. Diese können Sie als Favoriten markieren oder in Ordner sortieren. In „Werkzeuge“ finden Sie einen Passwortgenerator, Berichte über schwache oder kompromittierte Passwörter und die Funktionen zum Importieren und Exportieren von Passwort-Sammlungen. Bitwarden beherrscht die meisten geläufigen Formate (.csv, .json, .xml, .txt). Hier können Sie auch die eigene Passwortdatenbank exportieren. Wählen Sie dabei vorzugsweise das Format „.json (encrypted)“, sonst exportiert Bitwarden die Zugangsdaten im Klartext.

Sie sollten für den Login unbedingt einen zweiten Faktor verlangen. Andernfalls könnte es Angreifern potenziell gelingen, sich mit Brute-Force-Angriffen Zugriff auf Ihre Passwortdatenbank zu verschaffen. Die nötigen Handgriffe nehmen Sie in den Einstellungen im Untermenü „Zwei-Faktor-Authentifizierung“ vor. Der Passwortmanager bietet Zwei-Faktor-Authentifizierung mittels 2FA-Apps wie Authy, Duo oder Microsoft Authenticator, via E-Mail und mit FIDO-kompatiblen Hardware-Sicherheitsschlüsseln an.

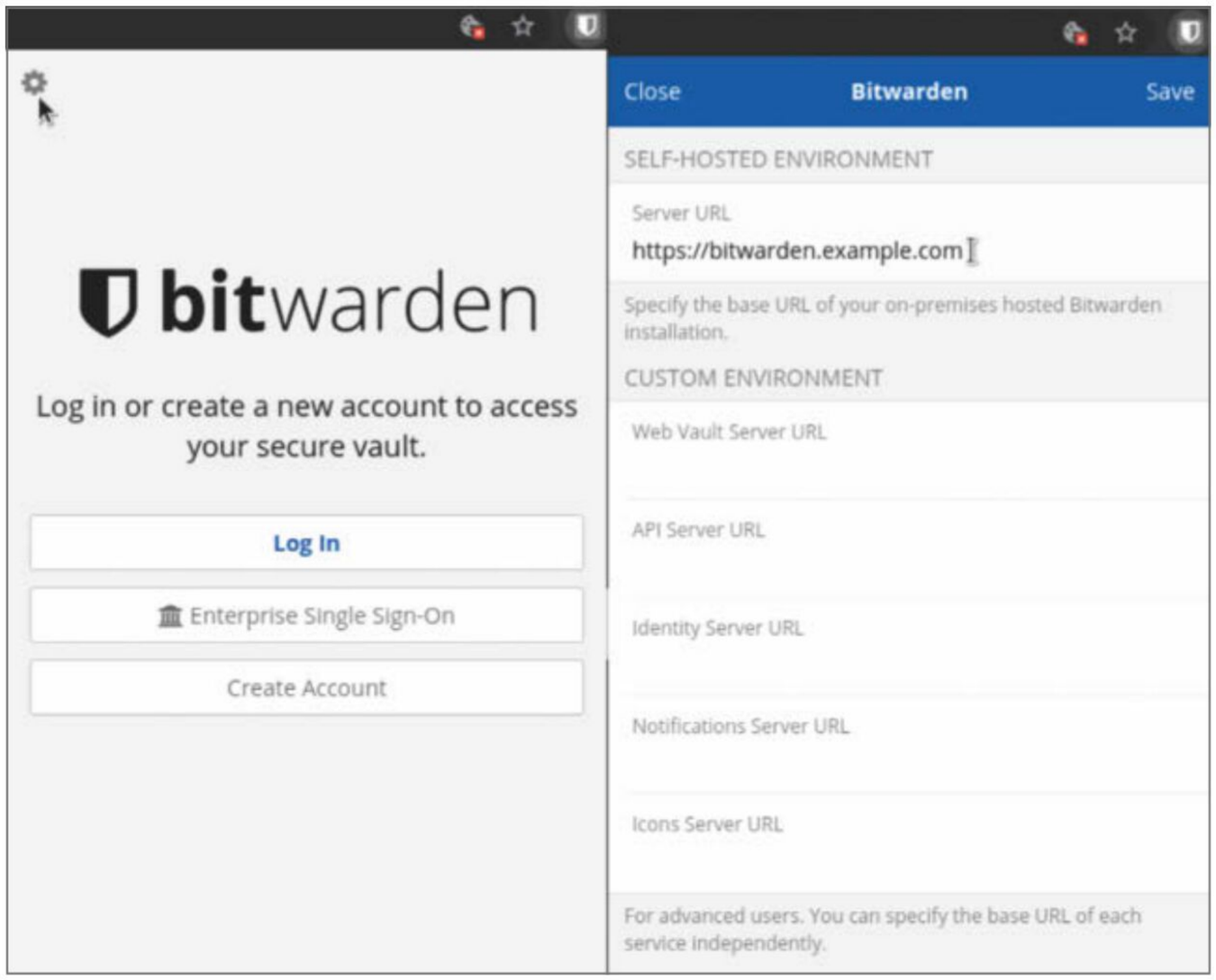
Sobald ein zweiter Faktor eingerichtet ist, können Sie im Menü „Zwei-Faktor-Authentifizierung“ einen Wiederherstellungsschlüssel anzeigen lassen. Falls Sie beispielsweise Ihr Mobiltelefon und damit Zugriff auf den zweiten Faktor verlieren, ist der Wiederherstellungsschlüssel die letzte Möglichkeit, erneut Zugang zum Vault zu bekommen. Notieren Sie den Schlüssel und verwahren Sie ihn an einem sicheren Ort. Tritt das Szenario ein, dann rufen Sie im Browser die Adresse bitwarden.example.com/#/recover-2fa/ auf und folgen Sie den Anweisungen. Wenn Sie direkt mehrere Methoden zur Zwei-Faktor-Authentifi-

zierung einrichten, dann kommen Sie erst gar nicht in diese Situation.

Aktuell kann noch jede Person, die die URL Ihrer Web-Vault kennt, ein Konto anlegen. Wer also keinen Gratis-Passwortmanager ins Internet hängen möchte, tut gut daran, neue Registrierungen zu deaktivieren. Rufen Sie das Admin-Panel im Browser unter der Adresse bitwarden.example.com/admin auf. Wir empfehlen, im Admin-Panel einige Einstellungen vorzunehmen, um die Angriffsfläche Ihres Passwort-Servers zu verringern.

Im Bereich „General“ müssen Sie den korrekten Wert im Feld „Domain URL“ eintragen, damit automatisch versandte Mails die richtigen Links enthalten. Verbieten Sie Registrierungen auf der Hauptseite, indem Sie den Haken beim Eintrag „Allow new signups“ entfernen. Die Schaltfläche und das Eingabeformular zum Registrieren bleiben zwar weiterhin sichtbar, Registrierungen sind aber nicht mehr möglich. Im Bereich „SMTP Email Settings“ sollten Sie einen SMTP-Postausgangsserver konfigurieren, damit der Passwort-Server Mails verschicken kann, etwa, um Accounts zu verifizieren oder zu informieren, falls eine Anmeldung in Ihrem Account von einem zuvor unbekannten Gerät erfolgt ist. Im Admin-Panel können Sie auch dann weitere Nutzer via Mail einladen, wenn die Registrierung auf der Hauptseite deaktiviert ist. Teilen Sie den Passwort-Server beispielsweise mit Freunden, sollten Sie darüber nachdenken, ihnen zu verbieten, weitere Nutzer einzuladen. Dazu entfernen Sie den Haken bei „Allow Invitations“ im Bereich „General“.

Wem das nicht genügt, der deaktiviert das Web-Vault mit der Umgebungsvariable WEB_VAULT_ENABLED=false oder betreibt Vaultwarden ausschließlich im Heimnetz mit selbsterzeugten Zertifikaten. Um dann trotzdem von unterwegs auf den Passwort-Server zuzugreifen, müssten Sie sich mit einer VPN-Lösung behelfen. Die Entwickler raten davon ab, die integrierte Methode ROCKET_TLS für HTTPS zu nutzen. Stattdessen empfehlen sie, private Instanzen mit dem Reverse-Proxy Caddy und Let's-Encrypt-Zertifikaten abzusichern. Eine Anleitung für das nicht ganz triviale Verfahren steht auf GitHub im Wiki des Projekts zur Verfügung, das wir unter ct.de/w7gs verlinkt haben.



Bitwarden-Clients existieren für diverse Plattformen, hier sehen Sie das Browser-Add-On in Chromium. Damit der Client den Passwort-Server ansteuern kann, braucht er die Server-URL.

Den Passwortmanager nutzen

Der Passwort-Server ist jetzt einsatzbereit. Vaultwarden bietet viele Features, die für gewöhnlich einen Bitwarden-Premium-Account voraussetzen. Einige Funktionen fehlen jedoch, etwa Push-Benachrichtigungen in iOS und Android, Single-Sign-On oder Notfall-Vollmachten (Emergency Access). Welche Unterschiede zum offiziellen Bitwarden-Server bestehen, haben die Entwickler im Wiki des Projekts in einer Liste festgehalten, die Sie in der Linksammlung unter ct.de/w7gs abrufen können.

Sie können zum Speichern, Verwalten und Synchronisieren von Passwörten neben dem Web-Vault auch die Bitwarden-Browser-Erweiterungen sowie die Apps für Android und iOS nutzen. Auch Desktop-Clients für Windows, Linux, macOS und sogar Tools für die Kommandozeile sind verfügbar. Eine vollständige Liste aller Clients finden Sie auf der offiziellen Bitwarden-Website, die wir unter ct.de/w7gs verlinkt haben. Damit die Anwendungen mit der Server-API kommunizieren können, müssen Sie die URL Ihrer Vaultwarden-Instanz eintragen. Das zuständige Menü verbirgt sich hinter dem Zahnrad in der linken oberen Ecke des Anmeldefensters.

Doch Vorsicht: Die Schaltfläche „abmelden“ in den Clients ist irreführend und bedeutet „vom Server abmelden“. Wenn Sie sich vollständig abmelden und die Server-API nicht erreichbar ist, dann verweigert der Bitwarden-Client einen neuen Login. Um sich dann erneut anzumelden, muss eine Verbindung zum Server bestehen. Wählen Sie darum stets die Option „Jetzt sperren“, um Ihr Nutzerkonto zu sperren, es sei denn, Sie beabsichtigen, das Nutzerkonto zu wechseln oder den Client an einem anderen Server anzumelden.

Sie können jetzt loslegen und den Passwort-Tresor befüllen. Wenn Sie zukünftig im Web eine Login-Seite ansteuern und Anmeldedaten eingeben, bietet beispielsweise die Bitwarden-Browsererweiterung an, die Login-Daten im Vault zu speichern. Für neue Logins kann der integrierte Passwortgenerator zufällige, sichere Passwörter erzeugen. Falls bereits Anmeldedaten im Vault gespeichert sind, kann Bitwarden Login-Formulare automatisch ausfüllen. Das Auto-Fill-Verhalten können Sie für einzelne Seiten an ihre Vorstellungen anpassen. Gespeicherte Passwörter werden von nun an automatisch synchronisiert.

Fazit

Mit Vaultwarden verwandeln Sie ihr System im Handumdrehen in einen Passwortspeicher mit Cloud-Funktionalität, müssen dafür jedoch Ihre Passwortsammlung nicht aus der Hand geben. Mit dem Zugewinn an Freiheit kommt allerdings auch Verantwortung: Nehmen Sie regelmäßig Backups vor und prüfen Sie die Container-Images auf Sicherheitsupdates. Richtig angewendet ersetzt Vaultwarden einen kostenpflichtigen Passwortmanager und eignet sich optimal für die Nutzung in kleinen Teams oder gemeinsam mit Freunden oder der Familie. (ndi) c't

Literatur

[1] Jan Mahn, **Container-Komponist**, Docker-Container mit Docker-Compose einrichten, c't 26/2018 S. 148

Linksammlung zum Projekt

ct.de/w7gs

Es gibt 10 Arten von Menschen. iX-Leser und die anderen.

Jetzt Mini-Abo testen:
3 Hefte + Bluetooth-Tastatur nur 16,50 €
www.iX.de/testen

www.iX.de/testen 49 (0)541 800 09 120 leserservice@heise.de
MAGAZIN FÜR PROFESSIONELLE INFORMATIONSTECHNIK

Schutz oder trügerische Sicherheit?

VPN-Anbieter versprechen, die übertragenen Daten stets zu verschlüsseln, geografische Sperren aufzuheben und Anonymität herzustellen. Doch auch wenn die Technik selbst über jeden Zweifel erhaben ist, hat sie ihre Tücken. Man sollte sich schon deshalb nicht blind einem Anbieter anvertrauen.

Von **Peter Siering**

Bild: Andreas Martini

Vor- und Nachteile der Technik	84
Elf VPN-Anbieter im Vergleich	90
Übersicht gängiger VPN-Varianten	98

Sie haben sicher auch schon davon gehört, dass es ganz einfach sei, gesperrte Serien oder Sportereignisse in einem Streamingportal über ein VPN anzusehen. Sie sind bestimmt schon davor gewarnt worden, offene WLANs ohne VPN zu verwenden, weil Ihre Daten dann leicht abhörbar durch den Äther fliegen. Sie haben vielleicht auch mal darüber nachgedacht, anonym ins Internet zu gehen, um sich die dunkle Seite der Macht anzusehen, und haben dazu VPN-Anbieter empfohlen bekommen. Doch ist das immer eine gute Wahl und welcher Anbieter ist seriös?

Anvertrauen

Virtual Private Network (VPN) als Technik baut verschlüsselte Tunnel zwischen Netzwerken auf. Ursprünglich diente das vor allem dazu, Netze über unsichere Verbindungen zu koppeln und mobile Nutzer (Road Warriors) sicher ins Firmennetzwerk zu holen. Beim Firmeneinsatz ist das Verhältnis eindeutig: Der Firmenadmin, der dazu die Zugangsdaten oder Schlüssel ausgibt, wird zumeist vertraglich vom Arbeitgeber zu Vertraulichkeit verpflichtet. VPN-Anbieter hingegen erlegen sich solche Pflichten selbst auf. Kunden sollten deswegen wissen, dass die Anbieter stets alle Schlüssel kennen, um Klartext mitzulesen.

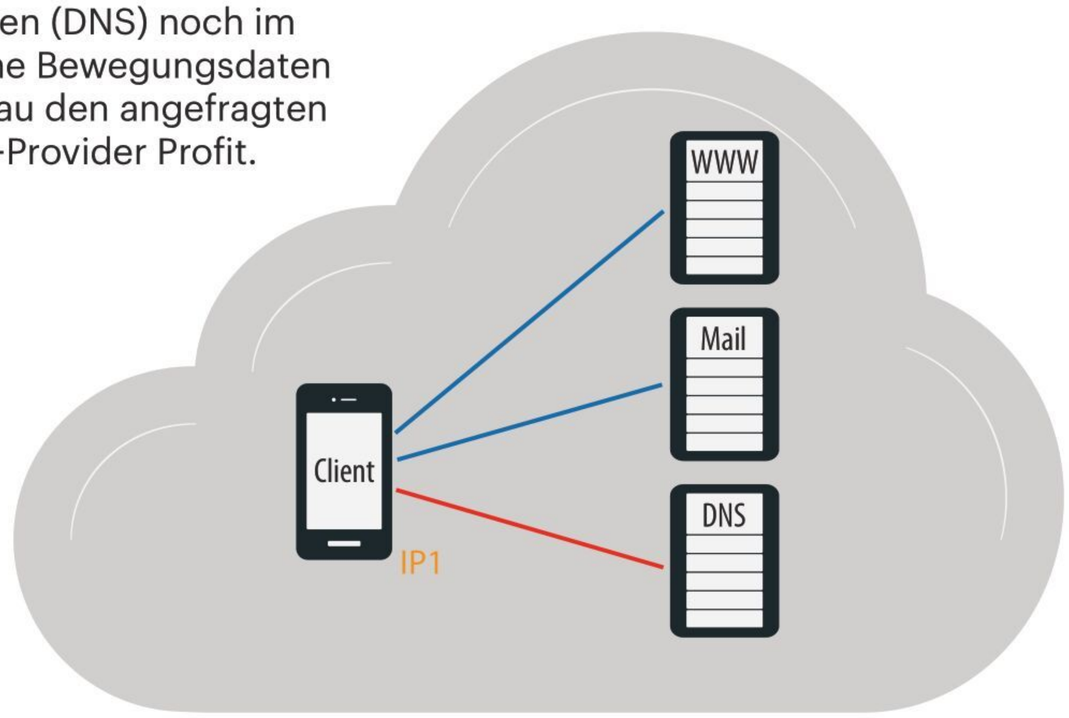
Dass das keine theoretische Möglichkeit ist, sondern in der Praxis ausgeschöpft wird, um aus den Nutzungsdaten Profit zu schlagen, ist kein Geheimnis: Bei VPN-Anbietern, die ihre Dienste kostenlos anbieten, besteht darin oft das Geschäftsmodell. Sie machen daraus nicht mal einen Hehl, sondern gestehen das in Geschäftsbedingungen und Datenschutzerklärung ein. Aber nicht jeder: Facebook kaufte 2013 den Dienst Onavo mit seinem VPN-Angebot und nutzte ihn heimlich zum Sammeln von Nutzerdaten. 2019 verschwand das Angebot.

Doch nicht nur mit den Daten wird getrickst. Es tauchen immer mal wieder auch Anbieter auf, die VPN kreativ interpretieren. 2015 machte die Runde, dass der Anbieter Hola die Internet-Anschlüsse der Kunden seines Gratisangebots benutzt, um dort den Datenverkehr anderer Kunden auszuleiten. Das klingt auf den ersten Blick elegant, aber hat rechtliche Implikationen. Wenn nämlich ein anderer VPN-Nutzer Urheberrechtsverletzungen begeht, könnten sich die auf den Plan gerufenen Anwälte an den nichts ahnenden Anschlusseigner halten. In der FAQ weist

Ohne VPN mit TLS

Wenn heute ein PC oder ein Smartphone Internet-Dienste anspricht, geschieht das in der Regel verschlüsselt. Die globale IP-Adresse des Clients ist den angesprochenen Servern bekannt. Web- und E-Mail-Server lassen sich heute nicht mehr auf Klartextverbindungen ein. Häufig aber laufen Namensanfragen (DNS) noch im Klartext durchs Netz. So entstehen schon recht umfangreiche Bewegungsdaten eines Surfers. Obendrein verpetzt der TLS-Verbindungsaufbau den angefragten Hostnamen (SNI). Aus solchen Daten schlagen dubiose VPN-Provider Profit.

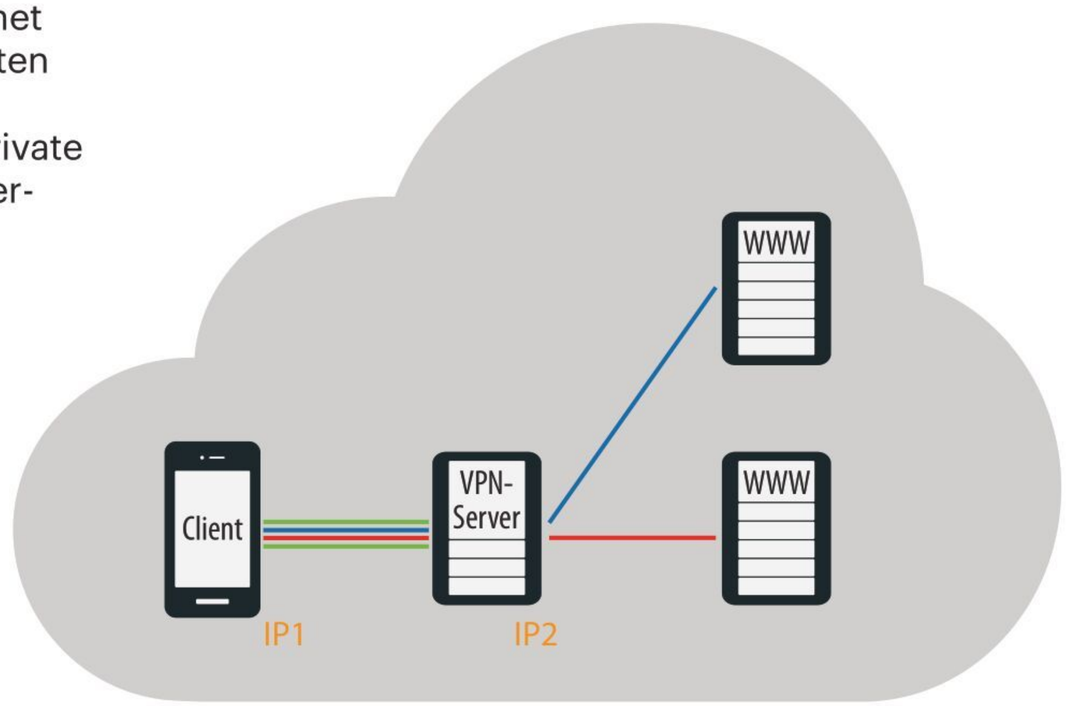
IPX unterschiedliche, globale IP
— verschlüsselte Verbindung (TLS)
— unverschlüsselte Verbindung



Mit VPN

Ein VPN-Tunnel verschlüsselt alle darin transportierten Daten. Aber der Tunnel führt letztlich nur von einer Stelle im Internet zu einer anderen. Hinter dem VPN-Server reisen Klartextdaten lesbar weiter. Die angesprochenen Server erfahren nur die IP-Adresse des VPN-Servers. Viele Schaubilder zu Virtual Private Networks tun so, als würde ein Client erst durch die VPN-Verbindung Zugriff aufs Internet erhalten, aber das ist falsch: Der Client benutzt seinen Internet-Zugang ja schließlich, um auf den VPN-Server zuzugreifen.

IPX unterschiedliche, globale IP
verschlüsselte Verbindung (TLS)
verschlüsselte Verbindung (VPN-Tunnel)
unverschlüsselte Verbindung



Hola auf die Technik hin, ohne aber vor möglichen Gefahren zu warnen. Zahlende Kunden sollen nicht betroffen sein.

Misstrauen

Wer vorschnell zu einem VPN-Angebot greift, läuft also Gefahr, über den Tisch gezogen zu werden. Besonders gilt das, wenn man sich an einer der vielen im Internet zugänglichen Bestenlisten orientiert. Viele dieser Sites leben vom Affiliate-Geschäft, also von Provisionen, die der Betreiber erhält, wenn ein Besucher direkt per Link in den Shop des VPN-Providers hüpft. Der eine oder andere VPN-Provider wirbt unterdessen damit, dass er sich an diesem Zirkus nicht beteiligt. All das sind Indizien, die bei der Wahl eines geeigneten VPN-Providers helfen können. Wir haben uns elf VPN-Provider genauer angesehen und stellen deren Angebote ab Seite 90 im Detail vor.

Alle, die gern tüfteln, können auch einen eigenen VPN-Dienst aufsetzen: Dazu braucht man entweder einen Router, der das schon von sich aus beherrscht, oder einen dauerhaft laufenden Computer wie einen Raspi. Ihr VPN-Tunnel überbrückt dann fremde Netze, etwa unverschlüsselte WLANs im Hotel, bis zu Ihrem Heimnetzwerk. Erst dort wird der verschlüsselte Verkehr entpackt und gelangt über den dortigen Anschluss ins Internet. Dadurch entstehen keine Kosten und Sie müssen sich nicht Dritten anvertrauen. Hilfestellung in Form von c't-Artikeln finden Sie unter ct.de/wrqr.

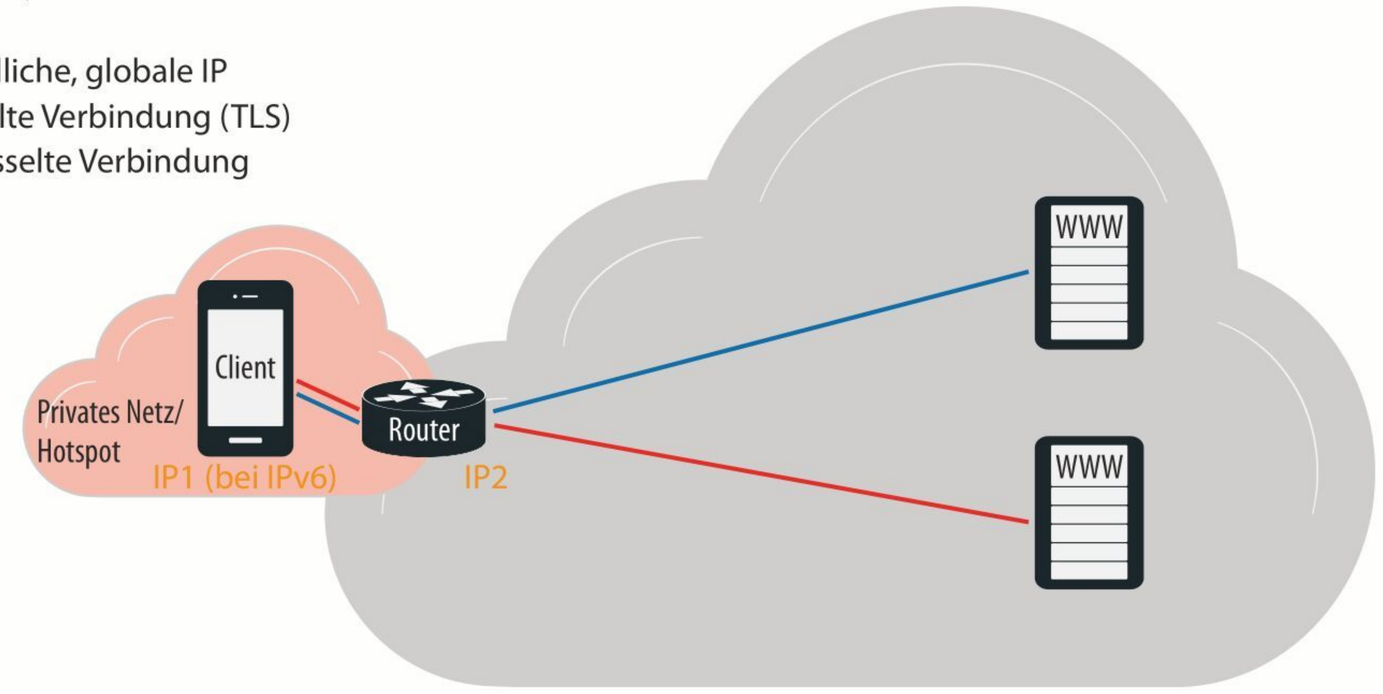
Für all diejenigen, die schon dem eigenen Internet-Provider misstrauen, ist das keine Lösung. Wenn Sie Ihre Aktivitäten hinter den IP-Adressen eines VPN-Providers verstecken wollen, dann müssen Sie sich eben solchen Angeboten anvertrauen. Oft aber ist der Gewinn, den sich Kunden dadurch versprechen, ein Irrtum: Die IP-Adresse, mit der Sie sich im Internet bewegen, lässt vor allem dann Rückschlüsse auf Sie zu, wenn es hart auf hart kommt und sich jemand mit juristisch berechtigtem Interesse bemüht, Ihre Identität ermitteln zu lassen. Internet-Provider geben Ihre Daten dann heraus. VPN-Provider behaupten, das nicht zu tun.

Für die Betreiber von Websites und anderen Diensten ist eine IP-Adresse nicht so sehr viel wert. Zum einen verbergen sich hinter einer Adresse oft viele Nutzer, zum anderen wechselt sie häufig. Bei IPv6 sorgen die Privacy Extensions dafür, dass Windows alle 12 Stunden die Adresse ändert. So haben die Anbieter längst bessere und perfidere Methoden

Eigene IP ohne VPN verstecken

Offene WLAN-Hotspots, viele Mobilfunkprovider oder andere große Netzwerke, die Clients eine private IP-Adresse verpassen, erreichen einen ähnlichen Effekt wie ein VPN-Server: Ein aufs Internet zugreifender Client versteckt sich in der Masse der anderen Clients hinter der öffentlichen IP-Adresse dieses Netzes. Wie detailliert der Betreiber protokolliert und ob er einen konkreten Nutzer zu fassen bekommt, dazu gibt es meist keine Auskunft. VPN-Provider versprechen, das nicht zu tun. Im Fall globaler IPv6-Adressen, wie sie Mobilfunkprovider heute vergeben, funktioniert das Verstecken nicht.

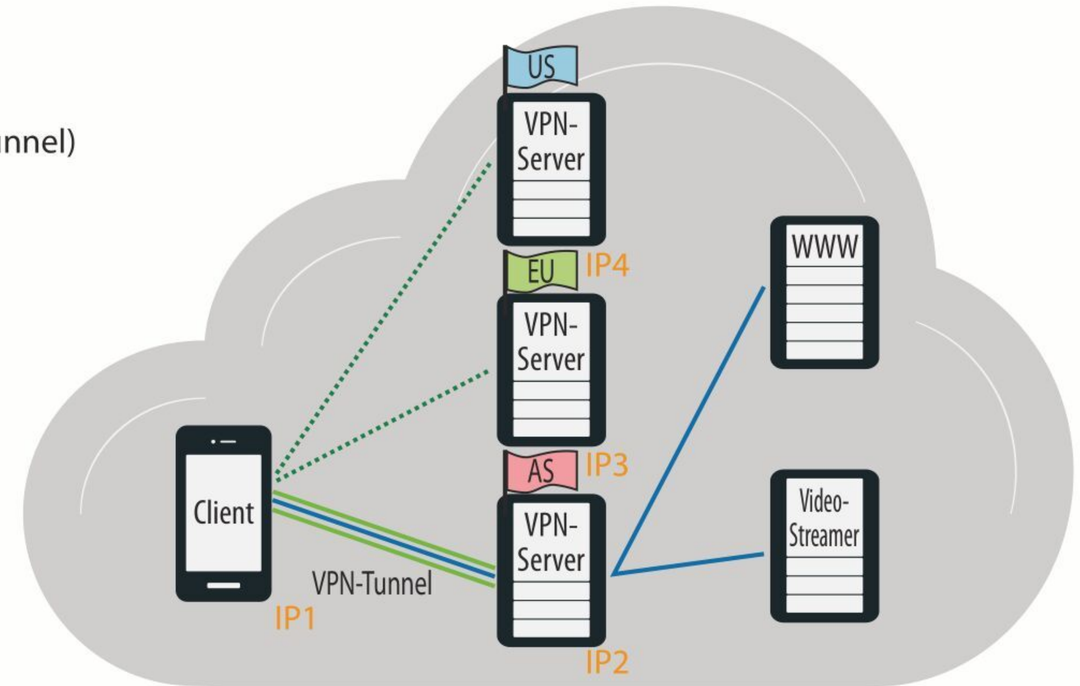
IPX unterschiedliche, globale IP
verschlüsselte Verbindung (TLS)
unverschlüsselte Verbindung



Virtuelle Ortswechsel per VPN

VPN-Provider betreiben Server in vieler Herren Länder. So erhält der Kunde eine IP-Adresse, die Internet-Dienste dem Land zurechnen. Videostreaming-plattformen werten die aus. Allerdings pflegen die auch Blacklisten mit den IP-Adressen der VPN-Server, sodass ein Zugriff auf die Plattform über das VPN früher oder später misslingt.

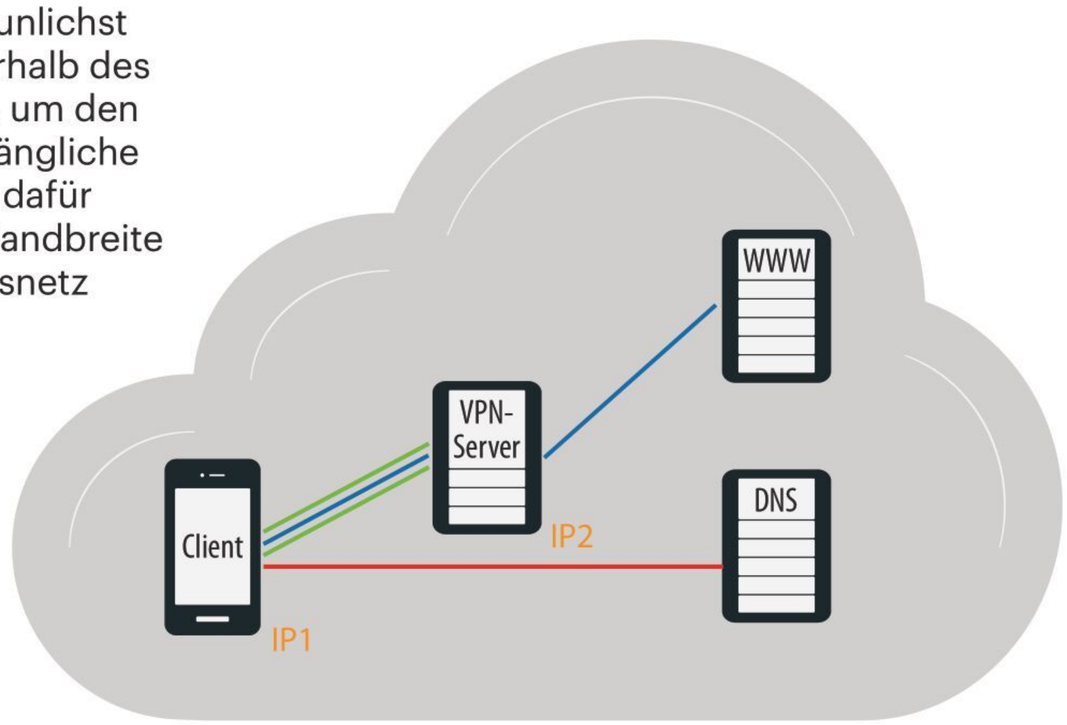
IPX unterschiedliche, globale IP
verschlüsselte Verbindung (TLS)
verschlüsselte Verbindung (VPN-Tunnel)
alternative Verbindung (VPN)



Split-Tunneling im VPN

Wer sich hinter einem VPN-Server verstecken möchte, sollte tunlichst vermeiden, dass – vom VPN-Verkehr abgesehen – Daten außerhalb des Tunnels den Client verlassen. Schon ein Paket könnte reichen, um den Schutz auffliegen zu lassen. DNS-Anfragen oder nicht vollumfängliche IPv4- und IPv6-Unterstützung durch das VPN können Ursache dafür sein. Firmen schätzen hingegen das Verhalten, wenn Sie die Bandbreite Ihres VPN-Servers schonen wollen: Nur der fürs Unternehmensnetz gedachte Verkehr fließt dann durch den Tunnel.

IPX unterschiedliche, globale IP
— verschlüsselte Verbindung (TLS)
— verschlüsselte Verbindung (VPN-Tunnel)
— unverschlüsselte Verbindung



entwickelt, Benutzer wiederzuerkennen. Erst wenn man sich auf das mühsame Unterfangen eingelassen hat, all diese Plagegeister aus dem Fell zu schütteln (siehe ct.de/wrqr), gewinnt man noch mehr Anonymität durch das Verschleiern der IP-Adresse per VPN.

Einen Vorteil verspricht eine andere IP-Adresse allerdings: Dienste erkennen nicht mehr zwangsläufig, in welcher geografischen Region der Internetanschluss liegt. Anhand der Adresse lässt sich das nämlich ziemlich exakt bis hinunter zur Stadt ermitteln. Größere VPN-Provider betreiben weltweit mehrere tausend Server, sodass ihre Kunden sich gezielt auf andere Kontinente begeben können – jedenfalls denken die Dienste das anhand der IP-Adresse, die sie zu sehen bekommen.

Urvertrauen

Anbieter von urheberrechtlich geschütztem Material, das noch dazu unterschiedliche Veröffentlichungstermine auf verschiedenen Kontinenten oder in verschiedenen Ländern hat – Streamingdienste oder lokale Mediatheken –, haben sich allerdings längst auf die VPN-Trickserei eingestellt. Sie blockieren Zugriffe, die von ihnen bekannt gewordenen VPN-Servern stammen. Allzu schwer ist das nicht, weil die von den Providern in Rechenzentren angemieteten Server typischerweise andere IP-Adressbereiche verwenden als die Kunden, die von ihren DSL-, Kabel- und Glasfaseranschlüssen aus die Angebote nutzen.

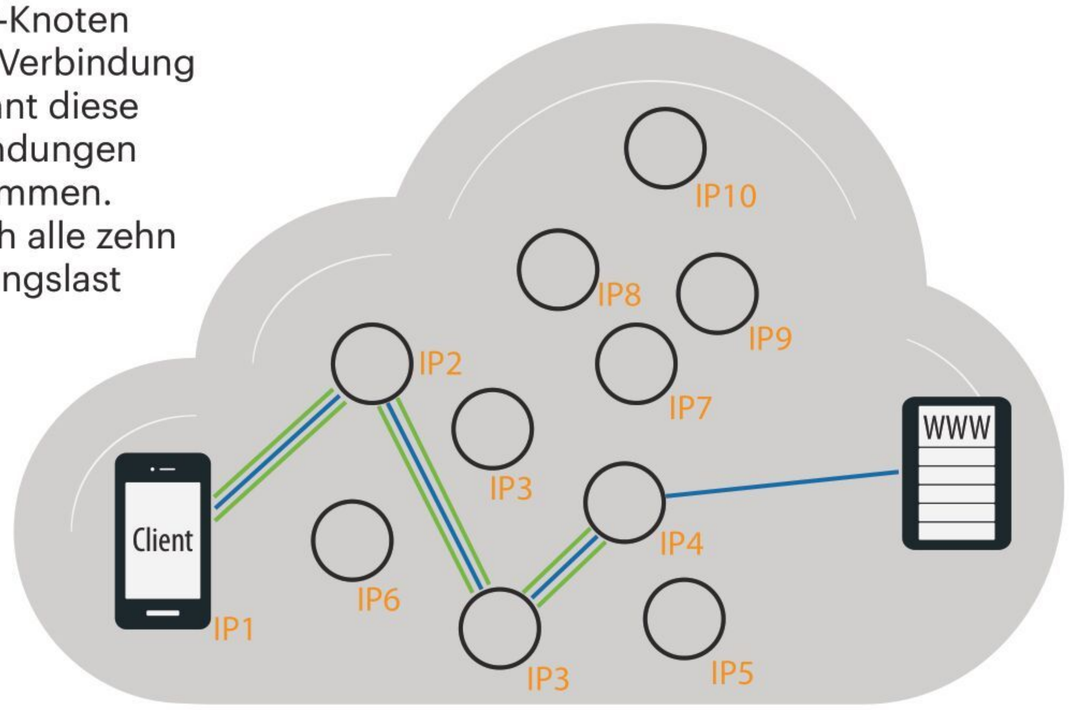
Von der Tatsache, heute mit einem VPN-Provider hierzulande noch nicht erhältliche US-Serien ansehen zu können, sollte man nicht auf Morgen schließen. Wer das allzu voreilig tut und stark rabattierte Zwei-Jahres-Verträge abschließt, tappt in die Muckibudenfalle des Internet. Obendrein: Viele VPN-Provider brüsten sich zwar mit einer riesigen Zahl von Servern weltweit. Gezielt ansteuern kann man die aber oft nicht – die Provider versuchen, Kunden gleichmäßig auf die Server zu verteilen, sodass man mit Pech und ohne Handarbeit vielleicht nur an die Server gerät, die auf Blacklisten stehen.

Apropos Handarbeit: Achten Sie darauf, die Dienste eines VPN-Providers ohne dessen Spezialsoftware nutzen zu können. Zum einen können Sie so selbst beeinflussen, mit welchem seiner VPN-Server Sie sich verbinden. Zum anderen stellen Sie so sicher, dass der Betreiber keine Extras einbaut, etwa Ihren Internetanschluss andere Kunden mitbenutzen lässt (wie das eingangs erwähnte Hola). Im Zweifel ist die offizielle Software der Open-Source-Projekte wie WireGuard oder OpenVPN oder die bereits in Client-Betriebssystemen integrierte VPN-Zugangssoftware die beste Wahl.

Tor als VPN-Alternative

Im Tor-Netzwerk wählt ein Client aus der Gesamtzahl der Tor-Knoten einen Eintritts-, Vermittlungs- und Austrittsknoten. Auf jeder Verbindung kommt ein anderer Schlüssel zum Einsatz. Nur der Client kennt diese und gibt jeweils einen an den beteiligten Node weiter. Verbindungen scheinen stets von der IP-Adresse des Austrittsknoten zu stammen. Der Knoten und damit die IP-Adresse ändert sich automatisch alle zehn Minuten. Die vielen beteiligten Knoten und die Entschlüsselungslast verlangsamen den Datenfluss.

IPX unterschiedliche, globale IP
verschlüsselte Verbindung (TLS)
verschlüsselte Verbindung (via Tor)
Tor-Nodes



Wenn Sie dieser Empfehlung folgen, vergeben Sie ein viel gepriesenes Feature, den sogenannten Kill-Switch. Darunter verstehen die VPN-Provider eine Funktion, die sicherstellen soll, dass sämtliche Daten von Ihrem Client nur durch den VPN-Tunnel fließen. Bei einer VPN-Störung sollen so – für den Nutzer womöglich unbemerkt – keine Daten über den regulären Internetzugang des Clients laufen. Vom Prinzip her ist das eine gute Idee. Wer das aber wirklich in Perfektion braucht, sollte das anders sicherstellen: Filterregeln auf Ihrem DSL-Router, die nur Verbindungen zum VPN-Server zulassen, sind aus unsere Sicht weitaus vertrauenswürdiger.

Ähnliches gilt auch für die weiteren Extras, mit den einige VPN-Provider ihren Nutzwert aufhübschen wollen: Sie betreiben eigene, filternde DNS-Server, um ihren Kunden Werbung vom Hals zu halten. Aus unsere Sicht sind solche Angebote eine gute Idee. Aber sie zahlen sich vor allem dann voll aus, wenn sie unabhängig betrieben werden – also ohne etwaige andere Interessen. Wenn Sie wirklich darauf angewiesen sind, sich maximal zu schützen, bieten sich vertiefende Artikel aus c't an, die Sie als Digitalabonnent über den Link erreichen (siehe ct.de/wrqr). Betreiben Sie gegebenenfalls einen eigenen filternden DNS-Server wie Pi-Hole oder Adguard und lassen Sie den verschlüsseltes DNS verwenden (siehe ct.de/wrqr).

Vertiefende Artikel

ct.de/wrqr

Vertrauen

Auch wenn gegenüber den VPN-Providern eine Grundskepsis angebracht ist, liefern sie doch einen sinnvollen und durchaus empfehlenswerten Dienst: Sobald Sie sich mit Ihren Geräten in einem öffentlichen, offenen, nicht verschlüsselten WLAN bewegen, sollten Sie das nur mit einer VPN-Verbindung tun. Die stellt sicher, dass alle Daten verschlüsselt sind, die Ihr Client verschickt und empfängt. Selbst wenn Sie sich versehentlich in den Maschen eines Netzes verfangen, das Bösewichte mit dem Ziel betreiben, Daten abzufischen, wären Sie dann sicher.

Sollte Ihr Ziel sein, unerkannt im Internet aktiv zu werden, sind VPNs ein zweifelhaftes Mittel: Wie Ihr Internet-Provider kennt der VPN-Betreiber meist Ihre Identität. Wie haltbar seine Versprechen sind, nichts zu protokollieren und die Identität seiner Kunden nicht preiszugeben, ist meist unbelegt. Hinweise, dass einzelne VPN-Server übernommen worden sind, gibt es. Ob das genügt, um Ihre Identität aufzudecken, steht auf einem anderen Blatt. Mit Tor oder auch offenen WLANs, die von nicht kommerziellen Initiativen wie Freifunk betrieben werden, gibt es gute Alternativen. Keine der Methoden garantiert jedoch unter allen Umständen Anonymität.

(ps) c't

Bild: Andreas Martini

Elf VPN-Anbieter im Vergleich

Intransparente Rabatte, vollmundige Versprechen, fragwürdige Werbeprogramme: Die VPN-Branche gibt kein gutes Bild ab, dabei geht es doch um Vertrauen. Wer genau hinschaut, findet aber auch datenschutzfreundliche VPN-Anbieter mit klaren Tarifen und nützlichen Funktionen.

Von **Keywan Tonekaboni**

Wenn das Internet die Datenautobahn ist, dann sind die VPN-Anbieter die Gebrauchtwagenhändler des Internets. Es gibt unzählige Anbieter mit teils sehr großspurigen Versprechen zu Anonymität, Privatsphäre und Sicherheit. Dabei sind einige der vollmundigen Behauptungen schlicht falsch und andere lassen sich nicht verifizieren.

Dieser Artikel soll etwas Klarheit in die trübe VPN-Angebotssuppe bringen. Der Fokus liegt auf Anbietern für Privatpersonen, die sich in öffentlichen WLANs schützen wollen oder sich im Netz mit einer

im Ausland verorteten IP-Adresse bewegen möchten. Wir erklären, worauf es bei der Auswahl eines VPN-Anbieters ankommt und von welchen gewagten Werbeaussagen Sie sich nicht blenden lassen sollten.

Wer ein VPN verwenden möchte, muss dem Anbieter vertrauen. Was auf dem Server passiert, bleibt für Außenstehende verborgen. Daher sollte zumindest der Verbindungsaufbau so transparent wie möglich sein. Unsere Übersicht haben wir deshalb auf solche Dienstleister eingeschränkt, die Verbindungen mittels WireGuard über die im Betriebssystem integrierte VPN-Funktion oder die Zugangssoftware des WireGuard-Projekts anbieten. Dazu müssen die Anbieter die VPN-Konfiguration oder Zugangsdaten bereitstellen. WireGuard ist sicher, schnell und besonders für den mobilen Einsatz geeignet, mehr zu VPN-Protokollen erklärt der Artikel ab Seite 98. Anbieter, die den Quelltext ihrer eigenen Zugangssoftware veröffentlicht haben, haben wir ebenfalls mit aufgenommen.

Wir haben elf Anbieter ausgemacht, die diesen Kriterien entsprechen: AzireVPN, Hide.me, IVPN, Mozilla VPN, Mullvad, OVPN, Private Internet Acccess (PIA), StrongVPN, VPN.AC, WeVPN und Windscribe. Anbieter wie CyberGhost oder NordVPN fielen durch Raster, da sie WireGuard nur mit eigenen Apps zulassen. Was uns bei diesen Anbietern aufgefallen ist, haben wir dennoch im Text festgehalten. ProtonVPN bot WireGuard-Zugänge erst an, als wir unseren Anbietervergleich bereits abgeschlossen hatten.

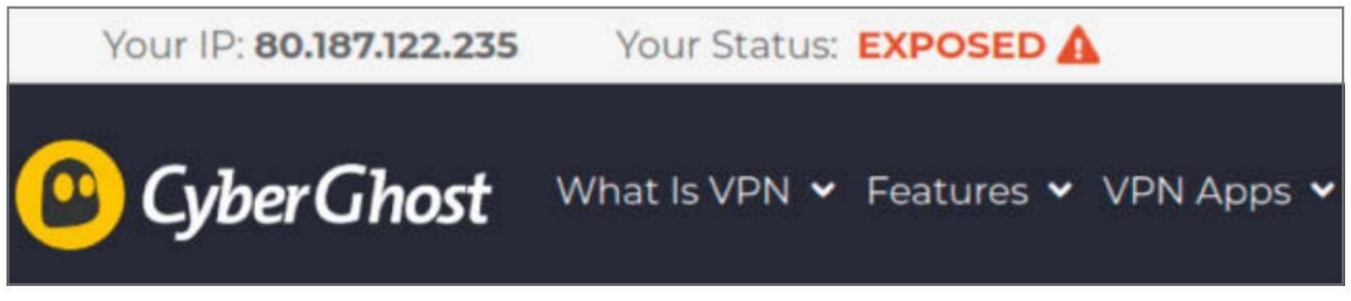
Marktschreier

Viele VPN-Anbieter arbeiten zum Ankurbeln der Nachfrage mit Affiliate-Marketing. Blogs und Websites mit fadenscheinigen Produkttests erhalten für Empfehlungen eine Vergütung. Das ist an sich nicht verwerflich, wenn dies dem ratsuchenden Publikum transparent gemacht wird. Das ist leider nicht immer der Fall, beziehungsweise sind die Hinweise darauf sehr versteckt. Zudem besteht die Gefahr, dass die Aussicht auf eine Provision das Testergebnis beeinflusst. Das geht sogar so weit, dass in einem Test von WireGuard-Anbietern ein VPN-Provider gewinnt, der der über WireGuard überhaupt keinen Zugang bereitstellt. Firmen wie IVPN oder Mullvad lehnen dieses Geschäftsgebaren als unseriös ab und haben ihre Affiliate-Programme, wenn überhaupt vorhanden, eingestellt (siehe ct.de/w7mk).

Neben mutmaßlich gekauften Reviews und massiver Werbung in sozialen Netzwerken nutzen VPN-Anbieter noch eine weitere Masche: das Spiel mit der Angst. Wer die Webseiten von VPN-Anbietern besucht, sieht häufig eine auffällige Warnung: Die eigene Internetverbindung oder IP-Adresse sei ungeschützt. Um die Behauptung zu bekräftigen, enthält die Warnung der IP-Adresse zugeordnete Daten wie den Internet-Provider oder den vermuteten geografischen Standort. Daneben heißt es in markigen Aussagen, nur der angebotene VPN-Dienst biete Schutz, damit niemand in den Datenverkehr reinschauen kann. Dass sowohl der VPN-Anbieter selbst als auch Lauscher auf dem Weg zwischen VPN-Gateway und Zielhost weiter Einblick in den Datenstrom haben können, verschweigen die Marketing-Sprüche hingegen oft. Deutschsprachige Kundinnen und Kunden werden außerdem mit angeblich erhöhtem Datenschutz geködert.

Dagegen fragt IVPN prominent auf der eigenen Startseite „Brauchen Sie wirklich ein VPN?“ und rät explizit vom unnötigen Einsatz eines VPN-Dienstes ab. Anonymität, Schutz vor Internetkriminalität und Datensammlern wie Facebook oder Google gewährleiste ein VPN nicht. Nur wer seinem Internet-Provider nicht vertraue oder Schutz vor einem Angreifer in einem ungeschützten Netzwerk suche, oder Zensur und Geoblocking umgehen wolle, solle einen VPN-Dienst buchen.

Manchen Menschen geht es aber gar nicht um Privatsphäre, sondern um den Zugang zu medialen Inhalten, wie ausländischen Streamingangeboten, etwa Netflix USA oder dem BBC iPlayer. Auch diese Klientel umwerben die VPN-Anbieter. Sie listen auf, welche der eigenen Server sich dafür besonders eignen. Hide.me wirbt so offensiv mit dem freien Zugang zu diversen Streamingdiensten wie BBC iPlayer, HBO Go oder Hulu, dass man fast den Eindruck gewinnt, Hide.me wäre ein Kabelnetzbetreiber und kein VPN-Dienst. StrongVPN geht sogar so weit, detailliert zu erklären, wie man eine gefälschte Rech-



Mit Warnungen versuchen VPN-Anbieter, zum Abschluss eines Abonnements zu drängen.

nungsadresse erzeugt, um sich bei einem US-Streaming-Dienst anzumelden.

Keiner der Anbieter blockiert P2P-Filesharing und Torrent-Software, obwohl deren Nutzung rechtlich meist unzulässig ist. Vielmehr ist es wohl ein Verkaufsargument. IVPN bittet lediglich höflich darum, für Filesharing nicht die US-Server zu verwenden; aufgrund zahlreicher Urheberrechtsbeschwerden (DMCA Takedown Notices) seien die von einer Abschaltung bedroht. Windscribe missbilligt floskelhaft den Einsatz seines Dienstes für illegale Aktivitäten, während es an anderer Stelle penibel erklärt, wie man Torrents sicher und ohne Sorge vor juristischer Verfolgung nutzt. Ähnliche Anleitungen stellen auch Hide.me, OVPN und PIA bereit; Mullvad bietet sogar einen Online-Check auf Torrent-Leaks. VPN.AC gibt Tipps, welche Server für Filesharing die beste Anbindung haben und CyberGhost hat in seiner Zugangssoftware eine eigene Kategorie dafür.

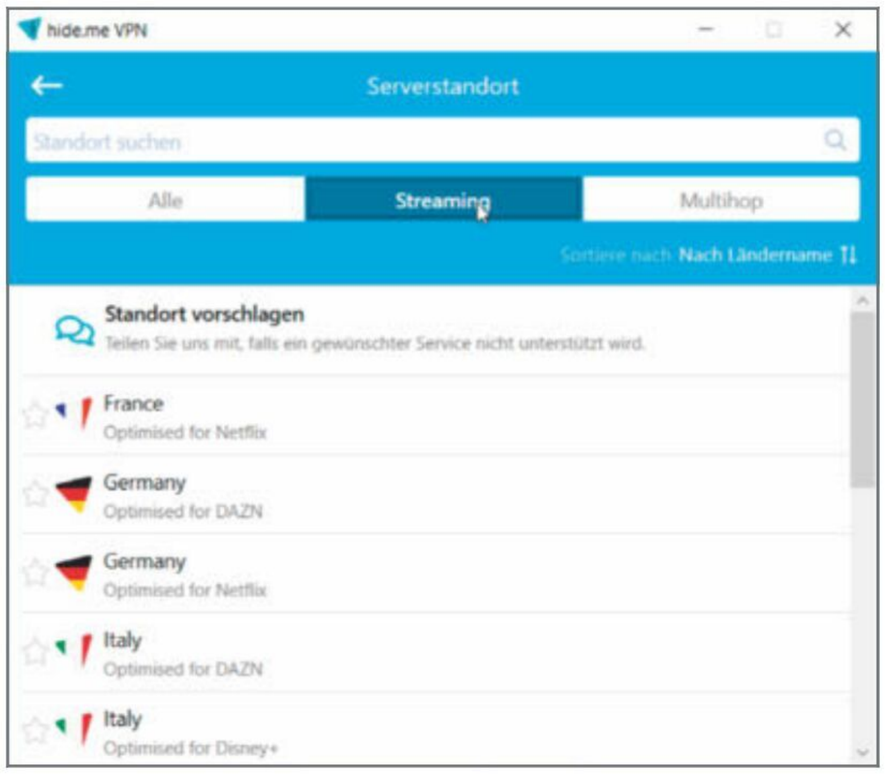
Tunnel ins Steuerparadies

Die Firmensitze der VPN-Anbieter lesen sich wie eine Liste bekannter Steueroasen: Britische Jungferninseln, Gibraltar, Malaysia oder Panama. Dadurch hoffen die Anbieter, sich dem Zugriff der Sicherheitsbehörden und der Justiz aus den USA, der Europäischen Union und anderen Ländern zu entziehen. Wer vor hiesigen Behörden zu solchen Firmen flüchtet, darf anderseits aber auch nicht auf europäisches Verbraucherschutzrecht hoffen. Oft fehlt es schon an einem Impressum, Kontaktdaten oder klaren Angaben, welche Firma hinter dem Angebot steckt.

Es gibt aber auch etliche Anbieter aus der EU: AzireVPN und Mullvad aus Schweden, VPN.AC aus Rumänien. Beide Länder haben den Ruf einer datenschutzfreundlichen Gesetzgebung.

Vertrauensbildende Maßnahmen

Um für Vertrauen zu werben, versprechen alle Anbieter, für die VPN-Nutzung keine Protokolle (Logs) zu speichern. Die einen speichern zumindest temporär die dem Client vom VPN-Server zugewiesene IP-Adresse, andere haben eine strikte „Zero Logs“-Policy. All diese Angaben sind jedoch kaum unabhängig überprüfbar. Windscribe musste kürzlich eingestehen, dass in der Ukraine zwei ihrer Server beschlagnahmt wurden. Brisant an der Geschichte: Die Server waren nicht verschlüsselt und auf ihnen lief OpenVPN mit einer unsicheren Konfiguration.



Hide.me listet für Streaming-dienste geeignete VPN-Server in einer eigenen Kategorie auf.

Als Steigerung werben einige Betreiber mit datenträgerlosen Servern, deren Systeme ausschließlich im Arbeitsspeicher laufen. AzireVPN und WeVPN betreiben laut eigenen Angaben ihre Server im „Blind Operator Mode“. Ein Kernel-Modul verwehrt selbst Root den Zugriff auf den Netzwerkverkehr und versteckt die von WireGuard genutzten IP-Adressen. WireGuard-Erfinder Jason A. Donenfeld hat das Modul auf Initiative von AzireVPN entwickelt. Ironischerweise bezeichnet er selbst das Modul als Quacksalberei, rät von der Nutzung ab und macht sich darüber lustig („Für ahnungslose Betreiber, die noch ahnungsloser werden wollen“, siehe ct.de/w7mk).

Ein Siegel für vertrauenswürdige VPN-Anbieter gibt es nicht. Einige Anbieter haben immerhin unter dem Label „VPN Trust Initiative“ (VTI) gemeinsame Prinzipien vereinbart. Die freiwillige Selbstverpflichtung klingt plausibel, lässt aber auch Schlupflöcher offen und es fehlen Mechanismen zur Durchsetzung. Zur VTI gehören unter anderem Hide.me, NordVPN, StrongVPN und WeVPN. Mullvad und IVPN waren an einer ähnlichen, mittlerweile scheinbar eingeschlafenen Initiative beteiligt („Trustworthy VPNs“).

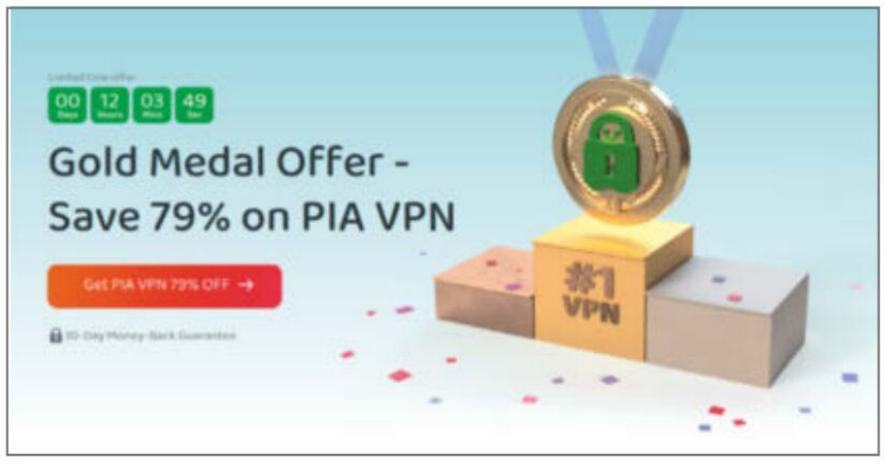
Indizien für die Glaubwürdigkeit der Zero-Logs-Bekundungen liefern Gerichtsverfahren, wenn VPN-Anbieter trotz entsprechender Beschlüsse keine Daten aushändigen und vor Gericht versichern, über keine Nutzungsdaten zu verfügen. OVPN hat gegen einen Urheberrechtsverband ein Verfahren gewonnen und wirbt damit.

Aussagekräftiger sind Audits, in denen unabhängige Firmen die Infrastruktur und Software auf Sicherheitslücken untersuchen und die Aussagen der

Anbieter bestätigen. So soll PricewaterhouseCoopers (PwC) laut NordVPN ein Audit durchgeführt haben. Merkwürdigerweise haben weder NordVPN noch PwC den vollständigen Bericht veröffentlicht, was übrigens gegen die VTI-Prinzipien verstößt. Andere Berichte stellt NordVPN vollständig im Kundenbereich bereit. Die Berliner Sicherheitsfirma Cure53 hat bei mehreren VPN-Anbietern, darunter IVPN, Mullvad und Surfshark, Audits durchgeführt und veröffentlicht. Darin sind auch die gefunden Schwachstellen dokumentiert. Wenn ein VPN-Anbieter mit einem Audit wirbt, achten Sie darauf, ob der Bericht veröffentlicht und was genau geprüft wurde: die Sicherheit der Server, nur eine Browser-Extension oder die No-Log-Policy? Zudem sind Audits immer nur eine Momentaufnahme.

Zur Beruhigung der Kundschaft pflegen AzireVPN, IVPN und WeVPN einen sogenannten Warrant Canary. Wie der Kanarienvogel im Bergbau soll dieser vor Gefahren warnen: Gesetze wie der berüchtigte Patriot Act erzwingen unter Strafandrohung eine stille Zusammenarbeit mit Sicherheitsbehörden. Um dem vorzubeugen, veröffentlicht der Betreiber turnusmäßig eine PGP-signierte Erklärung, dass weder gerichtliche Verordnungen oder Beschlagnahmungen vorliegen noch Durchsuchungen stattgefunden haben. Bleibt deren Aktualisierung aus, ist die Kundschaft gewarnt, ohne dass für den Anbieter eine Strafe droht. So zumindest die Theorie. Die Wirksamkeit eines Warrant Canary ist umstritten, da dessen Erneuerung erzwungen werden könnte.

Damit erst gar keine Daten in falsche Hände geraten, sollten möglichst wenige erhoben werden. Gut die Hälfte der Anbieter verlangt für die Registrierung eine gültige E-Mail-Adresse, bei den anderen ist selbst die optional. Mullvad und IVPN beschränken sich auf eine anonyme Zugangsnummer. Für die Anmeldung bei OVPN muss man ein Google-Captcha lösen, was dem Versprechen von mehr Privatsphäre zuwiderläuft.



Mit angeblich zeitlich begrenzten Rabatten erhöhen manche VPN-Provider den Verkaufsdruck. Das identische Angebot sahen wir aber an mehreren Tagen.

Preiskarussell

Wer einen VPN-Tarif buchen will, hat die Wahl zwischen Monatstarifen und Verträgen von mehreren Monaten bis hin zu einem oder zwei Jahren Laufzeit, bei manchen Anbietern sogar bis hin zu drei Jahren. Um Anbieter, die gegen Einmalzahlung einen lebenslangen VPN-Zugang versprechen, sollten Sie einen großen Bogen machen, da dies kein seriöses Geschäftsmodell ist.

Das gilt aber auch für die Mehrjahresverträge. Viele VPN-Anbieter locken mit hohen Rabatten. So kostet ein Monatstarif meist um die 10 Euro, der Jahrestarif nur 60 Euro, also umgerechnet 5 Euro im Monat. Aber ob der Dienst auch in Zukunft die gewünschte Bandbreite oder den Zugang zur Lieblingsmediathek bietet, kann niemand garantieren. In unsere Vergleichstabelle haben wir Preise für einen Monat, drei Monate und ein Jahr aufgenommen. Positiv sticht Mullvad hervor, der unabhängig von der Laufzeit nur 5 Euro pro Monat berechnet. Zudem sollte man sich bei den langfristigen Verträgen nicht vom angezeigten niedrigen Monatspreis täuschen lassen. Anders als beim Mobilfunkvertrag wird der Preis für die gesamte Laufzeit sofort fällig und im Voraus eingezogen.

Bei fast allen Anbietern ist die automatische Vertragsverlängerung voreingestellt. Azire-VPN und Mullvad bieten auch Einmalzahlungen an. Alle VPN-Dienste akzeptieren die Bezahlung per Kreditkarte, fast alle auch per PayPal und Kryptowährung. Über ein Bankkonto (Giropay, SEPA-Lastschrift) nehmen nur vier Anbieter das Geld entgegen. Wer ganz viel Wert auf Datenschutz legt, schickt per Post Bargeld an AzireVPN, IVPN, Mullvad oder OVPN. Wählerisch gibt sich Mozilla, das ausschließlich per Kreditkarte abrechnet.

Manchmal weicht der beworbene vom abgebuchten Preis ab, da einige Anbieter die Mehrwertsteuer erst während des Bestellvorgangs aufschlagen. Bei Anbietern, die die Preise in US-Dollar berechnen, können zusätzliche Bankgebühren für Zahlungen in Fremdwährung anfallen. Auskunft dazu gibt Ihnen Ihre Bank oder die Ausgabestelle Ihrer Kreditkarte.

Die Rabatte sind teilweise undurchsichtig. So gibt OVPN als Referenz für den Rabatt Mondpreise an, die deutlich höher sind als der Monatstarif über die gleiche Laufzeit. Die Ersparnis für den Zweijahresvertrag schrumpft so von angeblichen 264 Euro auf real 120 Euro, was immer noch beachtlich hoch ist. Auch VPN.AC wirbt beim Dreijahresvertrag mit einem prozentual geringfügig zu hohen Rabatt. VyprVPN

rechnet in den Rabatt auch die zusätzlichen Gratismonate ein und drückt so den Durchschnittspreis. Bei PIA sind in der Bestellübersicht für den Jahrestarif knapp 112 Euro aufgelistet. Der versprochene Preis von gut 37 Euro ergibt sich durch einen Rabatt von circa 74 Euro. Es bleibt aber unklar, ob der Nachlass nur im ersten Jahr gewährt wird.

Um eine Kaufentscheidung zu forcieren, zeigen beispielsweise CyberGhost, NordVPN, PIA oder VyprVPN einen Countdown für den versprochenen Rabatt an, der sekundenweise herunterzählt. Dieses „Pressure Selling“ ist nach EU-Recht eigentlich unzulässig, muss laut Verbraucherzentrale Bayern aber im Einzelfall juristisch geklärt werden. Unser Tipp: Lassen Sie sich von Sonderangeboten nicht unter Druck setzen, denn die Rabatt-Aktionen werden ständig neu aufgelegt.

Erfreulicherweise unterscheiden sich die verschiedenen Tarife abseits der Laufzeit kaum. Den Jahresverträgen vorbehalten oder zusätzlich kostenpflichtig sind höchstens nicht zwingend notwendige Zusatzfunktionen wie VPN-Verbindungen über mehrere Server (Multihop), Port-Forwarding oder eine öffentliche IP-Adresse.

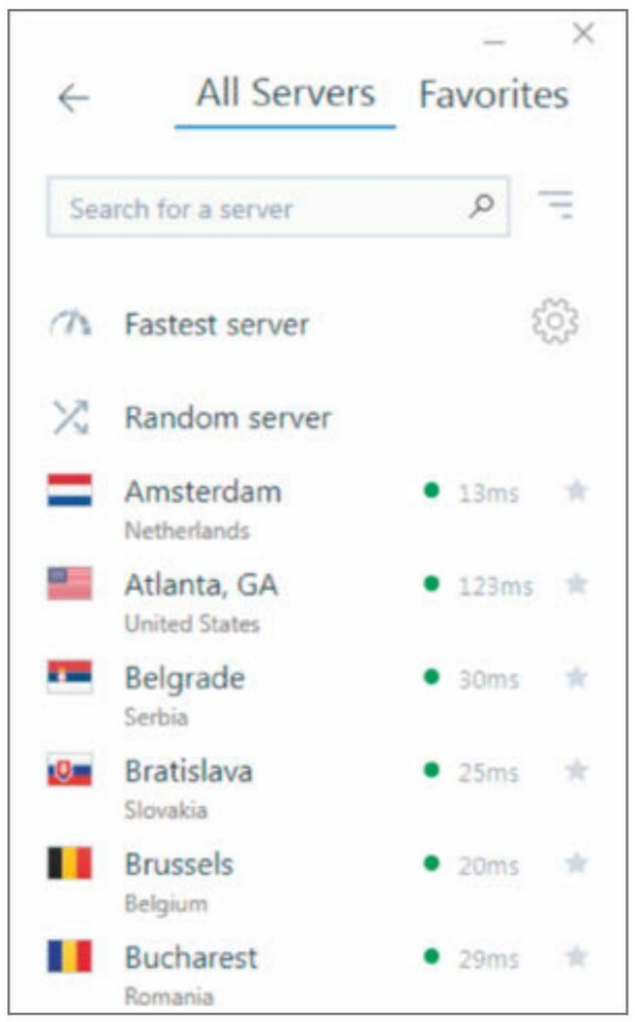
Alle Anbieter versprechen unbegrenztes Datenvolumen oder schränken es nicht von vornherein ein. Meist sind gleichzeitige Verbindungen von fünf bis zehn Geräten im Tarif enthalten. IVPN bietet auch einen vergünstigten Tarif für maximal zwei Geräte an. Im Unterschied dazu erlaubt Windscribe, beliebig viele Geräte gleichzeitig per VPN zu verbinden, solange der VPN-Zugang nur im engsten Familienkreis geteilt wird.

Die Verbindungsgeschwindigkeit schwankte bei unseren Stichproben zwischen den Anbietern, jedoch war sie in der Regel deutlich höher als 100 MegaBit/s, oft auch ein Mehrfaches davon. Eine richtige Schnarchnase fiel uns nicht auf. Lediglich ein von Hide.me für Netflix USA empfohlener Server war so langsam, dass die Verbindung nur für HD-Streaming gereicht hätte. Die gebotene Geschwindigkeit kann jederzeit schwanken, abhängig vom zugeteilten Server, dessen Auslastung und weiteren Faktoren.

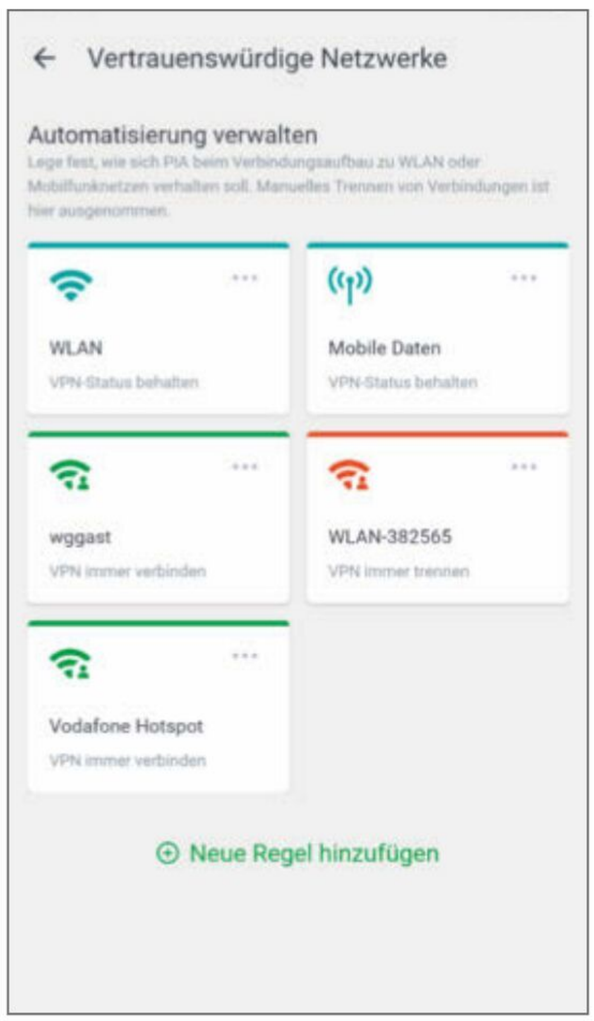
Die Anzahl der Serverstandorte schwankt zwischen 19 bei AzireVPN und 110 bei Windscribe. Gateways zu beliebten VPN-Ausflugszielen wie Großbritannien oder die USA stellen alle bereit, ebenso Server in Deutschland, den Niederlanden oder Schweden. Wenn Sie ein bestimmtes Land benötigen, prüfen Sie vor der Buchung die verfügbaren Standorte. Die sind meist auf der Webseite aufgeführt.

App ins VPN

Das WireGuard-Protokoll ist bei VPN-Anbietern nicht unumstritten. Der minimalistische Code überzeugt



Die VPN-Apps der Anbieter sortieren die Server nach Reaktionszeit, Region oder gewünschter Anwendung.

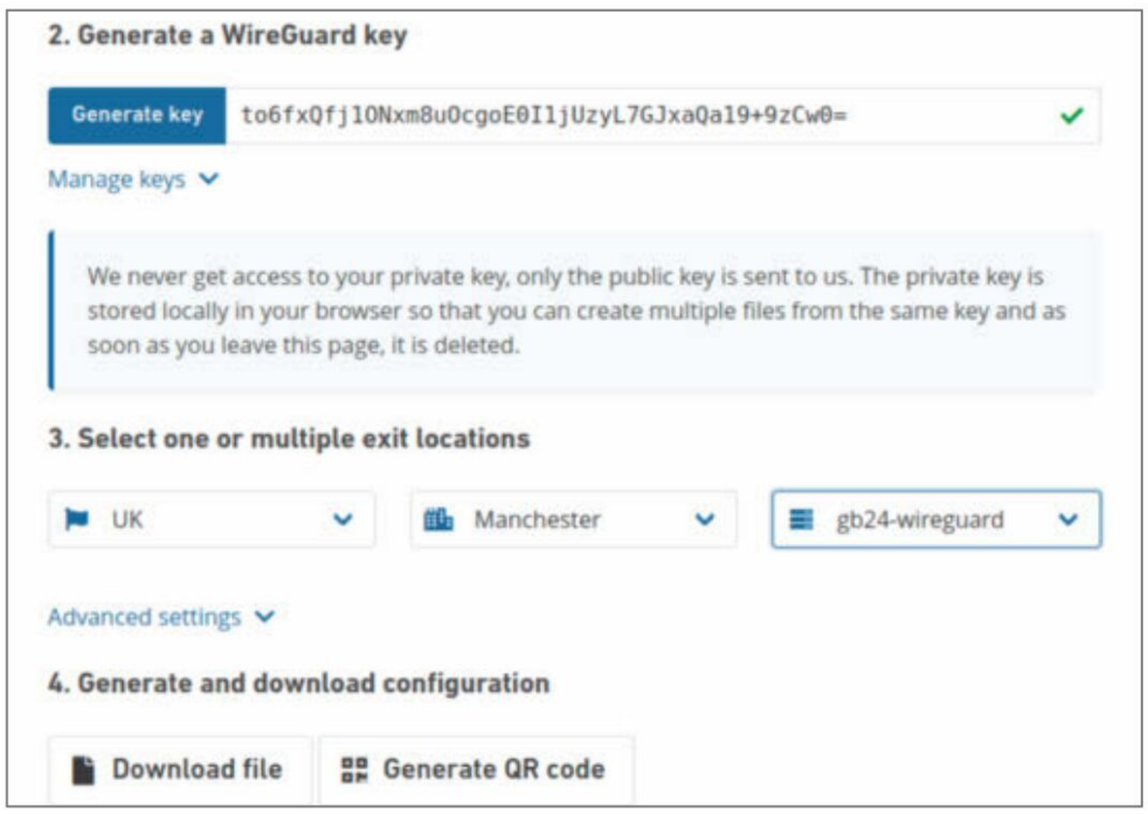


Erlaubt man der VPN-App den Zugriff auf den Standort, schaltet sie abhängig vom verbundenen WLAN das VPN an oder ab.

zwar durch Einfachheit und Geschwindigkeit. Kritiker bemängeln jedoch, WireGuard sei nicht optimal auf Privatsphäre ausgerichtet. Üblicherweise wird die dem VPN-Tunnel zugewiesene IP-Adresse fest in die WireGuard-Konfiguration geschrieben. Da man so bei jeder Verbindung die gleiche IP-Adresse verwendet, lässt sich das Surfverhalten einem Account zuordnen. Das gilt vor allem für die nur intern im VPN-Netz verwendete private IP-Adresse, während Webserver meist nur die nach außen sichtbare IP-Adresse des Gateways sehen.

WireGuard gibt diese feste Zuordnung nicht vor; sie resultiert aus der besonders einfach gestalteten Konfiguration mit `wg-quick`. Unter anderem Hide.me, Mozilla und NordVPN haben eigene Lösungen entwickelt, um die WireGuard-Verbindung mit dynamisch vergebenen IP-Adressen aufzubauen. Wie oft eine neue IP-Adresse zugeteilt wird, variiert zwischen den Diensten.

Dafür ist aber die Nutzung der anbieterspezifischen Zugangssoftware notwendig. In der Regel gibt man nur die Anmeldedaten an und die App generiert dann die benötigten WireGuard-Schlüssel und kümmert sich um den Schlüsselaustausch mit dem VPN-Server. Letztlich muss man auf die eine oder andere Weise dem VPN-Anbieter vertrauen. Mehrere Anbieter haben ihren Client unter einer Open-Source-Lizenz veröffentlicht.



Mit dem Web-Generator erzeugt man die passende WireGuard-Konfiguration. Fürs Mobiltelefon muss man nur noch den QR-Code scannen.

Auch sonst erleichtert eine Zugangssoftware das Surfen durch den VPN-Tunnel. In der App wählt man bequem aus einer Liste die gewünschte Region aus oder lässt sich mit dem schnellsten Server verbinden. Die Programme listen die Standorte sortiert nach Ländern oder Latenzen auf, vereinzelt werden Server für Streaminganbieter oder Filesharing hervorgehoben. Hinzu kommen diverse Zusatzfunktionen wie der automatische Verbindungsaufbau bei unsicheren Hotspots oder Ausnahmeregeln für einzelne Programme oder Hosts. Der Kill-Switch soll unbeabsichtigten Netzwerkverkehr außerhalb des VPN-Tunnels verhindern, aber darauf sollten Sie sich im Ernstfall nicht verlassen.

Alle VPN-Dienste verhinderten DNS-Leaks, da sie eigene DNS-Server anbieten und die Domainanfragen dort und nicht beim eigenen Internet-Provider landen. Der IPv6-Verkehr wird entweder ebenfalls durchs VPN getunnelt oder abgeklemmt. Lediglich WeVPN patzte dabei. Windscribe bietet unter Windows eine Option IPv6 abzuschalten, aber die verlangt einen Neustart. AzireVPN teilt eine globale IPv6-Adresse zu, aber Server im Netz sehen nur die des VPN-Gateways.

Wir haben uns den Netzwerkverkehr der Apps, die eine Verbindung per WireGuard aufbauen, unter Windows und Android angeschaut. Bei den meisten Anbietern mussten wir WireGuard explizit in den Einstellungen als Verbindungsprotokoll auswählen. Auch unter Windows ähneln die Programme vom Aussehen eher Handy-Apps. Die Anwendungen von StrongVPN und WeVPN verlangten bei jedem Start Admin-Rechte.

Positiv: Alle Programme und Apps verschlüsselten wie versprochen. Auch bei der Anmeldung beim VPN-Dienst selbst plauderten sie nichts aus. So konnten wir auch nicht kontrollieren, welche Daten durch den Tunnel gehen. Die Apps von StrongVPN, WeVPN und Windscribe enthalten laut der Tracker-Datenbank von „Exodus Privacy“ Bestandteile von Googles Analytics-Modulen Crashlytics und/oder Firebase Analytics. Ob die Bibliotheken fürs Tracking verwendet werden, bleibt unklar. IVPN schickt anonyme Fehlerberichte zu den Entwicklern, aber das lässt sich abschalten. Mozilla VPN fragt vorher, ob es Daten sammeln darf.

Handarbeit

Wenn Sie sich nicht mit den speziellen Apps herumschlagen wollen, erhalten Sie bei etlichen VPN-Anbietern die für WireGuard oder Ihr Betriebssystem

passenden Zugangsdaten. Meist gibt es einen Web-Generator, der im Browser die WireGuard-Keys erzeugt oder wo Sie einen vorhandenen Public Key eintragen können. Nach der Auswahl der gewünschten Server und weiterer Optionen erzeugt der Webdienst eine Konfigurationsdatei und bietet diese zum Download an, teilweise auch als QR-Code direkt zum Einscannen mit dem Handy oder als Zip-Archiv mit den Konfigurationsdateien für mehrere oder gar alle Server. Die Web-Generatoren von Mullvad und StrongVPN bieten für Linux an, über iptables-Regeln einen Kill-Switch einzubauen. Bis auf Windscribe hatten alle auf IPv4 beschränkten Anbieter die Konfigurationsdatei so erstellt, dass es keinen IPv6-Leak gab.

Merkwürdig ist der Ansatz von PIA: Für den Download der Konfigurationsdateien stellt der Anbieter nur einen komplexen Satz von Skripten bereit, die man als Root ausführen muss. Ebenso enttäuscht das Angebot von IVPN, denn dort muss man sich um alles selber kümmern: mit den WireGuard-Befehlen im Terminal ein Schlüsselpaar erzeugen, dann auf der IVPN-Webseite den Public Key hochladen und dort die Server-Daten heraussuchen und alles zusammen von Hand in eine Konfigurationsdatei eintragen.

VPN-Dienste mit WireGuard

Name	AzireVPN	Hide.me	IVPN	Mozilla VPN
Anbieter, Firmensitz	Netbouncer AB, Schweden	eVenture Ltd., Malaysia	Privatus Limited Inc., Gibraltar	Mozilla Corporation, USA
URL	azirevpn.com	hide.me	www.ivpn.net	mozilla.org/de/products/vpn
Anbieter-Apps mit WireGuard				
Windows / macOS / Linux	✓ / – / –	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓
Android / iOS	✓ / –	✓ / ✓	✓ / ✓	✓ / ✓
App Lizenz	proprietär	proprietär / GPLv21	GPLv3	GPLv3
Unterstützung für alternative Clients				
Konfigurationsdatei erhältlich via	QR-Code, Web-Generator, Skript	–	manuell[2]	–
Verbindung				
VPN-Server (IPv4 / IPv6)	✓ / ✓	✓ / ✓	✓ / –	✓ / ✓
Tunnel (IPv4 / IPv6)	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓
Schutz vor IPv6-Leak / DNS-Leak	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓
IP-Adresse öffentlich oder privat (IPv4 / IPv6)	privat / privat	privat / privat	privat / privat	privat / privat
Kill-Switch	–	✓	✓[4]	–
maximal verbundene Geräte	5	10	2 (Standard) / 7 (Pro)	5
freie Portwahl	✓	–	Auswahl	–
Protokolle zusätzlich zu WireGuard				
OpenVPN	✓	✓	✓	–
IPSec (L2TP / IKEv2)	–	– / ✓	– / ✓	–
Infrastruktur				
Standorte	19	53	45	52
Länder (Anzahl / Auswahl)[5]	14 / CA, FR, DK, RO, TH	46 / AU, BR, ES, HK, IT	32 / CH, IL, JP, SG, UA	33 / BR, CZ, HK, MD, NZ
Abonnement				
benötigte Daten	keine	E-Mail-Adresse	keine	keine
Abonnement / automatische Verlängerung	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓
Bezahlung per Bankkonto / Kreditkarte / PayPal / Bargeld / Kryptowährung	– / ✓ / ✓ / ✓ / ✓	✓ / ✓ / ✓ / – / ✓	– / ✓ / ✓ / ✓ / ✓	– / ✓ / – / – / –
Preise (mit WireGuard)				
1 Monat / 3 Monate / 12 Monate	5 € / 12 € / 45 €	12,99 € / – / 99,99 €	6 US-$ / – / 60 US-$ (Standard) 10 US-$ / – / 100 US-$ (Pro)	9,99 € / (kein 3-Monats-Preis) / 59,88 €

[1] nur unter Linux [2] Konfiguration und Keys muss man selber erstellen [3] öffentliche IP-Adresse gegen Aufpreis [4] nur mit Anbieter-App [5] alle Anbieter haben Standorte u. a. in DE, NL, SE, UK, US [6] 37,19 € im ersten Jahr

Ganz gleich ob Download oder QR-Code: Der Preis für die Autonomie ist das mit Ihrem Account verknüpfte Paar aus Schlüssel und IP-Adresse. Wollen Sie dieses austauschen, müssen Sie von vorne anfangen und neue Schlüssel und Konfigurationsdateien erzeugen. Ob man in einer festen (privaten) IP-Adresse oder in proprietären Apps das größere Übel sieht, ist Ansichtssache.

Fazit

Transparente und günstige Preise bieten AzireVPN, IVPN und Mullvad. Mozilla verpackt die Dienstleistung von Mullvad zum doppelten Preis in einer eigenen App. PIA und Windscribe verfügen über die meisten Serverstandorte in zahlreichen Ländern, aber bieten kein IPv6. Wer WireGuard mit den Apps der Anbieter nutzen will, sollte genau hinschauen, auf welcher Plattform das moderne Protokoll angeboten wird.

Weder der Unternehmenssitz an exotischen Standorten noch die vollmundigen Versprechen der Dienstleister garantieren wirklich Sicherheit. Dank der Vielfalt an VPN-Diensten können Sie den unseriösen Anbietern aber problemlos aus dem Weg gehen. (ktn) c't

Erklärungen zum Affiliate-Marketing und Blind Operator Mode

ct.de/w7mk

	Mullvad	OVPN	PIA	StrongVPN	VPN.AC	WeVPN	Windscribe
	Mullvad VPN AB, Schweden	OVPN Integritet AB, Schweden	Private Internet Access, Inc., USA	J2 Global, Inc., USA	Netsec (NSIS), Rumänien	WEVPN Ltd., British Virgin Islands	Windscribe Limited, Kanada
	mullvad.net	ovpn.com/de	privateinternetaccess.com	strongvpn.com	vpn.ac	wevpn.com	windscribe.com
	✓ / ✓ / ✓	– / – / –	✓ / ✓ / ✓	✓ / ✓ / –	– / – / –	✓ / ✓ / – /	✓ / ✓ / ✓ /
	✓ / ✓	✓ / –	✓ / ✓	✓ / ✓	– / –	✓ / ✓	✓ / ✓
	GPLv3	proprietär	GPLv3	proprietär	proprietär	proprietär	proprietär
	QR-Code, Web-Generator	QR-Code, Web-Generator	Skript	QR-Code, Web-Generator	Web-Generator	Web-Generator	Download
	✓ / ✓	✓ / –	✓ / –	✓ / –	✓ / –	✓ / –	✓ / –
	✓ / ✓	✓ / ✓	✓ / –	✓ / –	✓ / –	✓ / –	✓ / –
	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓[4] / ✓
	privat / privat	privat / privat	privat / –	privat / –	privat / –	privat / –	privat[3] / –
	✓	–	✓	–[1]	–	✓	✓[4]
	5	4	10	12	6	10	unbegrenzt (Haushalt)
	✓	–	–	Bereich	–	–	Auswahl
	✓	✓	✓	✓	✓	✓	✓
	–	–	–	✓ / ✓	✓ / ✓	– / ✓	– / ✓
	52	27	106	67	42	64	110
	33 / BR, CZ, HK, MD, NZ	17 / AU, DK, FR, JP, RO	78 / AU, CN, EG, IN, NZ	41 / AE, CO, EE, IE, ZA	23 / FR, JP, NO, PL, TW	47 / AT, BE, MX, PT, RU	63 / AZ, AQ, GR, PA, VN
	keine	keine	E-Mail-Adresse	E-Mail-Adresse	E-Mail-Adresse, Land	E-Mail-Adresse	keine
	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓
	✓ / ✓ / ✓ / ✓ / ✓	– / ✓ / ✓ / ✓ / ✓	– / ✓ / ✓ / – / ✓	– / ✓ / ✓ / – / –	✓ / ✓ / ✓ / – / ✓	– / ✓ / ✓ / – / ✓	✓ / ✓ / ✓ / – / ✓
	5 € / – / –	11 € / – / 59,88 €	9,29 € / – / 111,48 €[6]	10,99 US-$ /– / 79,99 US-$[7]	9 US-$ / 24 US-$ / 58 US-$	10,85 € / – / – ***	9 US-$ / – / 49 US-$

[7] 43,99 US-$ im ersten Jahr ✓ vorhanden – nicht vorhanden *** 37 € für 18 Monate

Bild: Andreas Martini

Übersicht gängiger VPN-Varianten

VPN ist nicht gleich VPN: Das eine mag nicht über IPv6 laufen, das andere ruckelt in Mobilnetzen. Der Blick auf die Details klärt, welche Technik für welche Situation am besten taugt. So findet man beim VPN-Provider das optimale Protokoll.

Von **Holger Zuleger**

Ein Virtual Private Network, kurz VPN, kennen alle, die sich aus dem Homeoffice mit einem meist mobilen Gerät in das Firmennetz einwählen. Dort bekommt man nach erfolgreicher Authentifizierung – der Anmeldung mit individuellen Zugangsdaten – Zugriff auf die gewohnte Arbeitsumgebung mit Drucker und Serverdiensten fast wie vor Ort. Da die VPN-Verbindung typischerweise über die Netze mehrerer Provider läuft, ist eine sichere Verschlüsselung unabdingbar, um Vertraulichkeitsvorgaben etwa aus der DSGVO einzuhalten.

Wer aus dem Homeoffice an den Arbeitsplatz zurückkehrt, vermisst nun vielleicht die heimische Netzumgebung. Dann liegt der Gedanke nahe, vom Arbeitsplatz aus mit den gleichen Techniken aufs Heimnetz zuzugreifen wie vorher umgekehrt. Im

Folgenden schildern wir, welche wichtigen Unterschiede es zwischen den VPN-Varianten gibt und welche Rolle die Netztopologie spielt.

Das Wissen um die Zusammenhänge erleichtert die Wahl des passenden VPNs. Denn neben der möglicherweise fehlenden Erlaubnis – viele Unternehmen sehen eine Verbindung aus dem Firmennetz heraus als kritische Sicherheitsverletzung – stehen dem Unterfangen häufig auch technische Gründe entgegen.

Schon Windows 95 und NT hatten einen Client für Microsofts **PPTP** (Point-to-Point Tunneling Protocol). Leider gelten die dort eingesetzten Verschlüsselungs- und Authentifizierungsverfahren seit mehr als einem Jahrzehnt als gebrochen und damit unsicher. Unmissverständlich ausgedrückt: Lassen Sie die Finger von PPTP, auch wenn es in Ihrem Router besonders bequem einzurichten oder gar das einzige angebotene VPN-Verfahren ist!

Als Alternative zu PPTP finden sich etwa in iOS und macOS allein drei Einwahlmethoden für **IPsec** (Internet Protocol Security), das seit Langem als sichere VPN-Methode gilt. Gründe für die IPsec-Vielfalt liegen in der historischen Entwicklung und darin, dass sich neue Standards – besonders in dem sich selbst gern als innovativ feiernden Netzwerkbusiness – nur sehr langsam durchsetzen.

IPsec wurde vor vielen Jahren als ergänzender IP-Header zur Verschlüsselung für IPv6 entwickelt. Damals gab es aber kaum IPv6-fähige Endgeräte und die Internetanbindungen waren ausschließlich für IPv4 ausgelegt. Folglich wurde IPsec für IPv4 zurückportiert – ohne dabei die Unterschiede beider Transportprotokolle gründlich zu beachten.

IPv6 hatte ab Werk einen Mechanismus zur IP-Adressautokonfiguration, IPv4 nicht. Deshalb musste anfangs – und auch heute manchmal noch – für die VPN-Einwahl die IPv4-Adresse des Geräts statisch konfiguriert werden. Das war bei den aufkommenden mobilen Endgeräten untragbar. So haben die IPsec-Entwickler nachgebessert und die damalige Authentifizierungsmethode IKEv1 (Internet Key Exchange) um Mechanismen zur IP-Autokonfiguration erweitert.

Mobil nachgeholt

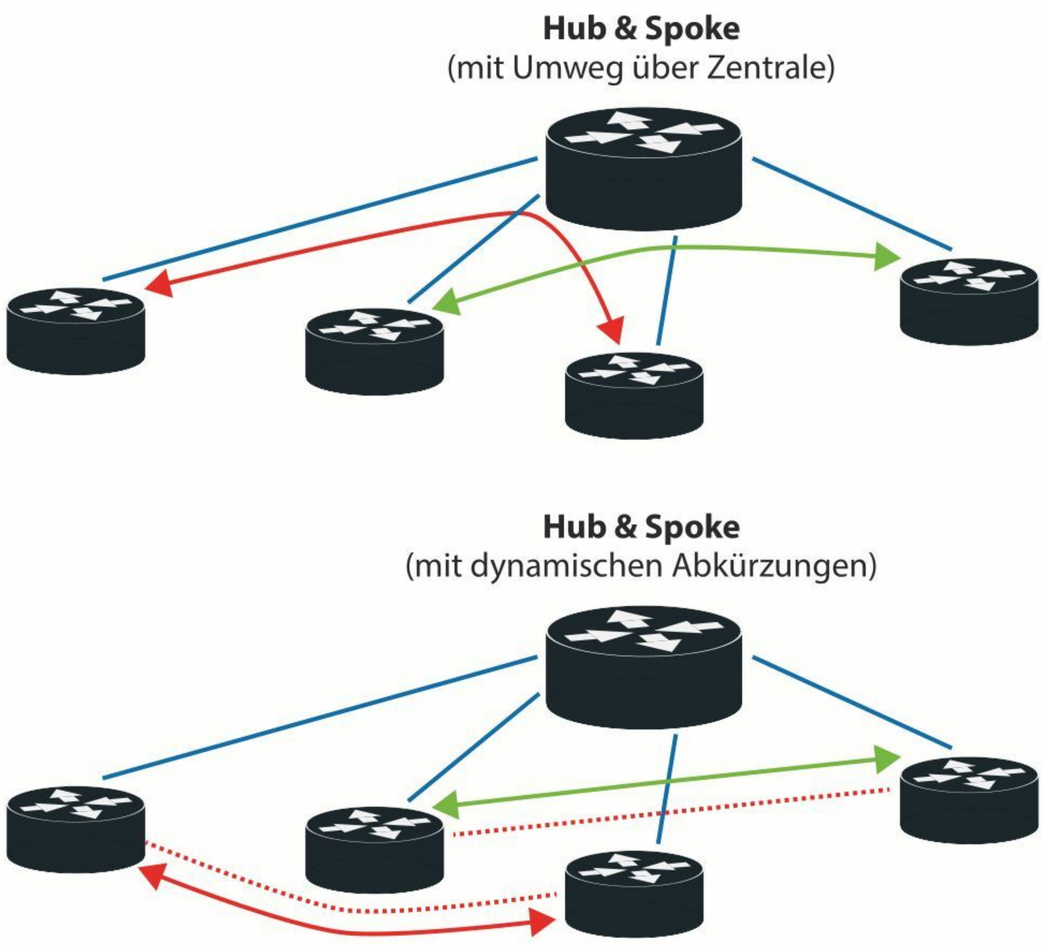
Ein weiteres Problem ergab sich aus der Authentifizierung der Geräte. Als IPsec entwickelt wurde, lag der Fokus auf der Standortvernetzung. Mobile Geräte gab es schlichtweg nicht. IPsec wurde bis dahin nur auf Gateways (Routern) eingesetzt, um Datenverkehr zwischen Standorten zu tunneln und dabei zu verschlüsseln.

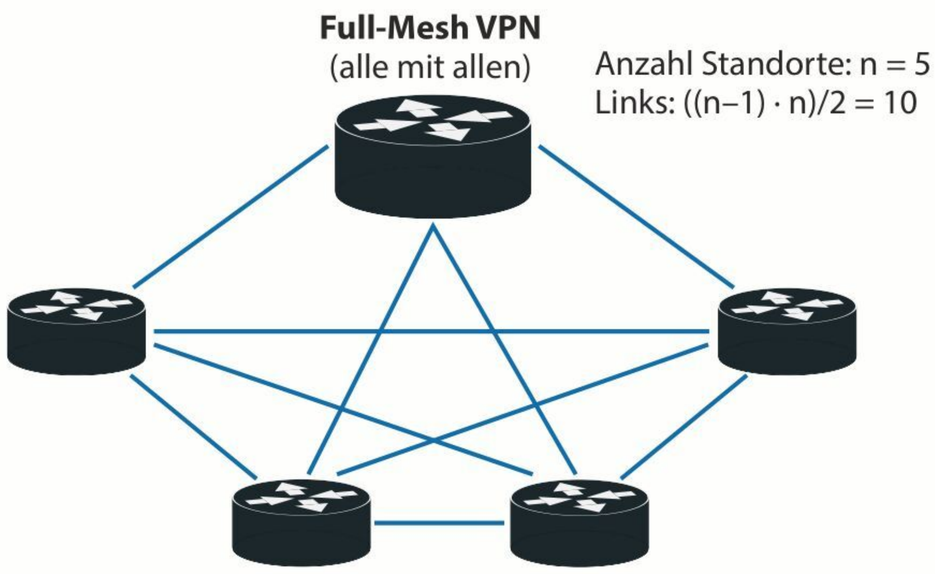
Die Gateways authentifizierten sich gegenseitig über Zertifikate. Für die aufkommenden, immer vielfältigeren mobilen Endgeräte war das aber zu unflexibel, da jedes Gerät ein eigenes Zertifikat benötigt.

Microsoft entwickelte mit dem oben erwähnten PPTP zwar sehr früh ein Protokoll, das zur Authentifizierung und Einwahl auf bekannte Verfahren aus

VPN-Vermaschung

Der Road-Warrior-Ansatz (VPN-Verbindung zur Zentrale à la Hub & Spoke, oben) funktioniert in Firmennetzen mit vielen Standorten wegen der doppelten Übertragungen schlecht. Voll vermaschte VPNs (unten) sind wegen der vielen Verbindungen aufwendig zu administrieren. Hub & Spoke mit dynamischem Linkaufbau hilft den Aufwand im Griff zu halten.





Modemzeiten zurückgreift. Es wurde jedoch bald durch ein Verfahren mit besseren Verschlüsselungskomponenten abgelöst: PPP (Point-to-Point Protocol) über L2TP (Layer 2 Tunneling Protocol) mit IPsec im Transport-Mode (siehe Kasten rechts).

Das Zusammenspiel verschiedener Protokolle bei L2TP/IPsec ist zwar komplex, hat gegenüber reinem IPsec aber mehrere Vorteile: Zum Transport dient L2TPv2, das auf UDP aufsetzt (User Datagram Protocol). Damit ist der Verbindungsaufbau NAT-freundlich (Network Address Translation, IPv4-Adressumschreibtechnik) und setzt zumindest auf einer Seite keine öffentliche IPv4-Adresse mehr voraus. Denn NAT-Router nutzen die von den Datenströmen verwendeten Ports zur eindeutigen Zuordnung der Kommunikationspartner. Bei reinen IPsec-Verbindungen stecken diese Informationen jedoch im verschlüsselten Tunnel und sind für den Router nicht erkennbar.

PPP über den Layer-2-Tunnel bringt einen Vorteil bei der Nutzerauthentifizierung: Sie lief historisch meist mit Name und Passwort, heutzutage mittels EAP (Extensible Authentication Protocol) über diverse andere Verfahren. So lässt sich bei L2TP/IPsec auch eine Gateway-seitige Zertifikatsauthentifizierung für die äußere Verschlüsselung mit vereinfachter PPP-Nutzerauthentifizierung innerhalb des Tunnels kombinieren.

Mit Einschränkungen

So praktisch und vielseitig die Lösung ist, kann sie heutzutage aber nicht mehr generell empfohlen werden: L2TPv2 ist nur für IPv4 als Transportprotokoll definiert und merkwürdigerweise auch nie für IPv6 umgesetzt worden. L2TP/IPSec kann deshalb zwar IPv6 als inneres Protokoll transportieren, der Tunnel selbst muss jedoch über IPv4 aufgebaut werden.

Ähnlich eigenwillig verhält sich IPsec mit IKEv1, wie es beispielsweise die verbreiteten Fritzboxen anbieten. Für jedes transportierte Protokoll (IPv4 oder IPv6) muss ein separater Tunnel mit dem gleichen

VPN-Topologien

Das klassische Road-Warrior-Szenario – ein Gerät verbindet sich per VPN mit der Firmenzentrale – arbeitet in derselben Topologie, die man bei VPN-Dienstleistern findet: Hub & Spoke, also Nabe (Zentrale) und Speichen (Geräte beziehungsweise Fernarbeitende) eines gedachten Rades.

Wenn Firmen ihre Standorte so vernetzen, dann läuft der Verkehr zwischen zwei Niederlassungen immer über die Zentrale. Der Nachteil ist offensichtlich eine Doppelbelastung der VPN-Verbindungen und damit der Internetanbindung. Durch einen VPN-Tunnel läuft nun auch nicht mehr nur der Verkehr des Road-Warriors, sondern der vieler Geräte auf beiden Seiten.

Um die Verkehrsverdopplung zu vermeiden, setzen manche Unternehmen auf ein voll vermaschtes VPN (Full Mesh), in dem jede Niederlassung direkt mit allen anderen Stationen kommunizieren kann. Was die Anbindung der Zentrale entlastet, verkompliziert aber den VPN-Aufbau, steigt doch die Zahl der Tunnel überproportional mit der Zahl der Niederlassungen: Drei Standorte lassen sich mit ebenso vielen VPN-Verbindungen vernetzen. Vier benötigen jedoch schon sechs Tunnel, fünf Standorte gar zehn und bei 10 Standorten müssen ganze 45 Tunnel eingerichtet und überwacht werden.

Als Alternative bieten sich VPNs an, die anfangs als Hub & Spoke konfiguriert werden. Damit steigt die Tunnelzahl nur linear. Wollen zwei Außenstellen kommunizieren, dann errichtet das System dynamisch einen neuen Tunnel zwischen ihnen. Cisco hat das unter dem Namen DMVPN (Dynamic Multipoint VPN) entwickelt. Es basiert auf IPsec in Kombination mit dem Next Hop Routing Protocol (NHRP) und GRE-Tunneln (Generic Routing Encapsulation). Eine vergleichbare, aber technisch völlig anders realisierte Open-Source-Lösung für Full-Mesh-VPN ist Tinc.

L2TP/IPsec

Klassisches IPsec, gleich ob IKEv1 oder IKEv2, verwendet auch bei der Remote-Einwahl IPsec im Tunnel-Modus. Dabei wird ein zweiter äußerer IP-Header vor das eigentliche IP-Datenpaket geschnallt und dieser mit dem Verschlüsselungsheader von IPsec versehen (ESP, Encapsulating Security Payload).

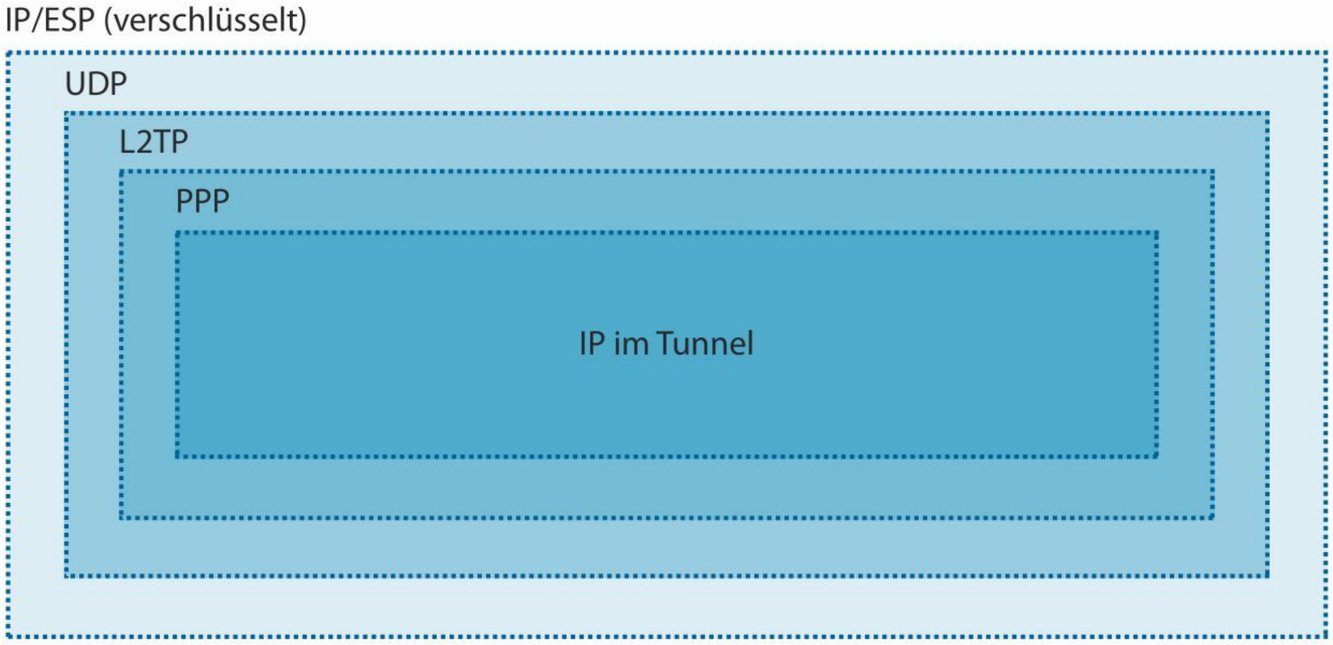
Der VPN-Client muss mit zwei IP-Adressen umgehen, einer aus dem Fremdnetz auf dem physischen Interface und einer zweiten virtuellen aus dem Heimatnetz, die ihm bei der Einwahl zugewiesen wurde. Die getunnelten Datenpakete gehen an das Remote-VPN-Gateway, das diese entschlüsselt, den äußeren Transport-Header entfernt und sie dann wie normale Pakete im internen Netz weiterleitet.

Bei dem oft mit IPsec kombinierten L2TP sieht der Aufbau komplett anders aus: Der VPN-Client baut zum VPN-Gateway eine L2TP-Verbindung auf und nutzt UDP auf Port 1701 als Transportprotokoll. So entsteht ein Layer-2-Tunnel, innerhalb dessen die Geräte wie früher zu Modemzeiten eine PPP-Verbindung aufbauen.

PPP erledigt das Authentifizieren der Benutzer, meist gegen einen Radius-Server. Der Client bekommt im Tunnel eine IPv4-Adresse und einen oder zwei DNS-Server aus dem Heimnetz zugewiesen. Außen drumherum verschlüsselt IPsec im Transport-Mode schließlich den L2TP-UDP-Verkehr. Das Verkapseln kostet 40 Byte, die Verschlüsselung außen nochmal zirka 50 Byte.

L2TP/IPsec-Verschachtelung

VPNs verpacken die zu schützenden Daten matroschkamäßig in mindestens zwei zusätzliche äußere Protokollschichten. L2TP/IPsec treibt das mit vier Hüllen auf die Spitze.



Transportprotokoll aufgebaut werden. Für Dual-Stack im Firmennetz wären demnach zwei Tunnel nötig.

Wegen der Adressknappheit bei IPv4 werden Internetanschlüsse zwar vermehrt parallel mit IPv6 ausgestattet. Privatkunden bekommen aber oft gar keine öffentliche IPv4-Adresse mehr. Nutzer von Internet per TV-Kabel und manchen Glasfaser-Anbietern können ein traurig Lied davon singen. Wegen des Provider-NAT muss man für den Betrieb extern erreichbarer Server im eigenen Netz nicht nur Klimmzüge machen [1, 2], sondern es steht auch häufig klassischen IPsec-Verbindungen im Weg. Selbst

wenn das Gegenüber, der Peer, eine öffentliche IPv4-Adresse hat, funktioniert IPsec mit IKEv1 und L2TP an solchen Anschlüssen nicht jederzeit stabil.

Aufgeräumt

IPsec Version 2 (IKEv2) soll all diese Probleme lösen. Es bringt unterschiedliche Authentifizierungsverfahren über EAP, NAT-Traversal, Dead Peer Detection zur Ausfallerkennung, IP-Autokonfiguration sowie nicht zuletzt IPv4-über-IPv6-Transport und umgekehrt.

Damit, sollte man meinen, kommt man auch als Internet-Nomade immer ins Heim- oder Firmennetz. Für Privatkundenanschlüsse stimmt das. In Firmennetzen steht jedoch meist eine Firewall am Internetzugangspunkt. Diese kontrolliert nicht nur den eingehenden, sondern häufig auch den ausgehenden Verkehr. IPsec-Verbindungen aus dem Firmennetz in Richtung Internet gelten gerne mal als suspekt und werden unterbunden.

Ähnliche Einschränkungen finden sich auch bei manchem WLAN-Hotspot oder bei Gastzugängen. Letztere lassen sich beispielsweise bei den verbreiteten Fritzboxen auf Surfen und Mailen begrenzen.

Die neuen Wilden

Durch die oben angesprochenen Probleme befeuert, kamen schon früh Alternativen zu IPsec auf. Diese arbeiten nicht auf Ebene 3 (IP) des OSI-Stacks, sondern auf der Transportebene 4 (TCP, Transmission Control Protocol, oder UDP).

OpenVPN zählt zu den ersten solcher VPNs und ist eine inzwischen weitverbreitete Open-Source-Implementierung. Die Peers authentifizieren sich über eine TLS-Verbindung (Transport Layer Security), ähnlich wie man es von HTTPS kennt, und tauschen darüber auch ihre Schlüssel aus. Die zu transportierenden Daten erhalten einen proprietären Verschlüsselungsheader und werden in UDP-Pakete verpackt. Das vermeidet die von reinen IPsec-Verbindungen bekannten NAT-Probleme. Wenn der VPN-Tunnel über UDP scheitert, kann OpenVPN per Konfigurationseingriff dafür auf HTTPS wechseln.

Das OpenVPN-Konzept war so erfolgreich, dass schnell Nachahmer auf den Plan traten, wenn auch für andere Anwendungsbereiche: **Tinc** soll besonders gut für VPNs mit sehr vielen Standorten skalieren. Es kommt bei Overlay-Community-Netzwerken wie etwa dem Freifunk-InterCity-VPN zum Einsatz.

OpenConnect soll in möglichst allen Netzwerksituationen einen verschlüsselten Tunnel errichten können: Es baut anfangs eine HTTPS-Verbindung zum VPN-Gateway auf, notfalls über einen Proxy. Darüber authentifizieren sich die Gegenstellen und tauschen ihre Schlüssel. Die Datenverbindung versucht OpenConnect dann über einen DTLS-gesicherten UDP-Link zum Gateway herzustellen (Datagram Transport Layer Security: TLS-Äquivalent für UDP). Blockiert eine Firewall den UDP-Tunnel, nutzt OpenConnect die bestehende HTTPS-Verbindung. Sie ist zwar nicht so performant, funktioniert aber in so gut wie allen Umgebungen.

VPN-Wunderkind

Das jüngste Kind im Reigen der VPN-Techniken heißt **Wire Guard**. Es wurde konsequent auf Einfachheit und damit auf Geschwindigkeit getrimmt. Ein einziger, nicht änderbarer Schlüsselalgorithmus einhergehend mit nur einem Authentifizierungsverfahren (Public/Private Key) spart nicht nur Programmcode, sondern baut auch die Verbindung wesentlich schneller auf, weil keine Verschlüsselungsparameter ausgehandelt werden müssen.

Zudem findet der IP-Transport inklusive Ein- und Auspacken der Verschlüsselungsheader bei Linux-Implementierungen komplett im Kernel statt. Daraus ergibt sich ein immenser Geschwindigkeitsvorteil gegenüber den anderen Nicht-IPsec-Verfahren. Ferner klappt das Authentifizieren der Gegenstellen unabhängig von deren IP-Adresse. So werden wechselnde IP-Adressen nicht zum Security-Problem und WireGuard funktioniert problemlos an Internetanschlüssen mit dynamischer Adresszuteilung, sogar mobil mit LTE-Routern.

WireGuard bringt auf manchen Plattformen zwar deutlich mehr Geschwindigkeit als IPsec [3], doch spielen für die Einzelplatzeinwahl auch andere Eigenschaften eine Rolle, beispielsweise Optionen für die Nutzerauthentifizierung.

Bekannte Fernarbeiter

Kleine Firmen-VPN-Verbünde lassen sich oft noch in „Handarbeit“ administrieren. Wenn sich aber eine größere Zahl Beschäftigte einwählen soll, müssen die VPN-Verfahren ein gut skalierendes Authentifizierungsverfahren mitbringen, das einen zentralen Server befragt.

In Windows-Netzen ist das der Domänencontroller, der das Active Directory führt. Radius-Server haben auch Vorzüge: Beispielsweise erlauben sie mehrere Einwahl-Gateways, um den Verkehr zu ver-

teilen oder Redundanz vorzuhalten, ohne die Nutzerdatenbank zu duplizieren. Zentrale Benutzersperren, zeitliche Einwahlbeschränkungen, nutzerspezifische Access-Listen und weitere Individualisierungsoptionen erhält man obendrauf.

OpenVPN und OpenConnect unterstützen viele Authentifizierungsmethoden (siehe Tabelle unten). Gerade bei Linux/Unix-Systemen lassen sich zusätzliche Verfahren wie etwa eine Zwei-Faktor-Authentifizierung ohne großen Aufwand über das PAM-API integrieren (Pluggable Authentication Modules).

Im Heimnetz genügen hingegen im Router hinterlegte Zugangsdaten (Nutzername, Passwort, optional zusätzlicher Pre-Shared Key) oder ein Public / Private-Key-Verfahren wie bei WireGuard.

Transporter

Jenseits von IPsec – doch selbst dort, wenn NAT-Traversal gebraucht wird – dient stets UDP als Spediteur, mal mit proprietärer Verschlüsselung, mal mit DTLS, oft verknüpft mit einer TLS-Authentifizierungssitzung.

Manche Protokolle schalten bei Problemen mit dem UDP-Transport auf TCP (OpenVPN) oder HTTPS über TCP um (OpenConnect). Dadurch sinkt zwar die Performance, aber die Verfügbarkeit verbessert sich.

IPv6 sollte heute ebenso als Trägerprotokoll wie auch als im Tunnel transportiertes Protokoll möglich sein. Erstens stellen viele Internetanschlüsse keine öffentliche IPv4-Adresse mehr bereit, was – siehe NAT-Problematik oben – stabile VPN-Verbindungen verhindert. Zweitens wird IPv6 längst in vielen Netzen genutzt: Im Sommer 2021 fiel der tageszeitlich schwankende IPv6-Anteil auf heise.de nicht mehr unter 30 Prozent. Google meldete für Deutschland 52 Prozent IPv6-Verfügbarkeit (siehe google.com/ipv6, Österreich: 17 Prozent, Schweiz: 34 Prozent).

Einer der Vorteile von IPv6: Es kann kein Problem mit überlappenden Adressbereichen im VPN entstehen. Bei IPv4 drohen hingegen Kollisionen, wenn im Ziel- und im gerade besuchten Netz der gleiche private Adressblock genutzt wird. Beispielsweise stellen wohl nur wenige Fritzbox-Nutzer die Werksvorgabe 192.168.178.0/24 auf einen anderen Bereich um.

So gesehen sind sowohl IPsec mit IKEv1 als auch die beliebte L2TP/IPsec-Kombination nicht mehr zeitgemäß. Bei den Alternativen ist inzwischen selbst der Oldie OpenVPN voll IPv6-tauglich. Die jüngeren Konkurrenten waren dies ab Start.

Fazit

Profis, die VPNs zur Standortvernetzung einsetzen, schätzen tinc und WireGuard. Für die Auswahl eines VPN-Providers für Endkunden ergibt sich eine andere Rangfolge: WireGuard glänzt bei der Geschwindigkeit und auf mobilen Clients. IPsec spielt dann seine Vorteile aus, wenn es ohne speziellen Client gehen soll. OpenConnect trumpft dann auf, wenn es widrige Netze zu überwinden gilt. Das verbreitete OpenVPN bleibt als die Universallösung, falls die anderen versagen. (ea) c't

Literatur

[1] Reiko Kaps, **Mauerspechte**, Internet-Dienste trotz DS-Lite nutzen, c't 6/2013, S. 178

[2] Ernst Ahlers, **Server-Umleitung**, Heimserver hinter DS-Lite oder CG-NAT erreichbar machen, c't 2/2018, S. 138

[3] Andrijan Möcker, **Fritz'scher Ausblick**, WireGuard-VPN: Was moderne Fritzboxen leisten (könnten), c't 14/2020, S. 130

VPN-Typen und ihre Eigenschaften

VPN	IPsec	L2TP/IPsec	OpenConnect	OpenVPN	Tinc	WireGuard
Einwahl / Vernetzung	✓ / ✓	✓ / –	✓ / –	✓ / ✓	– / ✓	✓ / ✓
Hub & Spoke / Full Mesh	✓ / ✓[1]	✓ / –	✓ / –	✓ / ✓[1]	✓ / ✓	✓ / ✓[1]
Verschlüsselung	IPsec	IPsec	HTTPS, DTLS	proprietär	proprietär	proprietär
Clients	alle OS	alle OS	Linux, iOS, Android[2]	alle OS	Linux, Windows	Linux[3]
IPv6-Transport	✓[4]	–	✓	✓	✓	✓
Ethernet-Bridging	–	–	–	✓	✓	–
Authentifizierung						
Zertifikate oder asym. Keys	✓	✓	✓	✓	✓	✓
Pre-Shared Key	✓	✓	✓	✓	✓	✓
Radius	nur mit IKEv2	✓	✓	✓	–	–
Windows AD (Kerberos)	nur mit IKEv2	✓	✓	–	–	–
Zwei-Faktor-Authentifizierung	✓	✓[5]	✓	✓[6]	–	–

[1] kleine Anzahl Standorte, da nur manuell konfigurierbar [2] kommerzielle Versionen für macOS und Windows erhältlich [3] originär für Linux-Kernel entwickelt, im Userspace auch für macOS, Windows, iOS und Android [4] bei IKEv1 kein Mixmode [5] implementierungsabhängig [6] über PAM-Oath-Modul ✓ vorhanden – nicht vorhanden

Hacking-Tools als Problemlöser

Gefährlich, nützlich – oder beides? c’t hat Hacking-Tools ausprobiert, um diese Frage zu klären. Viele entpuppten sich als Problemlöser und können auch Ihnen gute Dienste leisten, etwa um vergessene Passwörter zu knacken, Dateien zu retten oder das Netzwerk auf Sicherheitslücken abzuklopfen.

Von **Ronald Eikenberg**

Bild: Sven Hauth

Hacking-Tools als Problemlöser	104
Nützliche Hacking-Tools für den Alltag	106
Hacking-Werkzeug für Fortgeschrittene	114
Kali Linux auf USB-Stick einrichten	122
Rechtliche Aspekte bei Hacking-Tools	128
NitroPC: Mini-PC mit Security-Plus	134

Wer Hacker sagt, meint häufig Kriminelle, die unberechtigt Daten kopieren und veröffentlichen. Diese Black-Hats, benannt nach den bösen Cowboys mit schwarzen Hüten aus alten Wildwestfilmen, handeln mit gestohlenen Daten oder betrügen auf Kosten ihrer Mitmenschen. Doch es gibt auch Hacker, die ihr Know-how legal und moralisch einwandfrei einsetzen. Diese White-Hats sind gefragte Leute, sie spüren zum Beispiel als gut bezahlte Penetrationstester (Pentester) Sicherheitslücken für Unternehmen auf.

Allen Hackern gemein ist, neben ihrem technischen Know-how, dass sie sich die Arbeit oft mit speziellen Programmen erleichtern, um viele Aufgaben überhaupt erst erledigen zu können. Viele dieser Hacking-Tools sind frei verfügbar und völlig legitim einsetzbar – es besteht daher kein Grund, sie zu verteufeln. Es spricht sogar vieles dafür, die Tools selbst zu benutzen und damit die Sicherheit der eigenen Rechner, Router & Co. zu untersuchen – oder die eines Auftraggebers. Wer damit jedoch gegen geltende Gesetze verstößt und fremde Systeme attackiert, macht sich natürlich strafbar. Eine fundierte Einordnung der rechtlichen Lage finden Sie auf Seite 128.

Retter in der Not

Wir haben zahlreiche Hacking-Tools ausprobiert und stellen in dieser Ausgabe eine Auswahl der interessantesten Programme vor, die sogar das Zeug zum Retter in der Not haben. Viele der Hacking-Tools starten direkt unter Windows und sind dank einer grafischen Bedienoberfläche verhältnismäßig leicht bedienbar, während andere alle Klischees erfüllen und nur auf der textbasierten Linux-Shell laufen. Wir möchten Ihnen die ganze Bandbreite zeigen: Im folgenden Artikel finden Sie nützliche Helfer für den Windows-Alltag mit konkreten Tipps zur Verwendung. Ist zum Beispiel die Abgabe der Bachelorarbeit gefährdet, weil Sie das Passwort der Word-Datei vergessen haben, setzen Sie doch mal den Passwortknacker **John the Ripper** darauf an. Mehr dazu lesen Sie auf Seite 108. Haben Sie sich aus Ihrem Windows ausgesperrt, setzen Sie das Passwort mit dem **Windows Login Unlocker** einfach zurück. Auf Seite 107 erfahren Sie wie.

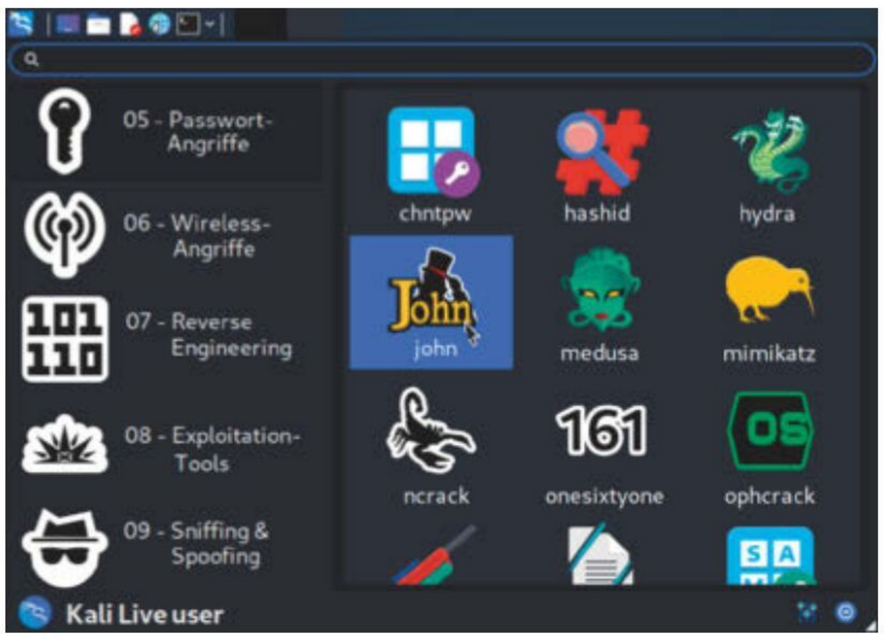
Sie helfen Ihren Schwiegereltern beim Umstieg auf einen neuen PC, aber das vor Jahren eingerichtete WLAN-Passwort ist nicht mehr auffindbar? Mit Tools wie **LaZagne** (S. 108) lesen Sie es vom alten Rechner aus und exportieren dabei gleich noch viele andere Zugangsdaten, die sich dort im Laufe der Zeit angesammelt haben und den Umzug beschleunigen. Auf Seite 110 zeigen wir außerdem, wie Sie vermeintlich unrettbar verlorene Dateien wieder ans Tageslicht befördern.

Security-Check

Ab Seite 114 geht es etwas härter zur Sache mit Spezialtools, mit denen zwar nicht jeder etwas anfangen kann, die jedoch erstaunliche Fähigkeiten haben. Mit dem vielseitigen Netzwerkscanner **Nmap** (S. 108) verschaffen Sie sich schnell einen Überblick über die Situation in Ihrem Netzwerk und entdecken vielleicht auch den Nachbarn, der seit der letzten Party immer noch im WLAN mitsurft. Im gleichen Durchgang können Sie Ihre Geräte auf Sicherheitsprobleme abklopfen.

WordPress-Websites stehen unter Dauerfeuer, weil Angreifer nur zu gut wissen, dass ein verpenntes Sicherheits-Update ausreicht, um den ganzen Server zu übernehmen. Auch veraltete und verwundbare Erweiterungen sind schon vielen WordPress-Betreibern zum Verhängnis geworden. Wenn Sie das gleiche Werkzeug wie die Angreifer nutzen, spüren Sie etwaige Sicherheitslücken rechtzeitig auf und können Gegenmaßnahmen ergreifen, bevor Ihre Daten im Darknet gehandelt werden. Blättern Sie hierfür zu **WPScan** auf Seite 117.

Last, but not least, zeigen wir Ihnen ab Seite 122, wie Sie sich einen bootfähigen Hacking-Stick erstellen. Als Grundlage dient **Kali Linux**, das etliche Security-Tools enthält, die Sie direkt ausprobieren können. Alles, was Sie brauchen, ist ein USB-Stick mit mindestens 8 GByte und etwas Zeit. Manche der Tools sind zwar etwas unhandlich, von dem gewonnenen Fachwissen können Sie jedoch lange profitieren. Genau das Richtige für verregnete Tage. (rei) c't



Machen Sie Bekanntschaft mit Hydra, Medusa und John the Ripper: Hacking-Tools mit gefährlich klingenden Namen sind, richtig eingesetzt, echte Problemlöser.

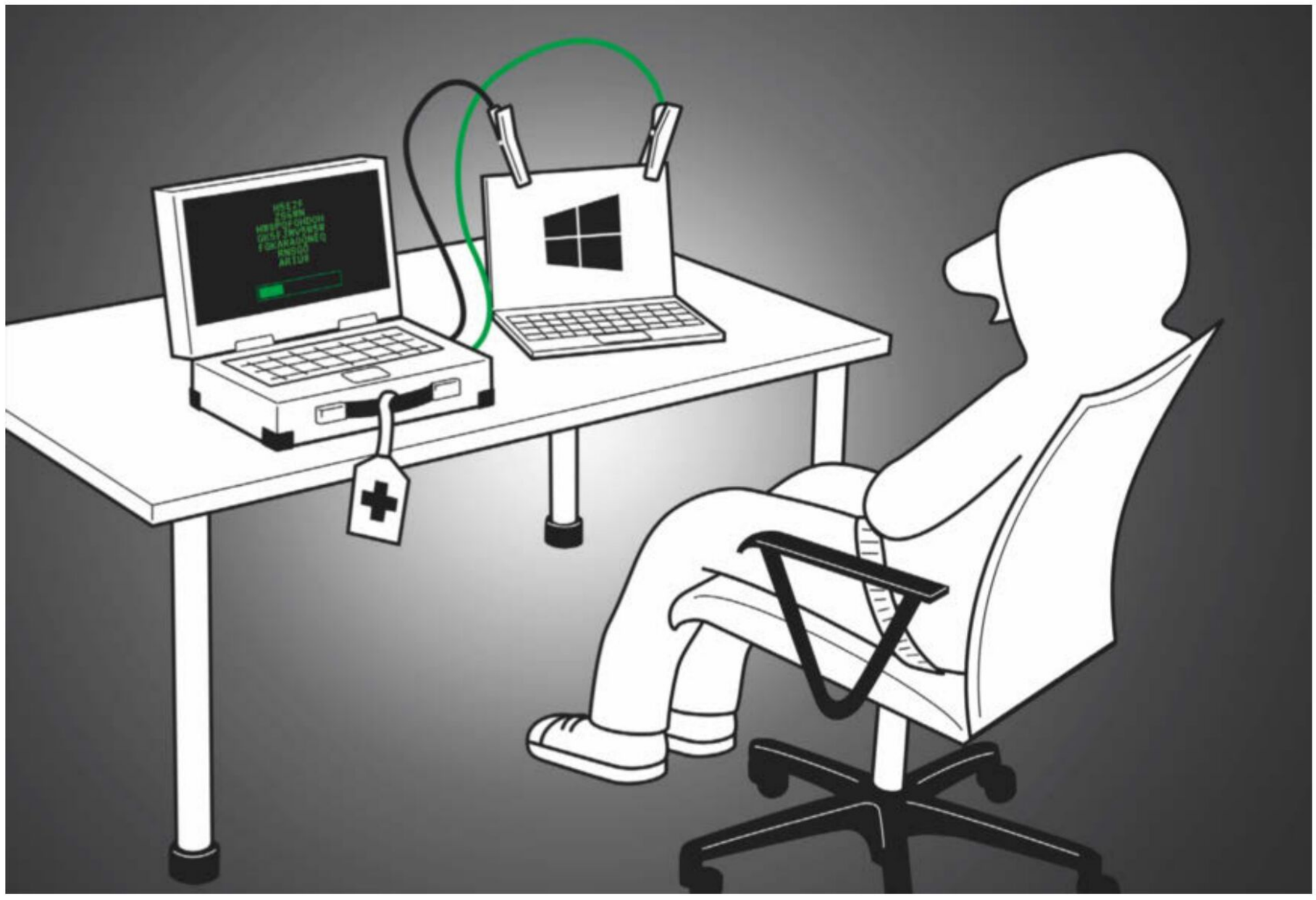


Bild: Sven Hauth

Nützliche Hacking-Tools für den Alltag

Haben Sie schon mal ein Passwort vergessen oder wichtige Dateien versehentlich gelöscht? Statt darüber zu fluchen, können Sie sich oftmals einfach selbst helfen: Schlüpfen Sie in die Rolle eines Hackers und verschaffen Sie sich wieder Zugriff auf Ihre Daten – ganz legal.

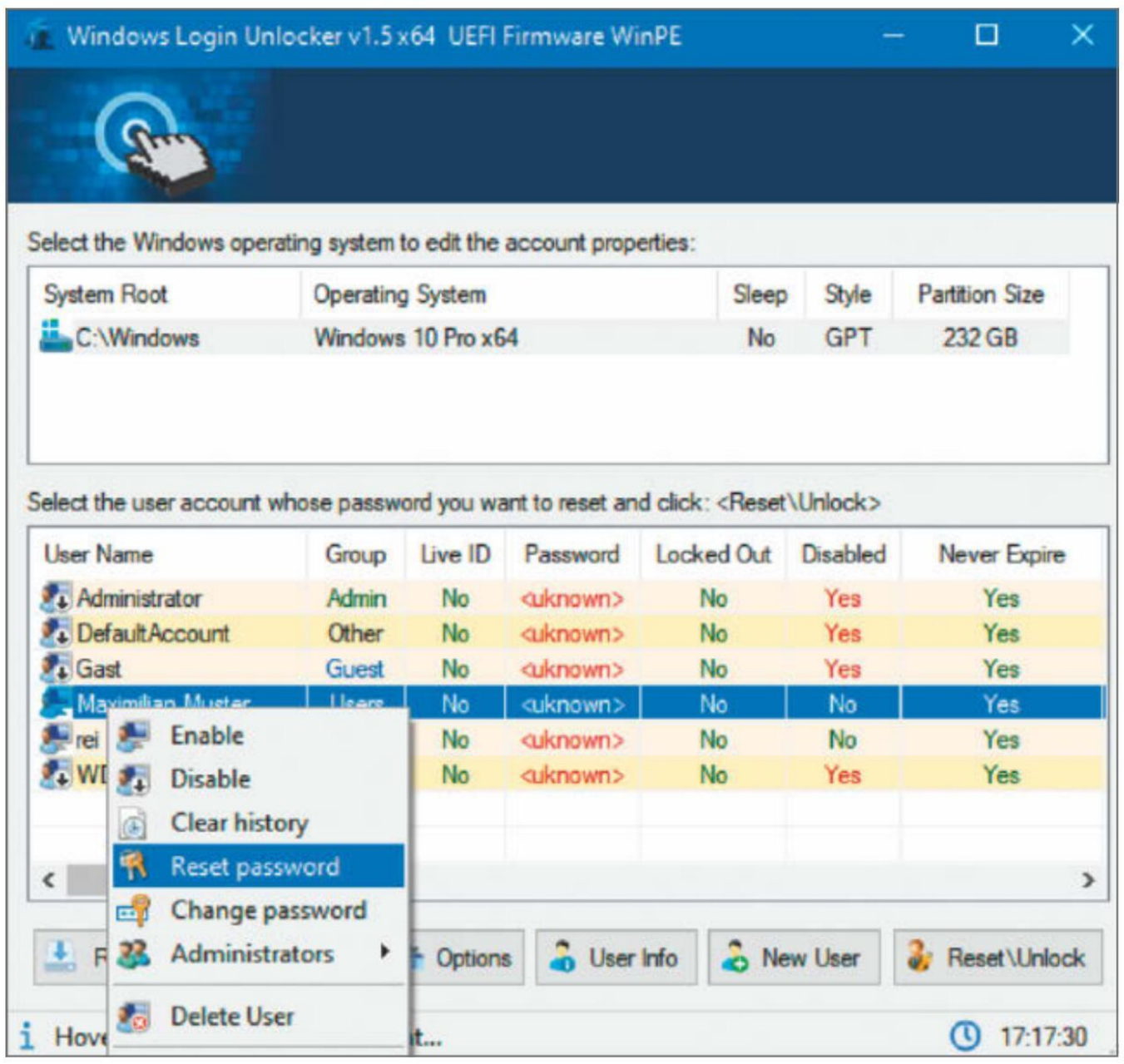
Von **Ronald Eikenberg und Alexander Königstein**

Hacken Sie Ihren eigenen Rechner: Was erstmal absurd klingt, kann Ihnen das Leben mit der Technik erheblich erleichtern. Denn mit den Werkzeugen der Hacker erledigen Sie nicht nur vieles schneller, Sie können damit auch echte Alltagsprobleme lösen und sich aus der Patsche helfen. Nicht alle Hacking-Tools sind automatisch böse, oftmals handelt es sich um harmlose, aber äußerst nützliche Programme, die spezielle Aufgaben besonders gut oder effektiv lösen.

Bei Hackerangriffen ist keine schwarze Magie im Spiel, häufig sind es frei verfügbare Open-Source-

Tools, die für sich genommen nicht gefährlich sind. Nach einer Infektion werden sie nachgeladen und automatisiert ausgeführt, um zum Beispiel Dateien oder Passwörter erstmal lokal einzusammeln. Ausgeleitet werden die Daten erst vom eigentlichen Schadcode (oder einem weiteren Tool). Andere Open-Source-Tools laufen direkt bei den Hackern, um zum Beispiel verschlüsselte Daten zu knacken oder gelöschte Dateien zu rekonstruieren.

Die missbräuchlich eingesetzten Werkzeuge werden von vielen Virenwächtern als „HackTool“ erkannt, weshalb den nützlichen Systemhelfern zu Unrecht ein schlechter Ruf anhaftet. Um das zu ändern, stellen wir Ihnen in diesem Artikel einige „Hacking-Tools“ vor, die sich bei uns bewährt haben. Wenn Sie sich erstmal langsam herantasten möchten, können Sie Programme gefahrlos in einer virtuellen Maschine oder auf einem ausgemusterten PC ausprobieren. Die Download-Links zu allen Tools sowie Verweise auf weiterführende c’t-Artikel finden Sie unter ct.de/wn7d.



Windows-Passwort vergessen? Mit dem Windows Login Unlocker setzen Sie es einfach zurück.

Windows-Passwort zurücksetzen

Anmelden klappt nicht, weil Windows-Passwort vergessen? Kann ja mal passieren. Wenn alle möglichen und unmöglichen Kennwörter durchprobiert sind und auch die Recovery-Fragen nicht weiterhelfen, ist guter Rat teuer. Eine Neuinstallation wäre naheliegend – ist jedoch meist gar nicht nötig. Ist die Systemplatte nicht verschlüsselt, können Sie das alte Passwort, genauer gesagt dessen Hash, einfach überschreiben. Doch Achtung: EFS-verschlüsselte Dateien lassen sich nach dieser Prozedur aus Sicherheitsgründen nicht mehr entschlüsseln (Das Encrypting File System, kurz EFS, ist die transparente Dateiverschlüsselung von NTFS). Der Hash liegt im Registry-Zweig des Security Accounts Managers (SAM), wobei es sich letztlich nur um eine Datei auf der Platte (c:\windows\system32\config\sam) handelt. Die ist allerdings im laufenden Betrieb stets von Windows geöffnet, sodass Sie sie nicht einfach so bearbeiten können.

Mit dem **Windows Login Unlocker** aus dem c’t-Notfall-Windows können Sie das Windows-Passwort dennoch zurücksetzen. Sie booten den Rechner vom Stick und der Unlocker übernimmt alle nötigen Schritte für Sie. Mit dem Tool können Sie das Passwort nicht nur zurücksetzen oder gleich ganz entfernen, sie können damit auch Konten anlegen und löschen. Der Unlocker entsperrt sogar Accounts, die mit einem Microsoft-Konto verknüpft sind. Solche werden dabei in ein lokales Benutzerkonto umgewandelt. Einen bootfähigen USB-Stick mit dem Notfall-Windows und dem Unlock-Tool können Sie mit unserer Anleitung in c’t 26/2020 leicht selbst erstellen, alle nötigen Dateien gibt es kostenlos zum Download (siehe ct.de/wn7d). Sie finden das Tool im Notfall-Windows unter „Start/Datenrettung“.

Die Bedienung des Unlockers erklärt sich fast von selbst: Oben listet er die gefundenen Windows-Installationen auf, zum Beispiel `c:\Windows`. Wählen Sie die passende und darunter das Windows-Konto, das Sie retten möchten. Nach einem Rechtsklick haben Sie diverse Möglichkeiten, von denen Sie entweder „Reset“ oder „Change password“ wählen. Die Änderung ist beim nächsten regulären Hochfahren ohne Stick aktiv und Sie können sich wieder einloggen. Alternativ können Sie das etablierte Open-Source-Tool „chntpw“ nutzen, das auch unter Linux läuft. Es ist in Kali Linux (siehe Seite 122) bereits enthalten.

Ist das Windows-Konto mit einem Microsoft-Account verknüpft, können Sie es mit chntpw jedoch nicht entsperren.

Nach der Rettungsaktion ist das Windows wieder wie gewohnt nutzbar, allerdings mit einer Ausnahme: Daten, die über die Windows-Funktion `CryptProtectData()` verschlüsselt gespeichert wurden, können Sie weiterhin nicht entschlüsseln, da dazu das ursprüngliche Passwort nötig ist. Hiervon sind zum Beispiel die Passwortspeicher einiger Browser und durch Windows verschlüsselte Dateien (EFS, siehe oben) betroffen, nicht aber Bitlocker.

Das Unlock-Tool demonstriert anschaulich, dass ein Windows-Konto kein wirksamer Zugriffsschutz ist. Wenn Sie unbefugte Zugriffe verhindern möchten, sollten Sie Ihre Laufwerke zum Beispiel mit BitLocker oder VeraCrypt verschlüsseln. Dann sind nur nicht Ihre Dateien geschützt, sondern auch die Windows-Installation samt Passwort-Hashes (SAM). Das Entschlüsselungskennwort sollten Sie jedoch besser nicht vergessen.

Zugangsdaten einsammeln

Im Laufe eines Windows-Lebens sammeln sich etliche Zugangsdaten im System an, zum Beispiel im Browser, Mail-Client, VPN-Programm, aber auch alle WLAN-Kennwörter. Auf diese Datenbeute haben es üble Zeitgenossen natürlich abgesehen. Sie nutzen spezielle Programme, um die gespeicherten Logins in Sekundenschnelle einzusammeln. Solche Tools sind für sich genommen völlig harmlos, denn sie übertragen die gefundenen Zugangsdaten nicht, sondern zeigen sie lediglich an und können sie in eine Datei exportieren. Das kann im Alltag sehr nützlich sein, etwa um Zugangsdaten aus einer alten Windows-Installation zu retten, bevor man das System neu aufsetzt.

Schauen Sie sich zunächst im NirSoft-Fundus um: Hier finden Sie Password-Recovery-Tools für fast jeden Zweck, darunter **WebBrowserPassView**, das die Passwortspeicher der gängigsten Browser ausliest. **Mail PassView** liest Zugangsdaten aus Mail-Clients, **VaultPasswordView** aus der Windows-Anmeldeinformationsverwaltung und so weiter. Einen interessanten Zusatznutzen hat das Tool **WirelessKeyView**: Es zeigt nicht nur die im System gespeicherten WLAN-Zugangsdaten an, es kann daraus auch QR-Codes generieren, mit denen Sie Smartphones und Tablets schnell in Ihr WLAN helfen.

Die NirSoft-Tools sind leicht zu bedienen, da ihr Funktionsumfang überschaubar ist. Möchte Sie sich einen Überblick über die Gesamtsituation verschaffen, können Sie zum Python-Tool **LaZagne** greifen, das in einem Durchgang viele Speicherorte von Betriebssystem und Anwendungen durchforstet. Es wird selbst unter Linux und macOS fündig. Laden Sie das Tool am besten als Python-Skriptsammlung (Zip-Datei) von GitHub herunter – es existiert zwar eine direkt ausführbare Windows-Datei, diese konnten wir auf unseren Systemen jedoch nicht starten.

Falls nicht vorhanden, installieren Sie zuerst den Python-Interpreter. Unter Windows aktivieren Sie „Add Python to PATH“ und melden sich nach der Installation neu an, damit die folgenden Befehle funktionieren. Entpacken Sie das Zip-Archiv von LaZagne und installieren Sie mithilfe der Datei requirements.txt alle nötigen Python-Module: `pip install -r requirements.txt`. Anschließend wechseln Sie in das Verzeichnis, das zu Ihrem Betriebssystem passt (etwa „Windows“) und können dort LaZagne mit dem folgenden Befehl ausführen: `python laZagne.py all` Durch das „all“ führt LaZagne sämtliche vorhandenen Analysemodule aus. Wenn Sie es weglassen, erhalten Sie eine Übersicht über die möglichen Befehle.

Hat alles geklappt, liefert Ihnen das Tool eine lange Liste mit Zugangsdaten, Hashes et cetera – abhängig davon, was es auf Ihrem System zu holen gibt. LaZagne kann vieles mit den Rechten eines Standardnutzers auslesen, für manche Dinge – etwa WLAN-Passwörter – benötigt es jedoch Adminzugriff. Falls Sie das ausprobieren möchten, können Sie unter Windows die Eingabeaufforderung per Rechtsklick als Admin öffnen und anschließend LaZagne wie oben beschrieben starten.

Passwörter knacken

Passwortgeschützte Zip-Dateien sind ein einfaches und bewährtes Mittel, um Dateien zu verschlüsseln und so vor neugierigen Blicken zu schützen. Man kann sie fast überall mit Bordmitteln öffnen – sofern man sich noch an das richtige Passwort erinnert. Als Retter in der Not kann der legendäre Passwortknacker **John the Ripper** einspringen. Er versucht, das Passwort durch Durchprobieren zu erraten. Die Erfolgschancen stehen und fallen mit der Länge des Kennworts. Ist es recht kurz, wird John mit etwas Glück schon nach wenigen Sekunden fündig, bei sehr langen Zeichenfolgen können Millionen Jahre ins Land ziehen. Wenn Sie sich an Teile des Passworts oder zumindest an dessen Zusammensetzung erinnern, können Sie die Knackdauer jedoch deutlich reduzieren.

betterCode()

API 2021

Die Heise-Konferenz zu Design, Entwicklung und Management von Web-APIs

1. Dezember 2021 – Online

Schnittstellen, die die Welt bedeuten

Die betterCode() API im Dezember 2021 gibt Ihnen Antworten auf zahlreiche Fragen:

- **REST**: Wo liegen die Schwächen? Welches sind die Alternativen?
- **API Coding Guidelines**: Wie machen die das bei Zalando?
- APIs **versionieren**: Muss das sein?
- **Asynchrone APIs**: Wo kann die AsyncAPI helfen?
- Sind APIs grundsätzlich **unsicher**?

Jetzt Tickets sichern!

heise Developer dpunkt.verlag

api.bettercode.eu

John gibt es für Windows, Linux und macOS, bei Kali Linux (siehe S. 122) ist er bereits an Bord. Er liest die verschlüsselten Dateien nicht selbst ein, er benötigt stattdessen eine Datei, die den zu knackenden Passwort-Hash enthält. Die können Sie mit den mitgelieferten Hilfswerkzeugen leicht selbst erstellen. Im Lieferumfang befinden sich etliche davon für diverse Dateiformate, darunter neben Zip etwa Android Backup, Bitwarden, KeePass, Office und PDF. Manche Helfer sind Python-Skripte und setzen den dazugehörigen Interpreter voraus. Die Tools liegen im Ordner „run“, Kali-Nutzer schauen indes unter /usr/share/john/.

So weit die Theorie, jetzt folgt die Praxis: Um zum Beispiel ein verschlüsseltes Zip-Archiv mit John zu knacken, extrahieren Sie zunächst den Passwort-Hash mit dem Hilfstool zip2john daraus: `zip2john verschluesselt.zip > knackmich.hash`. Mit anderen Formaten klappt das ebenso leicht, bei Office-Dokumenten ersetzen Sie `zip2john` durch `office2john`, bei PDF-Dokumenten durch `pdf2john` und so weiter.

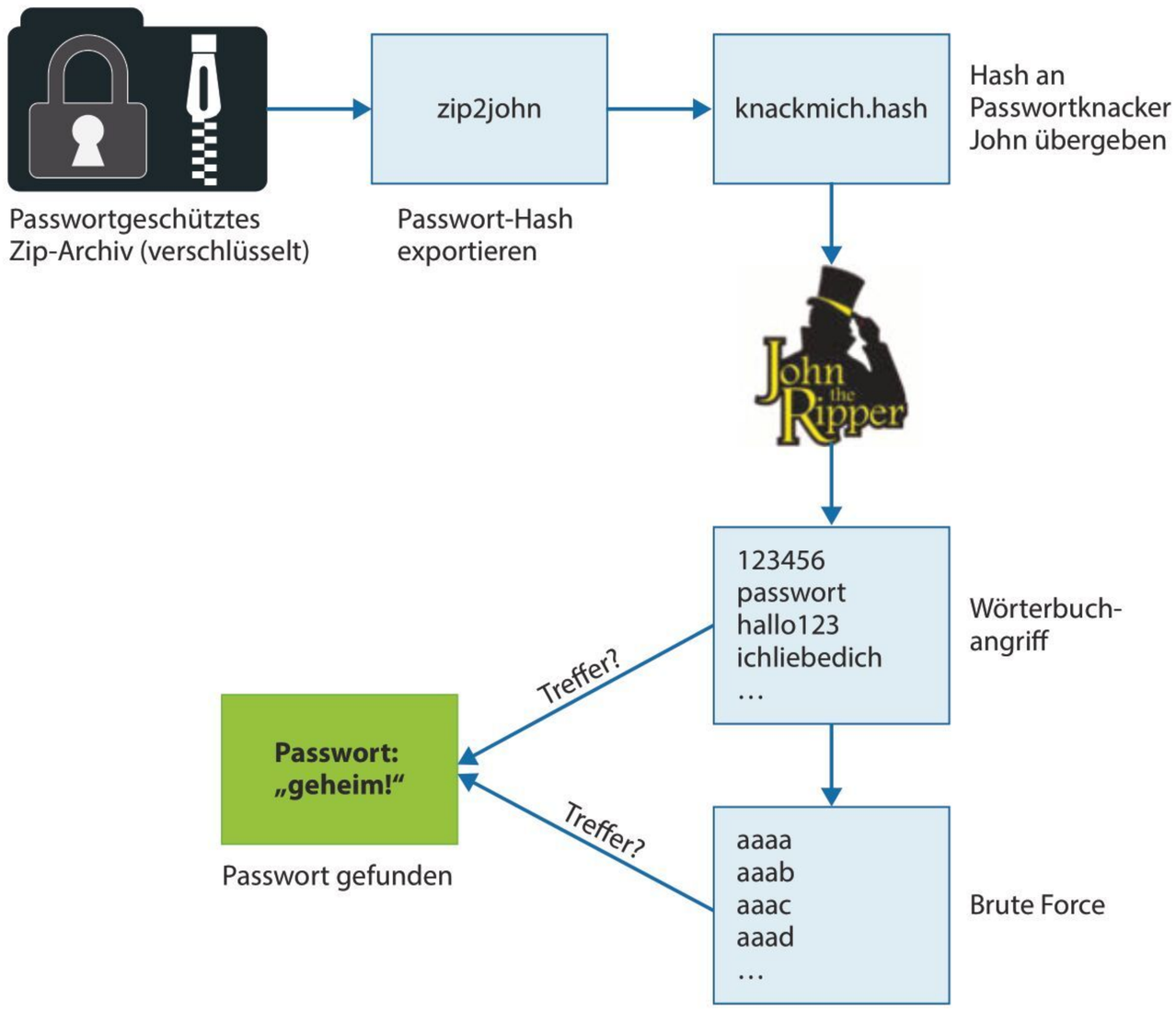
Anschließend setzen Sie John auf die Hash-Datei an, im einfachsten Fall mit `john knackmich.hash`. Dann probiert er zunächst die Kennwörter aus der mitgelieferten Liste password.lst durch, die einige zehntausend der am häufigsten genutzten Passwörter aus dem englischsprachigen Raum enthält. Dabei probiert John gängige Abwandlungen aus, ein Listeneintrag „mutti“ würde deshalb auch Varianten wie das Passwort „Mutti!“ zutage fördern. Das Abarbeiten der Liste dauert nur wenige Sekunden. Mit etwas Glück meldet John nach kurzer Zeit einen Treffer und zeigt das gefundene Passwort auf der Konsole an.

Wird der Passwortknacker noch nicht fündig, probiert er systematisch ASCII-Zeichenkombinationen aus, was deutlich mehr Zeit frisst – und bei langen Passwörtern aussichtslos ist. In diesem Fall sollten Sie den Suchradius möglichst weit eingrenzen.

Sie können zum Beispiel eine Mindest- und Maximallänge wie 5 und 6 Zeichen vorgeben, indem Sie `-min-length=5 -max-length=6` an den Befehl hängen. Mit `-incremental=digits` würden Sie den Suchradius auf Ziffern beschränken, um zum Beispiel ein Passwort zu finden, das aus einem Geburtsdatum besteht. Wer einen Teil seines Passworts kennt, sollte John nach einer Passwortmaske suchen lassen. Den Aufbau solcher Masken erklärt die Dokumentation en détail (siehe ct.de/wn7d). Im folgenden Beispiel ist bekannt, dass das Kennwort mit „passwort“ beginnt und darauf noch drei unbekannte Zeichen folgen: `john knackmich.hash -mask=passwort?a?a?a`

Zip-Passwort mit John the Ripper knacken

Wenn Sie das Passwort einer verschlüsselten Zip-Datei vergessen haben, können Sie den Passwortknacker John the Ripper darauf ansetzen. Er versucht es mit verschiedenen Methoden zu erraten, etwa mit Hilfe einer Wortliste oder durch stumpfes Durchprobieren (Brute Force). Die erforderliche Zeit zum Finden des Passworts hängt unter anderem von Passwortlänge und verfügbarer Rechenleistung ab. Sie können des Prozess abkürzen, wenn Sie sich an Teile des Passworts erinnern. John unterstützt neben Zip diverse Dateiformate, darunter Microsoft Office und PDF.



Probieren Sie doch mal aus, wie lange Ihre Kennwörter einem Angriff standhalten würden. Bedenken Sie aber, dass einem echten Angreifer wahrscheinlich mehr Rechenleistung zur Verfügung steht, etwa in Form eines Grafikkarten-Clusters in der Cloud. Zudem setzt er möglicherweise eine andere Passwortliste ein, auf der auch Ihr Kennwort steht. Daher gilt: Wählen Sie stets möglichst lange, individuelle Kennwörter – am besten zufällig generiert oder zumindest mit absichtlichen Tippfehlern.

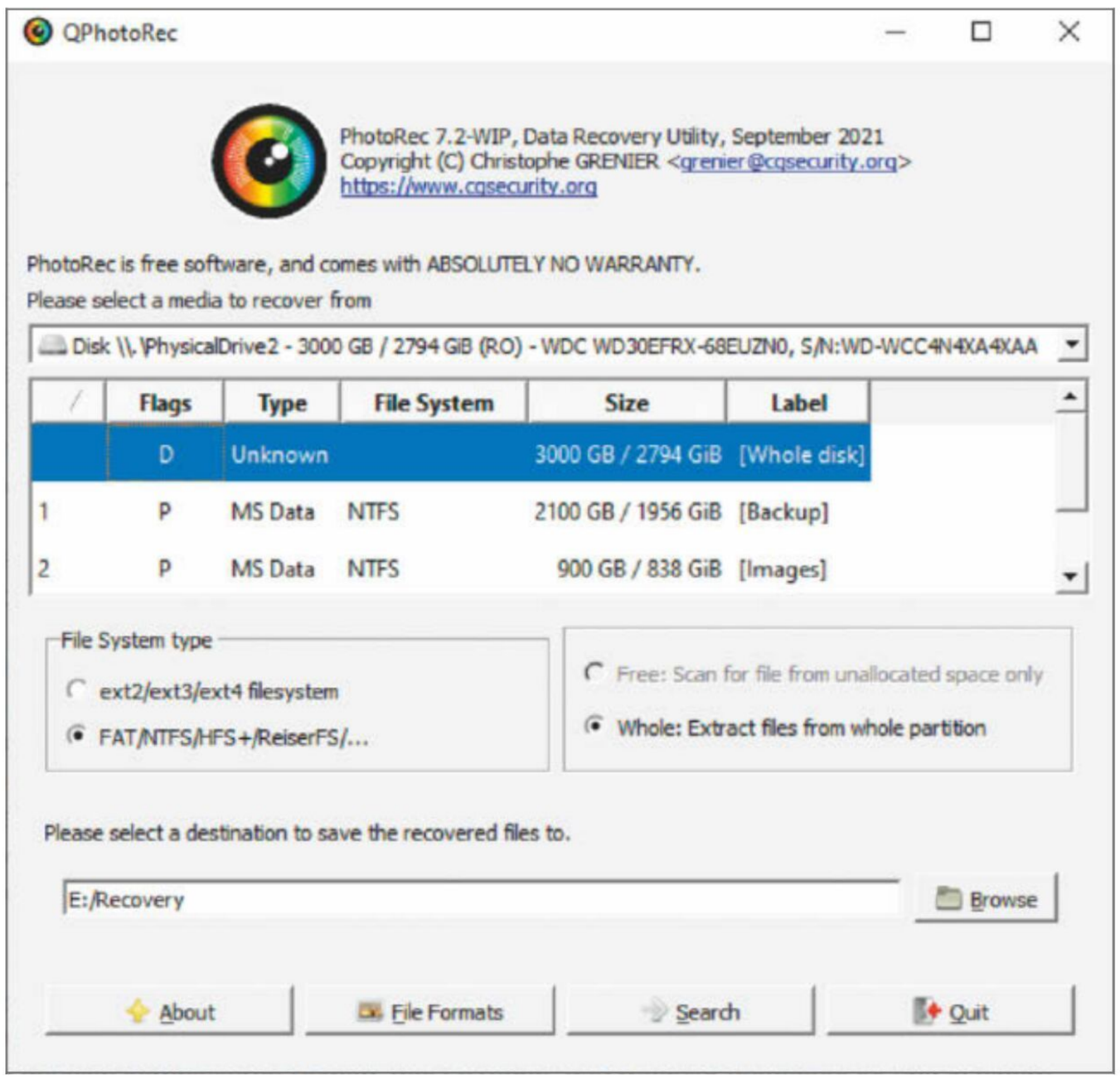
Dateien retten

Gelöschte Dateien sind nicht zwangsläufig unrettbar verloren. Das machen sich Hacker zunutze, um

vertrauliche oder pikante Daten von achtlos entsorgten Festplatten, USB-Sticks und Speicherkarten zu kratzen. Die genutzten Tools sind natürlich auch für die Rettung eigener Daten äußerst nützlich – zum Beispiel, wenn Sie wichtige Dateien versehentlich gelöscht haben oder die Daten aus anderen Gründen plötzlich nicht mehr auffindbar sind. Auch Dateien auf SSDs lassen sich mit etwas Glück wiederherstellen, wenn das System den TRIM-Befehl noch nicht ausgeführt hat, um die Daten endgültig zu löschen.

Ein bewährtes Werkzeug für diesen Zweck ist das Open-Source-Tool **PhotoRec**, das auf allen möglichen Betriebssystemen läuft. Es ist eigentlich auf der Kommandozeile zu Hause, mit QPhotoRec gibt es inzwischen jedoch auch eine einfache Bedienoberfläche. Nach dem Start wählen Sie oben das zu durchsuchende Laufwerk oder ein Laufwerksabbild und darunter entweder eine bestimmte Partition oder das gesamte Speichergerät. Weiter unten stellen Sie das Dateisystemformat ein und rechts daneben wählen Sie aus, ob nur die unbelegten Speicherblöcke abgesucht werden sollen („Free“) oder alles („Whole“). Zu guter Letzt geben Sie einen Zielordner für die aufgespürten Dateien an und starten die Rettungsaktion mit „Search“.

Falls Ihre Dateien nicht lesbar sind, weil Partitionen oder Dateisystem beschädigt sind, können Sie gezielte Reparaturen daran durchführen. Hierfür greifen Sie am besten zu **TestDisk**, das Sie ohnehin bereits besitzen, wenn Sie PhotoRec heruntergeladen haben. Starten Sie TestDisk über die Konsole, führt es Sie interaktiv durch die wichtigsten Fragen, ehe die Reparatur beginnt. Über die „Undelete“-Funktion können Sie mit dem Tool außerdem gezielt einzelne Dateien wiederherstellen, was schneller zum Ziel führen kann als ein groß angelegter Rettungsversuch mit PhotoRec.



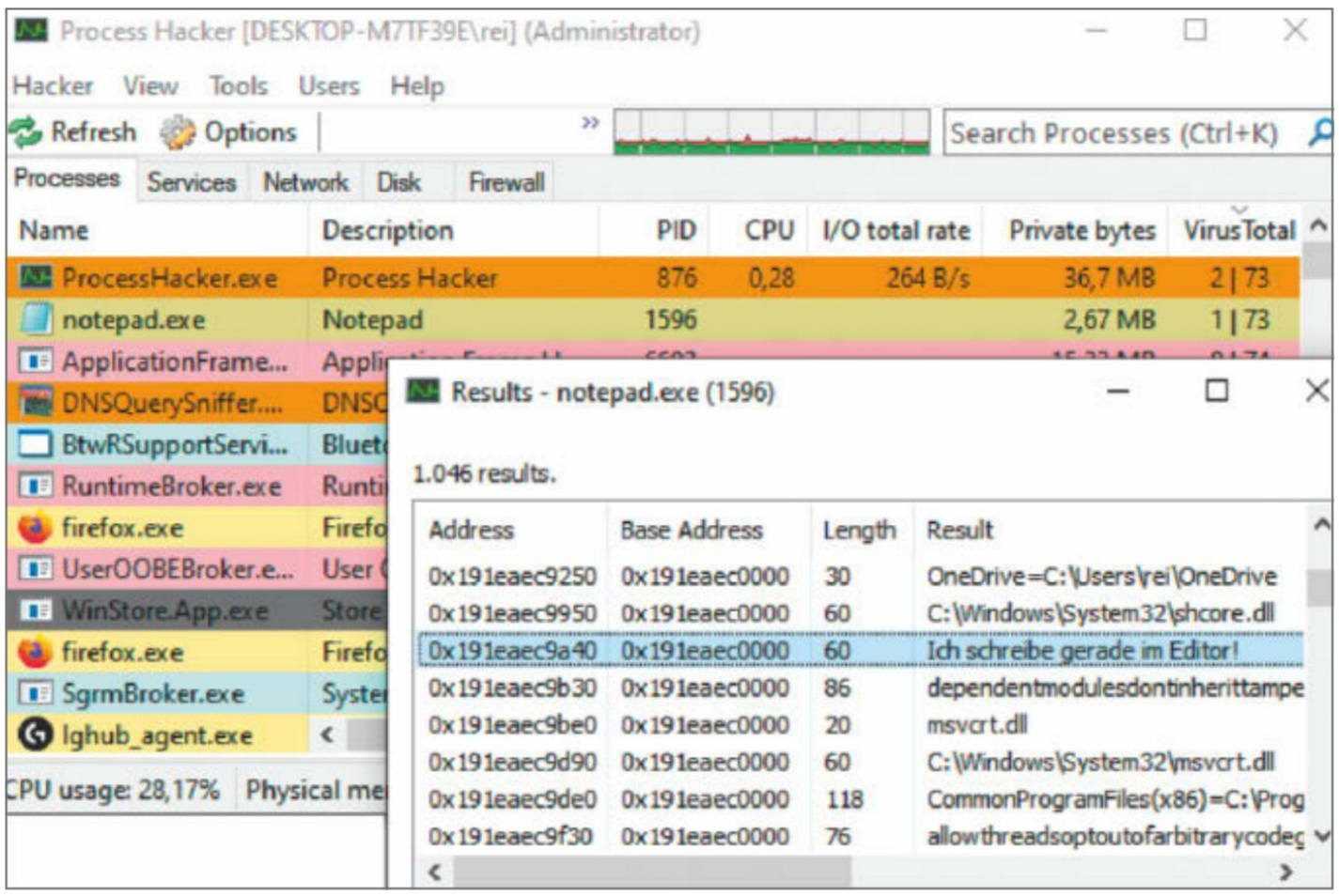
Sind Ihre Dateien noch zu retten? Mit PhotoRec finden Sie es heraus.

Prozesse hacken

Ein Windows-System gönnt sich selten eine Pause: Prozessor, Datenträger und Netzwerk stehen niemals still. Nur ein Blick hinter die Kulissen zeigt, womit der Rechner gerade beschäftigt ist. Installiert Windows gerade fleißig Updates oder wütet ein Krypto-Trojaner, der alles verschlüsselt, was er in die Finger bekommt? Mit den richtigen Systemtools finden Sie es heraus. Die Auswahl ist riesig, und am bekanntesten sind die SysInternals-Tools, die wir schon ausführlich in c’t präsentiert haben (siehe ct.de/wn7d). Im Rahmen dieser Vorstellung von Hacking-Tools möchten wir den Blick auf das Mehrzweck-Tool **Process Hacker** lenken, das einige besondere Extras enthält. Um von diesen Extras zu profitieren, benötigen Sie einen frischen Nightly-Build (3.x).

Das Hauptfenster des Process Hacker ist in fünf Tabs unterteilt: „Processes“ zeigt, ähnlich wie der Taskmanager, Informationen über laufende Prozesse an und „Services“ listet die Dienste auf. Über den „Network“-Tab schauen Sie nach, welche Prozesse aktuell mit dem Netz kommunizieren. „Disk“ macht Dateizugriffe sichtbar und „Firewall“ lässt Sie auf die Aktivitäten der Windows-Firewall blicken. Dort sehen Sie, welche aktuellen Verbindungen auf Grundlage welcher Regeln zugelassen oder blockiert wurden. Damit sind nur die Basics beschrieben, es gibt aber noch viel zu entdecken.

Klicken Sie doppelt auf einen Prozessnamen, um ihn unter die Lupe zu nehmen. Hier können Sie zum Beispiel die geladenen Bibliotheken (Modules) ein-



Der Process Hacker macht da weiter, wo andere Taskmanager aufhören: Das Tool erlaubt sogar Eingriffe in den Arbeitsspeicher der Prozesse.

sehen, aber auch im Arbeitsspeicher des Prozesses stöbern (Memory). Klicken Sie dort auf „Options“ und „String“, listet Ihnen Process Hacker sämtliche Zeichenfolgen auf. So können Sie den Speicher zum Beispiel nach Zugangsdaten, IP-Adressen oder API-Schlüsseln durchsuchen, die das Programm dort bereithält. Über den Tab „Windows“ der Prozesseigenschaften finden Sie heraus, welche Fenster einem Prozess zugeordnet sind und können sogar die einzelnen Fensterelemente verändern. So schalten Sie zum Beispiel – auf eigene Gefahr – gesperrte Buttons frei.

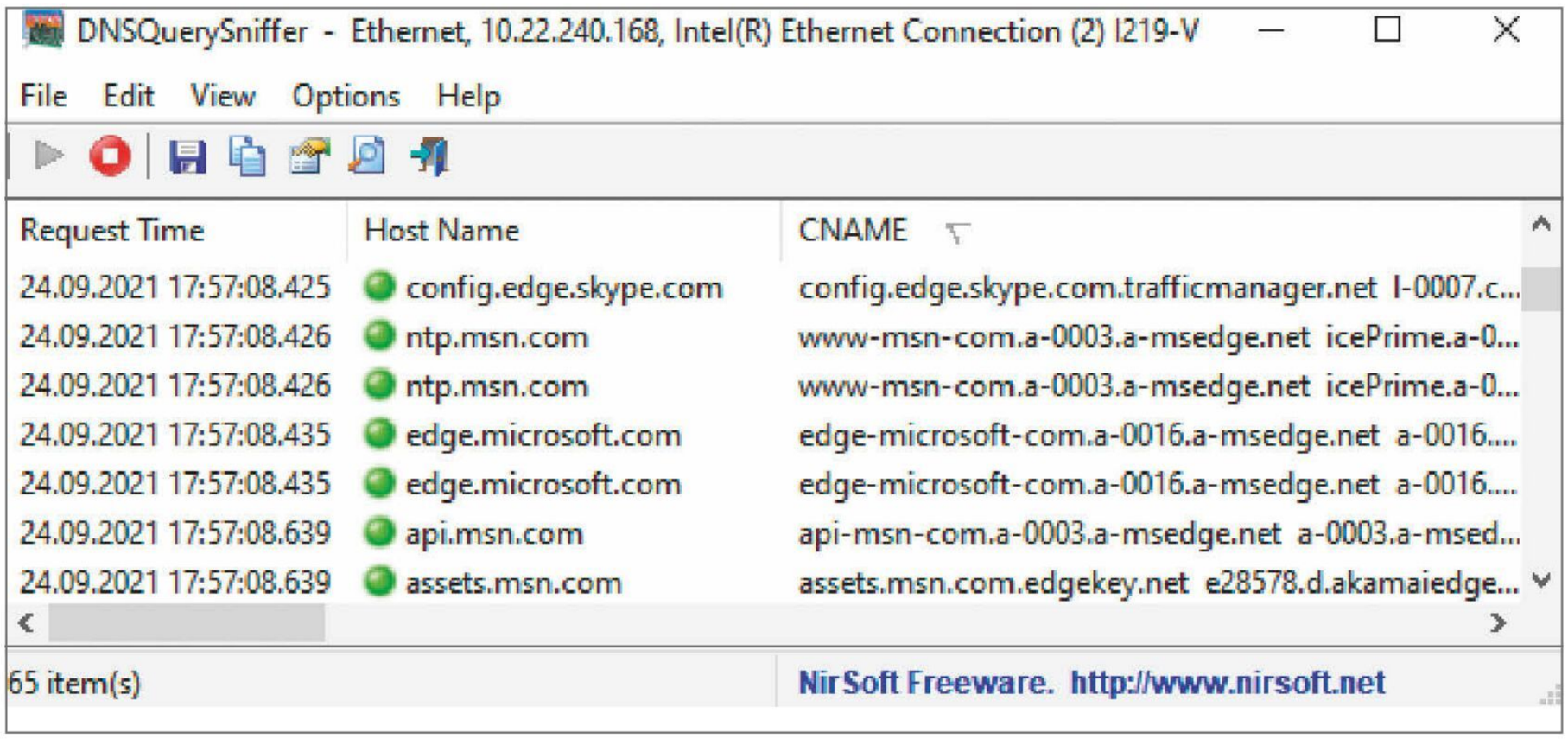
Abschließend noch eine kleine Übungsaufgabe: Tippen Sie doch mal einen kurzen Text in den Editor von Windows und ändern Sie das Getippte anschließend, indem Sie den Arbeitsspeicher von notepad.exe mit dem Process Hacker manipulieren.

Netzwerkverkehr untersuchen

Wenn sich Ihr System auffällig verhält, kann sich ein Blick in den Netzwerkverkehr lohnen. Dafür ist **NetworkTrafficView** von NirSoft sehr praktisch: Es zeigt die Netzwerkverbindungen Ihres Systems an und verrät Ihnen, von welchen Prozessen die Verbindungen ausgehen. Aufschlussreich sind auch die DNS-Anfragen, denn bevor eine Verbindung zu einer bestimmten Domain aufgebaut werden kann, muss ein Prozess erstmal die dazugehörige IP-Adresse bei einem DNS-Server erfragen. Mit dem **DNSQuerySniffer**, ebenfalls von NirSoft, können Sie die Anfragen gezielt und live mitverfolgen. So können Sie auch prüfen, ob die DNS-Anfragen Ihres Systems noch im Klartext oder bereits verschlüsselt, etwa über DNS-over-HTTPS (DoH), übertragen werden. In letzterem Fall tauchen sie in dem Analyse-Tool nicht auf.

Mit **PacketCache** von Netresec schauen Sie bei der Analyse des Netzwerkverkehrs in die Vergangenheit: Der Dienst schreibt den IPv4-Traffic des Systems fortlaufend in den Arbeitsspeicher, wodurch Sie jederzeit herausfinden können, was in den letzten Minuten passiert ist. IPv6-Verkehr unterstützt er aktuell jedoch nicht. PacketCache wird von Hand eingerichtet, mit den Anweisungen auf der Herstellerseite (siehe ct.de/wn7d) ist das jedoch schnell erledigt. Dort erfahren Sie auch, wie Sie die aufgezeichneten Daten abholen, beispielsweise mit dem Analyseprogramm Wireshark oder dem Auswertungs-Tool **NetworkMiner,** das auch von Netresec kommt. Es erlaubt einen schnellen Einblick in die Kommunikation: Wer spricht mit wem, DNS-Anfragen, TLS-Zertifikate und mehr.

Aus Klartextverkehr (HTTP) extrahiert es darüber hinaus Zugangsdaten, URL-Parameter und Bilddateien. Alles, was hier auftaucht, kann auch ein Angreifer sehen, der Ihren Datenverkehr zum Beispiel an einem Hotspot belauscht. Nutzen Sie das Tool, um Datenlecks zu erkennen und gezielt durch Verschlüsselung (etwa per VPN) zu beheben. Wenn Sie mit NetworkMiner live auf den Datenverkehr schauen möchten, sollten Sie den Capture-Treiber Npcap (WinPcap) installieren und als Netzwerkadapter für die



DNS-Anfragen verraten viel über das Kommunikationsverhalten des Systems. DNSQueryView macht sie sichtbar.

Analyse wählen. Die zur Auswahl stehenden „Socket“-Adapter werten lediglich IPv4-Datenverkehr aus, nicht aber IPv6. Wenn Sie Wireshark installiert haben, besitzen Sie den Treiber wahrscheinlich schon.

PowerShell-Hacks

Die Windows PowerShell ist nicht nur ein fester Bestandteil des Betriebssystems, sie ist auch sehr mächtig – und das macht sie für Hacker interessant. Cyberschurken zweckentfremden die PowerShell längst für die feindliche Übernahme einzelner Rechner und ganzer Netzwerke (PowerShell Empire, siehe Seite 121). Aber sie lässt sich auch für nützliche Windows-Hacks einspannen, etwa um das Betriebssystem individuell zu konfigurieren und seine Geschwätzigkeit zu reduzieren.

Das PowerShell-Modul **Sophia Script** erlaubt Ihnen umfassende Eingriffe ins System, die normalerweise nur sehr umständlich möglich sind. Sie können damit zum Beispiel die Telemetrie- und Diagnosefunktionen zähmen, die Bing-Suche im Startmenü loswerden und den Windows Defender aufmotzen.

Die Einrichtung ist bei GitHub ausführlich dokumentiert (siehe ct.de/wn7d). In der Zip-Datei befindet sich das PowerShell-Skript Sophia.ps1, das demonstriert, wie Sie die Sophia-Kommandos aneinanderreihen, zum Beispiel um eine frische Windows-Installation nach Ihren Wünschen einzurichten. Führen Sie das Skript erst aus, nachdem Sie es inspiziert und die vorgegebenen Befehle an Ihre Bedürfnisse angepasst haben.

Sie können auch einzelne Funktionen direkt aufrufen. Der folgende Befehl etwa entfernt die Bing-Suche aus dem Startmenü:

```
. .\Functions.ps1
Sophia -Functions
    "BingSearch -Disable"
```

Grundsätzlich sollten Sie sich darüber im Klaren sein, was Sie tun und sich über Nebenwirkungen informieren. Wenn Sie etwa Telemetriedienste blockieren, müssen Sie beobachten, ob Windows weiterhin mit Updates versorgt wird. Es gilt die Devise: Weniger ist mehr! Falls Sie unsicher sind, was Sie mit einem Sophia-Befehl auslösen, können Sie einen Blick in den Powershell-Code werfen (Ordner „Module“).

Fazit

Das passende Hacking-Tool zur rechten Zeit kann echte Probleme lösen. Ganz gleich, ob es darum geht, ein vergessenes Passwort zu knacken, verloren geglaubte Dateien zu retten oder nervige Windows-Funktionen abzuschalten. Einigen der Helfer haftet zu Unrecht ein schlechter Ruf an – der Umstand, dass einige davon auch von Cyberschurken genutzt werden, zeigt eher, dass man mit den Tools sehr effektiv bestimmte Dinge erledigen kann. (rei) c't

Tools, Literaturhinweise

ct.de/wn7d

Bild: Sven Hauth

Hacking-Werkzeug für Fortgeschrittene

Mit den Hacking-Tools von Penetrationtestern finden Sie Sicherheitslücken in Ihren Websites, Netzwerken und Anwendungen, bevor es andere tun.

Von **Ronald Eikenberg und Alexander Königstein**

Hollywood weiß Hacker-Aktivitäten in Szene zu setzen: Vor unzähligen Monitoren mit monochromatischen Benutzeroberflächen sitzen Gestalten im Kapuzenpulli und brechen durch die Firewalls. In der Realität geht es weitaus nüchterner zu, denn die eigentliche Action spielt sich hinter den Kulissen ab. Das ist aber nicht weniger faszinierend, denn Hacking-Tools leisten erstaunliche Dinge, wenn man sie richtig einsetzt. Das setzt etwas Wissen und Erfahrung voraus, doch beides baut sich ganz von selbst auf, wenn Sie erst mal Feuer gefangen haben.

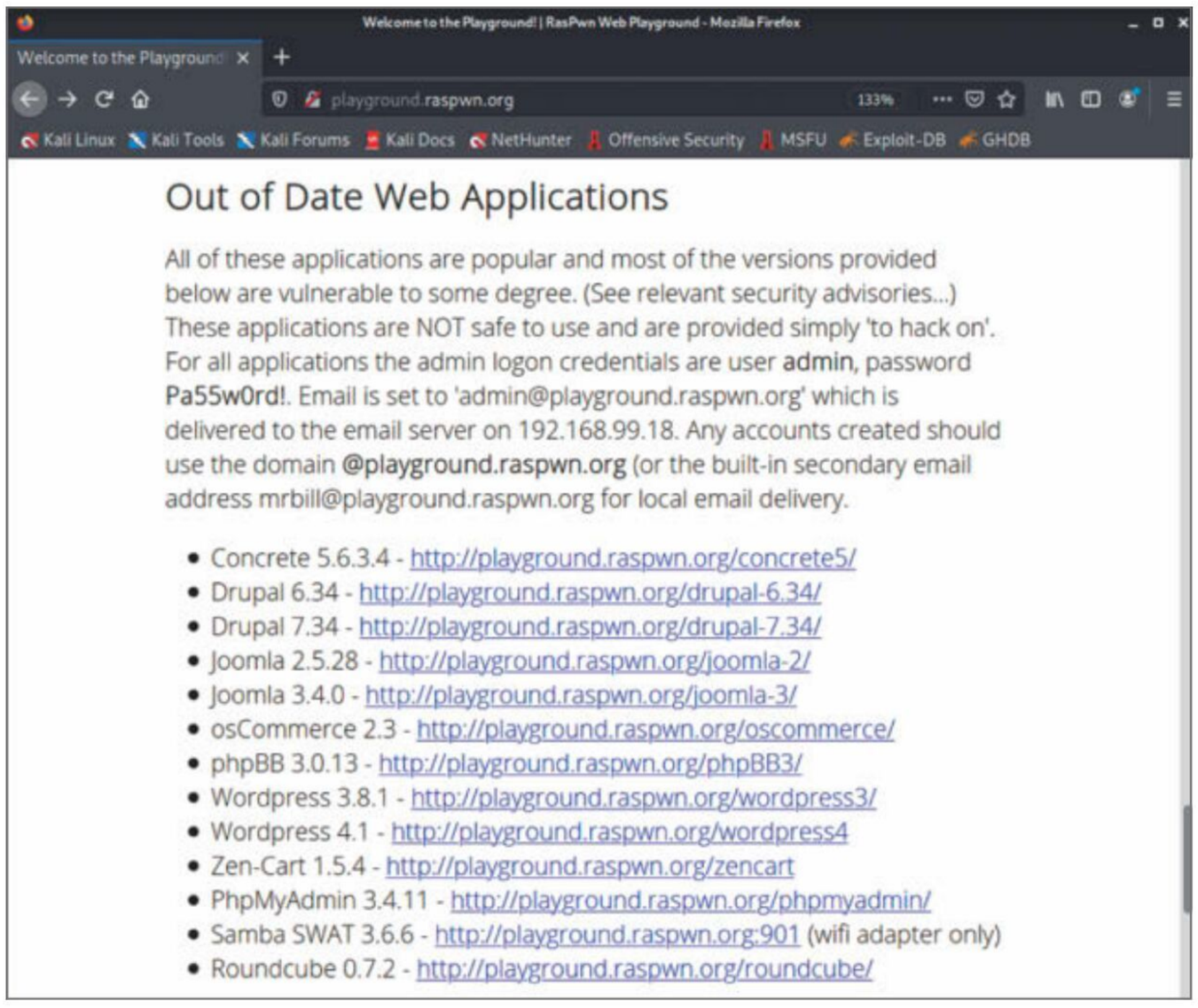
In diesem Artikel stellen wir eine Auswahl interessanter Profi-Werkzeuge vor, die sowohl auf der dunklen als auch auf der hellen Seite der Macht genutzt werden. Stöbern Sie auch in unserem Artikel für Einsteiger „Nützliche Hacking-Tools für den Alltag“ auf Seite 106.

Mit den im Folgenden vorgestellten Profi-Tools spüren Sie Sicherheitslücken in Ihren Websites, Netzwerken, Apps, IoT-Geräten und vielem mehr auf. Anschließend können Sie gezielt Schutzmaßnahmen ergreifen und die Schlupflöcher stopfen, bevor

es zu spät ist. Die meisten Hacking-Tools laufen am besten oder ausschließlich unter dem Betriebssystem Linux. Eine gute Grundlage für die ersten Schritte ist **Kali Linux**, das von Haus aus bestens auf die Bedürfnisse von Hackern zugeschnitten ist. Auf Seite 122 erfahren Sie, wie Sie sich einen Kali-USB-Stick mit persistenter Datenpartition für Ihre Experimente erstellen. Download-Links und weiterführende Informationen zu allen vorgestellten Tools finden Sie online unter ct.de/wrbu. Aber genug der Vorrede – jetzt geht es in die Vollen!

Angreifen erlaubt

Die hier genannten Hacking-Tools sind nicht illegal, aber natürlich dürfen Sie damit nicht gegen geltende Gesetze verstoßen (siehe Seite 128). Damit Sie gar nicht erst in Versuchung kommen, die Tools unerlaubt an fremden Servern zu testen, sollten Sie sich eine geeignete Übungsumgebung schaffen – zum Beispiel ein Testnetz, in dem sich ausschließlich Systeme befinden, die Sie attackieren möchten und dürfen.



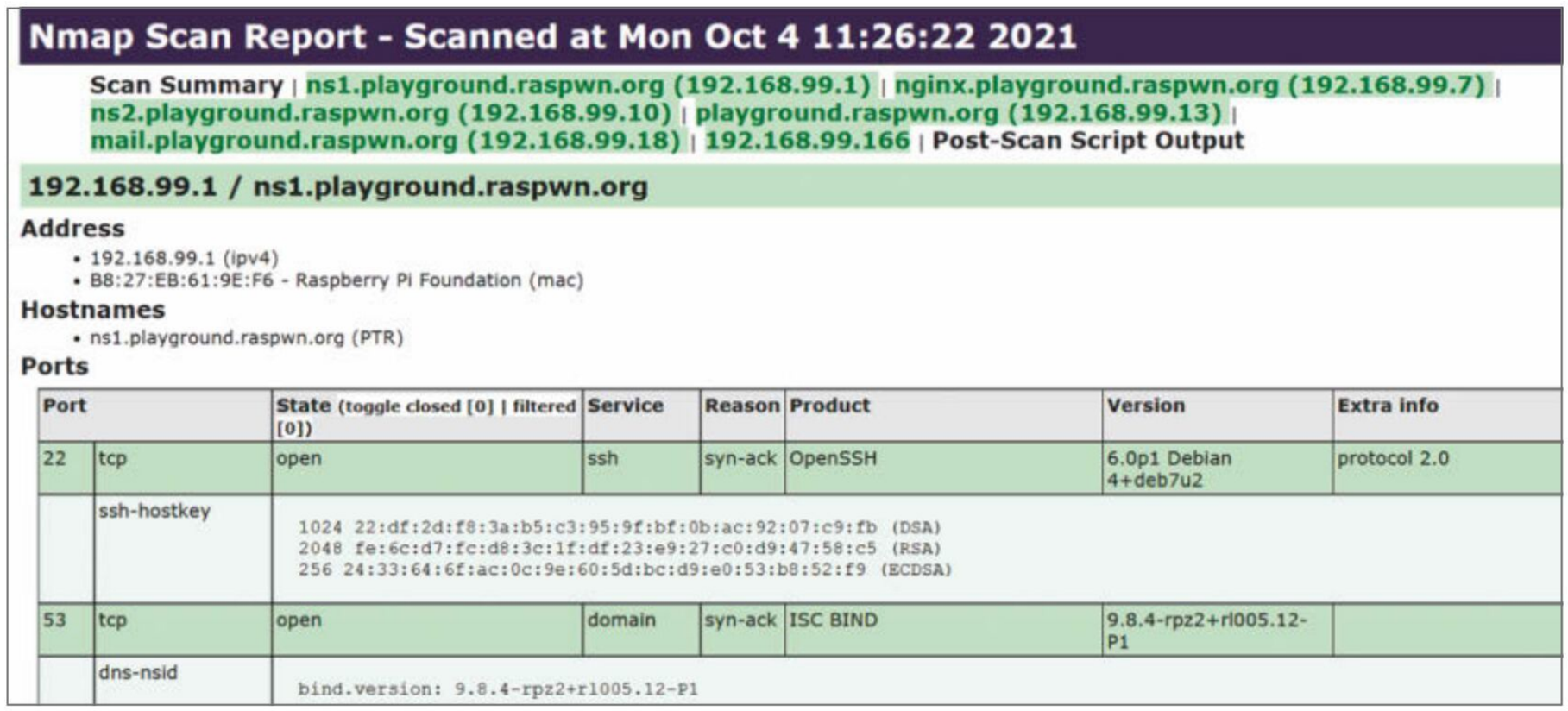
Das Raspi-Image RasPwn enthält etliche verwundbare Web-Apps – und das mit voller Absicht.

Ein geeignetes Angriffsziel ist **RasPwn**, das ein ganzes Netzwerk voller verwundbarer Server simuliert, an denen Sie sich austoben können. Sie übertragen es einfach auf eine MicroSD-Karte, die Sie anschließend in einen Raspi-Kleincomputer stecken (mindestens Raspi 2B). Nach dem Booten meldet sich ein WLAN namens „RasPwn OS“, zu dem Sie mit dem Passwort „In53cur3!“ eine Verbindung herstellen. Aus dem Netz öffnen Sie http://playground.raspwn.org mit einem Browser Ihrer Wahl, wo Sie mit allen wichtigen Informationen über das virtuelle Netzwerk und die angreifbaren Server versorgt werden. Ein Netzwerkkabel darf nicht mit dem Raspi verbunden sein, andernfalls hat das hochgradig verwundbare Image unter Umständen Zugriff auf Ihr Hauptnetzwerk und das Internet – was Sie tunlichst vermeiden sollten.

Zu den möglichen Angriffszielen zählen verwundbare WordPress-Installationen, eine steinalte Version des Webshop-Systems osCommerce, das Datenbank-Tool phpMyAdmin, ein Mailserver, Samba und so weiter. Auch das Debian-Linux, auf dem RasPwn basiert, hat schon fast sieben Jahre auf dem Buckel und ist so löchrig wie ein Schweizer Käse. Obendrauf gibt es zahlreiche Web-Applikationen wie OWASP Bricks und Damn Vulnerable Web Application (DVWA), die nur mit dem Ziel entwickelt wurden, möglichst verwundbar zu sein, um typische Sicherheitslücken am lebenden Objekt zu demonstrieren. Viele dieser Projekte sind online dokumentiert, wodurch sie sich hervorragend zum Lernen eignen (siehe ct.de/wrbu).

Netzwerk auskundschaften

Hat sich ein Angreifer Zugriff auf ein fremdes Netzwerk verschafft, etwa durch eine frei zugängliche Netzwerkbuchse im Aufenthaltsraum, eine per E-Mail eingeschleuste Malware oder ein schwaches WLAN-Passwort, dann wird er sich erst mal einen Überblick über die Geräte im Netz verschaffen, um mögliche Angriffsziele auszumachen. Hierbei ist der mächtige Netzwerkscanner **Nmap** (Network Mapper) die erste Wahl. Er spürt nicht nur die Rechner, Drucker, NAS, Server, Router und vieles mehr auf, sondern auch die darauf laufenden Dienste. Durch Skripte lässt sich der Scanner beliebig erweitern, etwa um die entdeckten Clients gleich noch auf Sicherheitslücken abzuklopfen. Das alles ist nützlich, um verwundbare Geräte im eigenen Netz aufzuspüren und sie anschließend entweder abzusichern oder aus dem Verkehr zu ziehen.



Nmap Scan Report - Scanned at Mon Oct 4 11:26:22 2021

Scan Summary | ns1.playground.raspwn.org (192.168.99.1) | nginx.playground.raspwn.org (192.168.99.7) | ns2.playground.raspwn.org (192.168.99.10) | playground.raspwn.org (192.168.99.13) | mail.playground.raspwn.org (192.168.99.18) | 192.168.99.166 | Post-Scan Script Output

192.168.99.1 / ns1.playground.raspwn.org

Address

- 192.168.99.1 (ipv4)
- B8:27:EB:61:9E:F6 - Raspberry Pi Foundation (mac)

Hostnames

- ns1.playground.raspwn.org (PTR)

Ports

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
22	tcp	open	ssh	syn-ack	OpenSSH	6.0p1 Debian 4+deb7u2	protocol 2.0
	ssh-hostkey	1024 22:df:2d:f8:3a:b5:c3:95:9f:bf:0b:ac:92:07:c9:fb (DSA) 2048 fe:6c:d7:fc:d8:3c:1f:df:23:e9:27:c0:d9:47:58:c5 (RSA) 256 24:33:64:6f:ac:0c:9e:60:5d:bc:d9:e0:53:b8:52:f9 (ECDSA)					
53	tcp	open	domain	syn-ack	ISC BIND	9.8.4-rpz2+rl005.12-P1	
	dns-nsid	bind.version: 9.8.4-rpz2+rl005.12-P1					

Was ist los im Netz? Der Netzwerkscanner Nmap liefert einen HTML-Bericht über alle Geräte und Dienste.

Nmap läuft auf Linux, macOS und Windows, bei Kali Linux ist er inklusive. Wenn Sie auf einer Shell `nmap` ohne Parameter eintippen, zeigt das Tool die wichtigsten Betriebsmodi an. Um einfach und schnell die offenen Ports eines bestimmten Hosts herauszufinden, hängen Sie einfach dessen IP-Adresse an den Befehl an, etwa `nmap 192.168.178.1`. Das müssen Sie zwar nicht als root ausführen, es lohnt sich aber: So finden Sie mehr über die Clients heraus, im konkreten Fall die MAC-Adressen. IPv6-Adressen scannen Sie mit dem Parameter `-6`.

Sie können den Scan auf einen IP-Bereich ausweiten, den Sie zum Beispiel mit `192.168.178.1-50` definieren (alle IP-Adressen, die mit 192.168.178 anfangen und mit .1 bis .50 enden). Oder Sie scannen gleich das gesamte /24-Subnetz (alle bis .255): `nmap 192.168.178.0/24`. Ist der Scan abgeschlossen, präsentiert Ihnen Nmap die Ergebnisse auf der Shell, vorher lässt das Tool nicht von sich hören. Wer ungeduldig ist, kann mit `--stats-every 10s` festlegen, dass Nmap regelmäßig ein Statusupdate ausgibt.

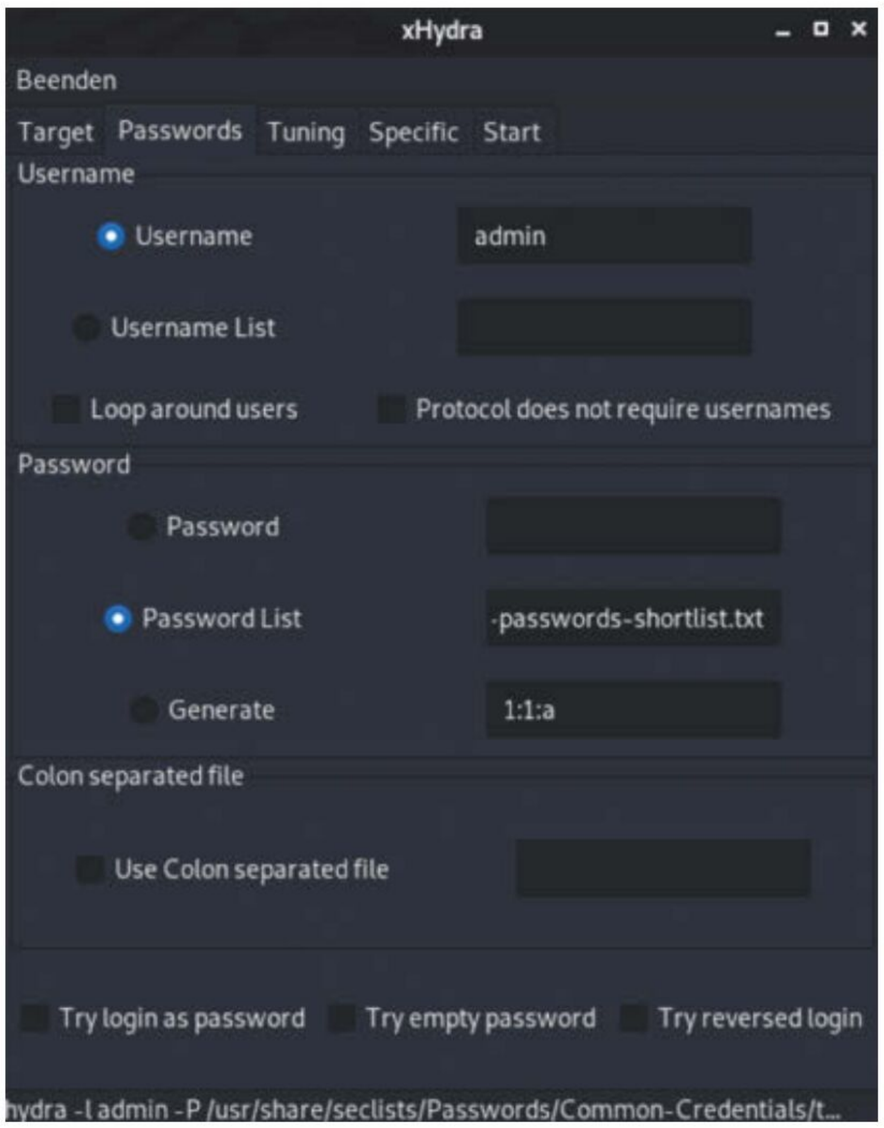
Wirklich komfortabel lesbar ist der Bericht auf der Shell nicht. Sie können jedoch leicht einen formatierten HTML-Report erstellen, indem Sie zunächst Nmap mit `-oX ergebnis.xml` anweisen, einen XML-Export der Ergebnisse zu schreiben. Anschließend bauen Sie daraus mit dem unter Kali vorinstallierten Tool xsltproc eine HTML-Datei, die Sie mit jedem Browser öffnen können: `xsltproc ergebnis.xml -o ergebnis.html`.

Mit dem einfachen Scan kratzen Sie erst an der Oberfläche der Möglichkeiten. Mehr können Sie Nmap über verschiedene Scan-Optionen entlocken (siehe ct.de/wrbu). Sehr umfangreich ist der Modus `-A`, der unter anderem die Betriebssystem- und Versionserkennung (Fingerprinting) scharf schaltet. Diesen Modus sollten Sie mit `sudo` starten, damit Ihnen nichts entgeht. Aber aufgepasst: Nmap greift in diesem Fall aktiv auf die entdeckten Server zu, um Informationen einzuholen. Das kann zu unerwarteten Effekten führen, unser Epson-Drucker etwa spuckt bei jedem Scan eine spärlich bedruckte Seite aus. Sie sollten Ihre ersten Schritte daher besser im oben erwähnten Testnetz machen.

Eine Übersicht über die mitgelieferten Skripte finden Sie in der Dokumentation von Nmap (siehe ct.de/wrbu). Praktisch ist etwa das vulners-Skript, das zu den ermittelten Serverversionen bekannte Schwachstellen aus einer Online-Datenbank heraussucht. Eigene Skripte können Sie in der Programmiersprache Lua entwickeln.

Zugriff auf Server

Vernetzte Geräte wie WLAN-Kameras oder Smart-Home-Komponenten sind oft für eine Überraschung gut: Auf manchen Exemplaren laufen unerwartete Dienste, die im Worst Case sogar mit einem Standardpasswort für Gott und die Welt aus dem Internet erreichbar sind. Die entdecken Sie zum Beispiel mit einem Nmap-Scan (siehe „Netzwerk auskundschaften“). Doch dann stehen Sie erst mal vor verschlossener Tür, denn das Zugriffspasswort ist häufig ebenso wenig dokumentiert wie der



Sesam, öffne Dich: Hydra probiert, sich mit beliebig langen Passwortlisten bei einem Server einzuloggen.

Dienst selbst. Solche Dienste sind ein unkalkulierbares Sicherheitsrisiko.

Fehlt Ihnen das Passwort, können Sie versuchen, es zu erraten – oder Sie überlassen dem Login-Cracker **Hydra** die ganze Arbeit. Er unterstützt viele gängige Protokolle wie FTP, HTTP(S), SMB, SSH, Telnet und VNC, wodurch er universell einsetzbar ist. Sie können Hydra wahlweise auf der Shell benutzen oder mit xHydra eine grafische Oberfläche starten, um ein paar Parameter einzustellen und die Passwortsuche zu starten. Wichtig sind das Ziel, der Port und das richtige Protokoll im ersten Tab. Danach folgt die Konfiguration des Nutzernamens und einer Passwortliste. Falls Sie gerade keine zur Hand haben, können Sie unter Kali das Paket seclists installieren, das diverse Listen unter /usr/share/seclists/Passwords ablegt. Im letzten Tab ist der Output des Tools zu sehen, also im besten Fall das gesuchte Passwort.

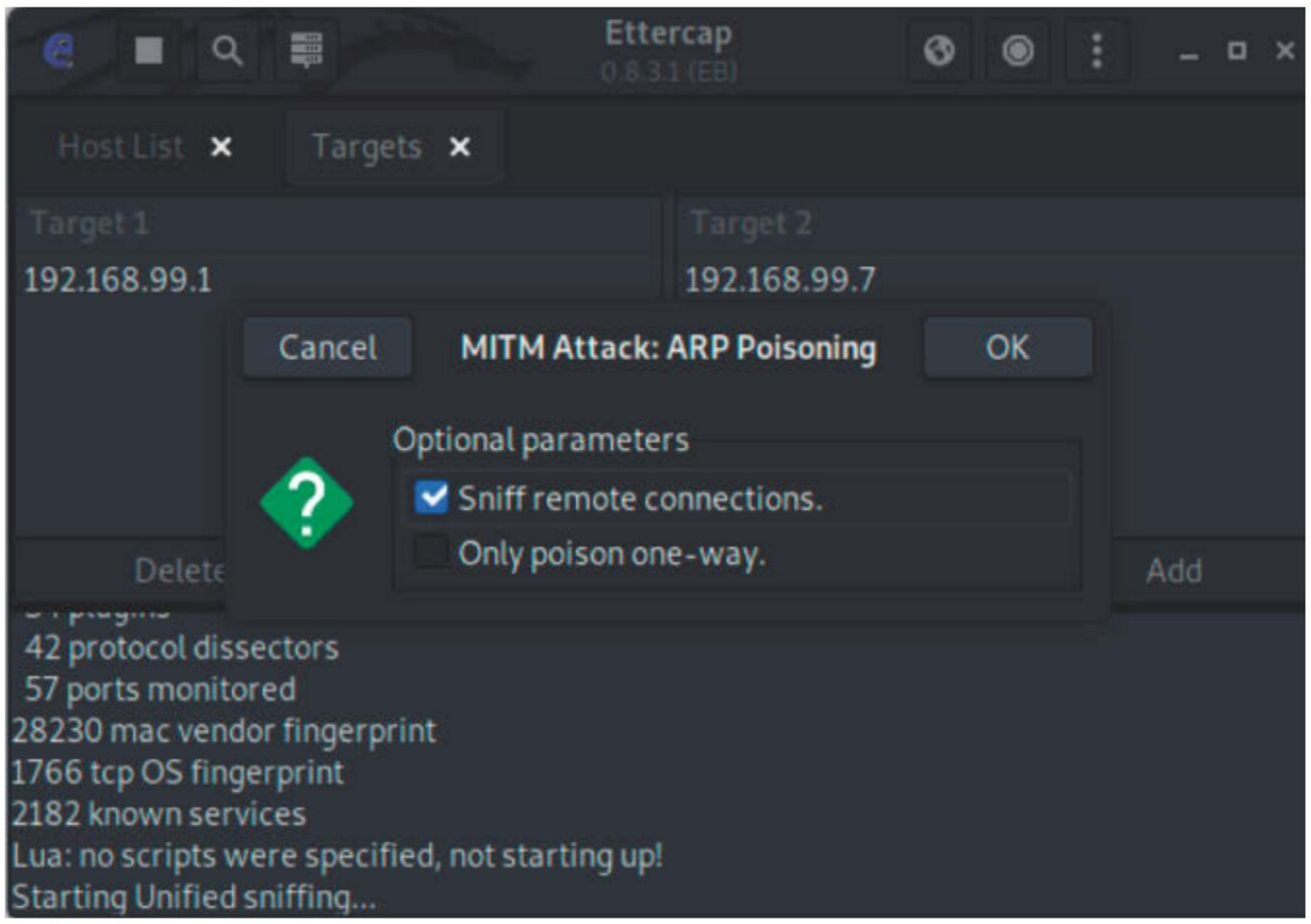
IPv4-Traffic umleiten

ARP-Spoofing (auch ARP-Poisoning genannt) ist ein alter, aber nach wie vor effektiver Trick, um IPv4-Netzwerkverkehr umzulenken. Ein Angreifer im gleichen Netzwerk kann so den Datenverkehr anderer Teilnehmer ohne deren Zutun mitlesen und manipulieren, etwa um sensible Daten abzugreifen oder Schadcode zu verbreiten. Das Ziel des Angriffs sind die ARP-Tabellen der Netzwerkclients. Darin ist vermerkt, unter welchen MAC-Adressen die IPs im lokalen Netz erreichbar sind. Durch gefälschte Nachrichten im Address Resolution Protocol (ARP) kann ein Angreifer die Tabellen verändern und Traffic umleiten, mitlesen und manipulieren. Eine solche Umleitung ist aber auch praktisch, um den Netzwerkverkehr einzelner Clients zu untersuchen, zum Beispiel, um herauszufinden, mit welchen Servern ein Smart-Home-Gerät spricht und ob die übertragenen Daten verschlüsselt sind.

Mit dem Sniffing-Tool **Ettercap** ist ARP-Spoofing sehr einfach, weil es alle nötigen Schritte vereint. Kali-Nutzer starten es über den Launcher („Sniffing & Spoofing/ettercap-graphical“). Wählen Sie zunächst das gewünschte Netzwerk-Interface. Anschließend müssen Sie noch die beiden IPs einstellen, zwischen denen Sie lauschen möchten, zum Beispiel Router-IP und die IP des Clients, für den Sie sich interessieren. Klicken Sie hierzu auf den Menüknopf (drei Punkte), „Targets“ und „Current Targets“. Über die Add-Buttons tragen Sie die IPs als Target 1 und Target 2 ein. Alternativ können Sie auch erst mal im lokalen Netz nach Clients scannen. Klicken Sie dafür im Menü unter „Hosts“ auf „Scan for hosts“. Kurz darauf können Sie die Netzwerkteilnehmer unter „Hosts/Host list“ einsehen und per Rechtsklick als Target hinzufügen.

Jetzt müssen Sie das ARP-Spoofing nur noch auslösen: Klicken Sie oben rechts auf den Knopf, der an eine Weltkugel erinnert („MITM menu“) und auf „Arp poisoning...“. Über das Menü und „View/Connections“ können Sie live beobachten, wie die Daten durch Ihr System fließen. Sie erfahren dort unter anderem IP-Adresse, Hostname und Land der Gegenstelle, den genutzten Port und den Datenumfang. Ein Doppelklick auf eine Verbindung zeigt die übertragenen Daten an. Interessant sind zum Beispiel unverschlüsselte HTTP-Verbindungen auf Port 80, weil Sie deren Inhalt ohne weitere Hilfsmittel als Klartext lesen können.

Ettercap bringt einige interessante Plug-ins mit, die Sie im Menü unter „Plugins/Manage plugins“ durchstöbern und per Doppelklick aktivieren können. Darunter findet sich auch ein Gegengift für ARP-Spoofing: Der „arp_cop“ soll ARP-Manipulationen anzeigen. Wenn Ihnen die Analysefunktionen von Ettercap nicht ausreichen, können Sie Werkzeuge wie Wireshark nutzen, denn der angezapfte Traffic ist auf dem anfangs eingestellten Netzwerk-



Verkehrsumleitung: Ettercap nutzt ARP-Spoofing, um den Datenverkehr anderer Rechner über sich umzuleiten.

Interface sichtbar. Mit den Linux-Werkzeugen iptables oder nftables können Sie den Datenverkehr zudem beliebig umleiten, zum Beispiel an einen lokalen Server.

WLAN auf dem Prüfstand

Funknetzwerke müssen viel aushalten, denn jeder in Reichweite kann sie attackieren. Wenn Sie sich nicht darauf verlassen möchten, dass Ihr WLAN schon sicher genug sein wird, können Sie mit Hacking-Tools die Probe aufs Exempel machen. Kali hat mehrere davon an Bord, die unterschiedliche Angriffsszenarien durchspielen. Zur Nutzung benötigen Sie ein WLAN-Interface, das sich in den „Monitor Mode“ schalten lässt und zudem gut von Linux unterstützt wird. Solche gibt es als USB-WLAN-Adapter schon für weniger als 20 Euro, zum Beispiel von CSL Computer (Modell 27395) oder Alfa Network. Ob Ihr Interface den nötigen Modus unterstützt, erfahren Sie über eine Google-Suche nach dem Chipsatz, etwa „Ralink RT5572 monitor mode“.

Um die gängigsten Angriffsarten zu simulieren, können Sie zu **wifite2** greifen, das diverse WLAN-Hacking-Werkzeuge für Sie ansteuert, um Sicherheitsprobleme aufzuspüren. Sie starten es wie folgt:

```
sudo wifite --random-mac --kill
```

Die Option `--random-mac` sorgt dafür, dass die genutzte Geräteadresse des WLAN-Adapters zufällig ausgewürfelt wird und `--kill` beendet störende Prozesse, die dem Tool in die Quere kommen könnten. Wifite fragt Sie zunächst, welches WLAN-Interface genutzt werden soll und macht sich anschließend sofort an die Arbeit. Kurz darauf listet es alle Netze in Reichweite auf.

Sobald Sie Ihr WLAN gefunden haben, beenden Sie den Scan mit Strg+C und geben die Indexzahl des Netzes ein. Wifite testet anschließend die wichtigsten Angriffsmöglichkeiten der Reihe nach durch, allen voran WPS-Attacken (Pixie Dust und Brute Force auf die PIN), die bei anfälligen Routern am schnellsten zum Ziel führen. Danach nimmt sich das Tool WPA(2) zur Brust und schließlich das steinalte WEP-Verfahren. Gegen WPA3 kommt es derzeit nicht an.

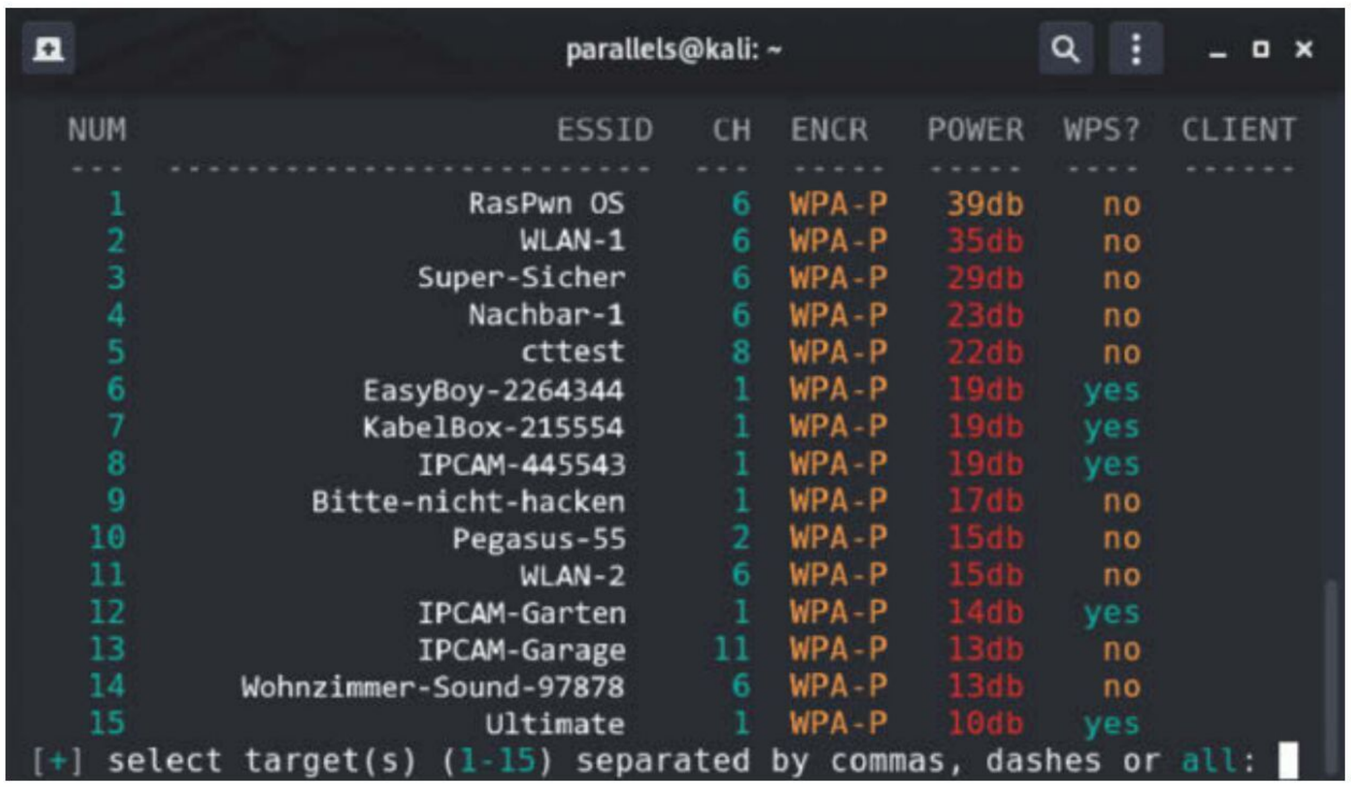
Der WPA(2)-Angriff läuf relativ simpel ab: Zunächst zwingt wifite die Clients per Deauthentication-Paket, die Verbindung zum Router zu trennen. Bei der anschließenden Neuanmeldung zeichnet es den Handshake auf und setzt anschließend den Passwort-Cracker hashcat darauf an. Der probiert eine Reihe von Passwörtern aus einer langen Liste durch, bis er fündig wird. Die wichtigsten Schutzmaßnahmen in aller Kürze: Nutzen Sie lange WPA-Passwörter (mindestens 16 Zeichen, besser mehr), aktivieren Sie möglichst WPA2/3 (Mixed Mode) und die geschützte

Anmeldung von WLAN-Geräten (Protected Management Frames, PMF).

Datenlecks im Webserver finden

Webserver sind prinzipbedingt meist für jeden erreichbar – und damit zwangsläufig auch für Angreifer, die nach Sicherheitslücken, Datenlecks und schwachen Passwörtern suchen. Das geschieht längst nicht mehr mühsam von Hand, sondern automatisiert. So können die bösen Buben tausende Websites innerhalb kurzer Zeit auf Schwachstellen abklopfen und müssen bei der Wahl ihres Angriffsziels nicht wählerisch sein.

Wenn Sie eine Website betreiben, müssen Sie also fest mit ungebetenem Besuch rechnen. Und wenn es eine Sicherheitslücke gibt, wird diese früher oder später auch ausgenutzt. Sie können den Angreifern jedoch die Petersilie verhageln, indem Sie sich deren Tools zu eigen machen, um etwaige Schwachstellen selbst frühzeitig zu finden. Auch diese Tools dürfen Sie nur gegen eigene Server und niemals unbefugt gegen fremde Systeme einsetzen, sonst drohen juristische Konsequenzen (siehe Seite 128). Beachten Sie, dass die Werkzeuge sehr viele Anfragen und damit potenziell auch eine hohe Last erzeugen, was die Erreichbarkeit des Servers beeinträchtigen kann.



Mit wifite2 finden Sie heraus, wie sicher Ihr WLAN wirklich ist. Im ersten Schritt zeigt es alle Netze in Reichweite samt Verschlüsselung und WPS-Status an.

Ein einfaches, aber effektives Werkzeug zur Suche nach Datenlecks ist **DIRB**. Es probiert eine lange Liste mit gängigen Verzeichnisnamen wie /admin, /backups oder /internal durch, um Ordner zu finden, die nicht für die Öffentlichkeit bestimmt, aber trotzdem für jeden zugänglich sind. Ferner kann das Hacking-Programm Verzeichnisnamen per Brute Force erraten. Gibt es einen Treffer, versucht DIRB auch noch mögliche Unterordner zu entdecken. Die Bedienung ist einfach:

```
dirb https://ihre-website.example
```

Unzureichend geschützte Verzeichnisse sind häufig die Ursache für Datenlecks, etwa wenn darin Backups der MySQL-Datenbank oder Konfigurationsdateien mit Zugangsdaten gespeichert sind. Diese Blindgänger sollten Sie rechtzeitig entschärfen, zum Beispiel durch einen Zugriffsschutz auf dem Verzeichnis, sofern die Daten überhaupt auf dem öffentlichen Server liegen müssen.

WordPress-Lücken aufspüren

Das Content-Management-System WordPress ist sehr verbreitet [1] und bei Angreifern entsprechend hoch im Kurs. Häufig wird es in veralteten – und somit verwundbaren – Versionen betrieben oder mit anfälligen Plug-ins und Themes. Auch Konfigurationsfehler begünstigen eine Fremdübernahme. Solche Schlupflöcher aufzudecken ist inzwischen ein Kinderspiel – zum Beispiel mit dem WordPress Security Scanner **WPScan**. Der kann Ihnen gute Dienste beim Absichern Ihrer Website leisten.

Auf der GitHub-Seite des Ruby-Tools erfahren Sie, wie Sie es unter Linux, macOS und als Docker-Container an den Start bringen (siehe ct.de/wrbu). Kali-Nutzer können sich das sparen, das Programm ist vorinstalliert. Um Ihre WordPress-Installation zu scannen, füttern Sie WPScan einfach mit der URL: `wpscan --url https://ihre-website.example/wordpress`

Bevor die Analyse beginnt, lädt der Security Scanner eine Datenbank mit aktuellen Infos aus dem Netz. Das geschieht normalerweise automatisch, wenn Sie es jedoch auf die verwundbaren WordPress-Installationen von RasPwn loslassen möchten (siehe „Angreifen erlaubt“), haben Sie keine Internetverbindung, solange Sie mit dem Raspi-Testnetz verbunden sind.

In diesem Fall sollten Sie sich zunächst mit Ihrem normalen Netz verbinden und das Update mit `wpscan --update` manuell starten. Trennen Sie die Verbin-

dung danach, ehe Sie den Scan aus dem RasPwn-Netz anwerfen. Nach und nach gibt WPScan interessante Informationen über die WordPress-Installation aus, darunter die WordPress-Version samt Erscheinungsdatum und eine Einschätzung, ob diese Ausgabe nach aktuellem Stand der Dinge sicher ist. Weiterhin identifiziert das Tool die Versionen von Webserver und PHP sowie Themes, Plug-ins und diverse Konfigurationsfehler. Prinzipiell kann man selbst im Netz recherchieren, welche Sicherheitslücken in den identifizierten Versionen klaffen. Aber auch das kann Ihnen WPScan abnehmen. Diese Informationen fragt das Tool über ein Web-API vom Server der Entwickler ab – dafür ist eine kostenfreie Registrierung nötig (siehe ct.de/wrbu).

Datenbank-Lecks verhindern

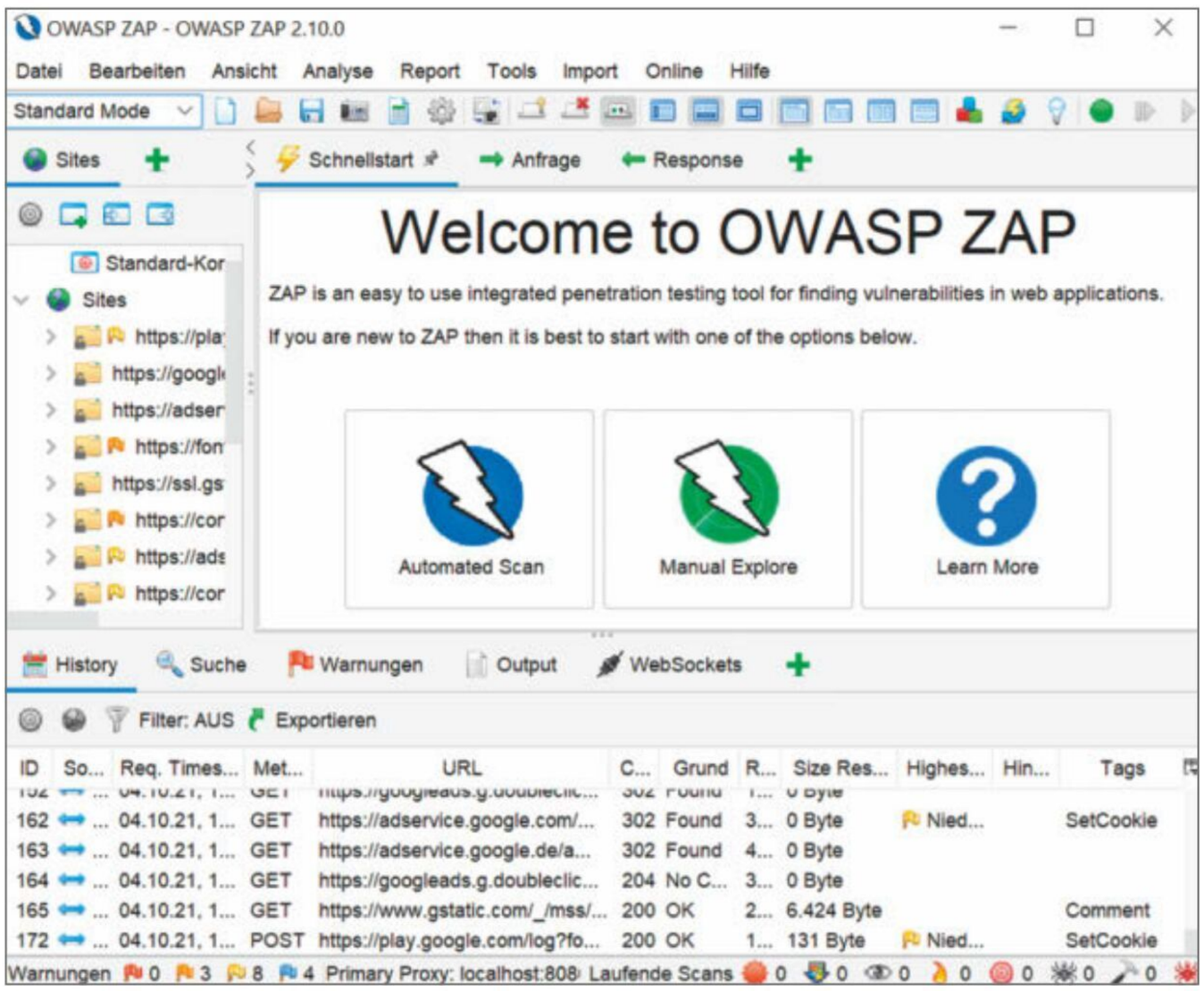
Die Kronjuwelen einer Website sind häufig Kunden- oder gar Nutzerdaten. Diese können Onlinegauner im Darknet leicht zu Geld machen. In der Regel bewahren Webanwendungen solche Daten in einer Datenbank auf, die natürlich gut geschützt sein sollte. Die Betonung liegt auf sollte, denn allzu oft gelingt es Cyberkriminellen, Kundendaten im großen Stil aus Datenbanken abzugreifen.

Eine häufige Ursache sind sogenannte SQL-Injection-Lücken: Dabei spricht der Angreifer nicht direkt mit dem Datenbankserver, sondern versucht stattdessen, die Webanwendung dazu zu bringen, eingeschleuste SQL-Befehle auf der Datenbank auszuführen. Das Resultat ist häufig, dass die Datenbank über die Web-Anwendung massenweise sensible Datensätze ausspuckt.

Sie ahnen es vielleicht schon: Auch für solche Lücken gibt es ein Hacking-Tool, in diesem Fall **SQLmap**. Es unterstützt zahlreiche Datenbanken, unter anderem Oracle, MySQL, MariaDB, MS SQL Server, PostgreSQL und SQLite. Je nach Datenbanktyp und Berechtigungen kann es auch Dateien auf den Webserver schreiben. Hacker können so versuchen, eine Web-Shell hochzuladen, um den Server dauerhaft fernzusteuern.

Für einen ersten Funktionstest können Sie die absichtlich anfällige „Wacko Picko“-Website von RasPwn mit SQLmap scannen. Das Login-Formular der Website sendet beim Abschicken zwei POST-Parameter, nämlich „username“ und „password“, die der Schwachstellenscanner in diesem Beispiel in die Mangel nehmen soll.

Um zu überprüfen, ob die Website bei der Auswertung dieser Parameter patzt, können Sie das Tool



Der Zed Attack Proxy (ZAP) macht verschlüsselten Datenverkehr im Klartext sichtbar und spürt Schwachstellen in Web-Anwendungen und APIs auf.

mit `--data` anweisen, genau das herauszufinden:

```
sqlmap -u "http://wackopicko.play↵
↳ground.raspwn.org/users/login.php" ↵
↳--data="username=1&password=1" ↵
↳--banner
```

Die Option „banner“ findet die Datenbankversion und das Betriebssystem des Servers heraus, wenn die Website verwundbar ist. Falls Sie den Datenbankinhalt gleich auslesen möchten, ersetzen Sie `--banner` einfach durch `--dump`.

Solche SQL-Injections vermeiden Sie, indem Sie Eingaben von außen konsequent überprüfen, bevor sie verarbeitet oder gar in Datenbankbefehle integriert werden. Weiterhin ist der Einsatz sogenannter „Prepared Statements“ sinnvoll, bei denen Sie zunächst den Aufbau des SQL-Befehls festlegen, ehe Sie darin einen Platzhalter mit den von außen angelieferten Werten füllen. Am besten basteln Sie die Datenbankbefehle nicht selbst zusammen, sondern setzen auf eine hinreichend getestete ORM-Bibliothek (Object-Relational Mapping), die bereits gegen alle Eventualitäten abgesichert ist.

Browser- und App-Traffic

Der **OWAP Zed Attack Proxy (ZAP)** ist ein universelles Werkzeug zur Analyse und Manipulation von Web-Traffic (HTTP/HTTPS). Sie können sich damit zum Beispiel zwischen Browser und Internet klemmen oder den Datenverkehr Ihres Smartphones durch den Proxy schleusen, um herauszufinden, welche Daten wohin übertragen werden. Eine Stärke des ZAP ist, dass es die identifizierten Gegenstellen, also Webanwendungen, API-Endpunkte und so weiter gleich noch auf Sicherheitsprobleme abklopfen kann. ZAP ist eine Java-Anwendung und läuft unter Windows, Linux und macOS.

Nach dem ersten Start klicken Sie am besten auf den Browser-Knopf in der Symbolleiste, um einen perfekt vorkonfigurierten Webbrowser zu starten. Dessen Datenverkehr wird automatisch durch den Proxy geschleust. Öffnen Sie damit eine Website, um den Traffic in ZAP zu inspizieren. Wenn Sie den Browser auf diese Weise starten, schleust ZAP in die geöffneten Websites eine eigene Oberfläche namens ZAP HUD ein, über die Sie zahlreiche Funktionen direkt aus dem Browser steuern können. Klicken Sie auf den Knopf „Take the HUD Tutorial“, um eine Einführung zu erhalten und einige der nützlichen Funktionen kennenzulernen.

Gemischtwaren

Dieser Artikel liefert Ihnen nur eine kleine Auswahl an Hacking-Tools. Das Angebot ist riesig und täglich kommen neue dazu. Einige davon sind sehr komplex oder nur für bestimmte Zielgruppen interessant. Dazu zählt das modular aufgebaute Pentesting-Framework **Metasploit**, das professionelle Penetrationtester nutzen, um einen kompletten Angriff zu simulieren: vom Aufspüren der Ziele über das Ausnutzen von Sicherheitslücken bis hin zum Ausleiten der Datenbeute. Falls Sie sich eingehender mit Hacking beschäftigen möchten, sollten Sie einen Blick darauf werfen. In eine ähnliche Kerbe schlägt **PowerShell Empire**, das Pentestern weitreichenden Rechnerzugriff verschafft, ohne verdächtigen Binärcode auf dem System zu hinterlassen – die Angriffsmodule bestehen aus Skripten für die Windows PowerShell.

Wer eine Windows-Domäne administriert, sollte Tools wie **mimikatz** kennen, das Anmeldeinformationen aus dem Arbeitsspeicher der Windows-Clients ausliest. Angreifer gelangen damit schlimmstenfalls an die Zugangsdaten eines Domänen-Administrators und können das gesamte Netzwerk übernehmen. Den Domänencontroller spüren die Eindringlinge vorher mit **AdFind** von joeware auf. Auch **PsExec** aus Microsofts SysInternals-Kollektion birgt ein gewisses Missbrauchspotenzial: Es wird genutzt, um Befehle auf anderen Rechnern im Netzwerk auszuführen. Angreifer nutzen es mit zuvor erbeutete Anmeldeinformationen.

Das von der NSA entwickelte Reverse-Engineering-Toolkit **Ghidra** ist interessant, wenn Sie ausführbaren Code (wie EXE- und DLL-Dateien) bis ins letzte Bit auseinandernehmen und verstehen möchten. Es dekompiliert Binärdateien und kann sie auch wieder zusammenbauen, ähnlich wie der kommerzielle Disassembler IDA Pro. In c’t 14/2020 haben wir Ghidra ausführlicher getestet (siehe ct.de/wrbu).

Fazit

Die vorgestellten Hacking-Tools decken einen weiten Bereich ab. Manche Techniken sind erschreckend simpel, andere fordern viel Einarbeitung und Erfahrung. Sich damit zu beschäftigen lohnt sich aber: Sie lernen so, wie ein Angreifer zu denken und Ihre eigenen Sicherheitsprobleme und -lücken aufzuspüren. Das ist hilfreich – ganz gleich, ob Sie nur eine private WordPress-Site betreiben oder gar für die Sicherheit Ihrer Kunden verantwortlich sind. (rei) c't

Literatur

[1] Jo Bager, **Loslegen mit WordPress**, Was das Content-Management-System so einzigartig macht, c’t 23/2021, S. 60

Hacking-Tools & weitere Infos

ct.de/wrbu

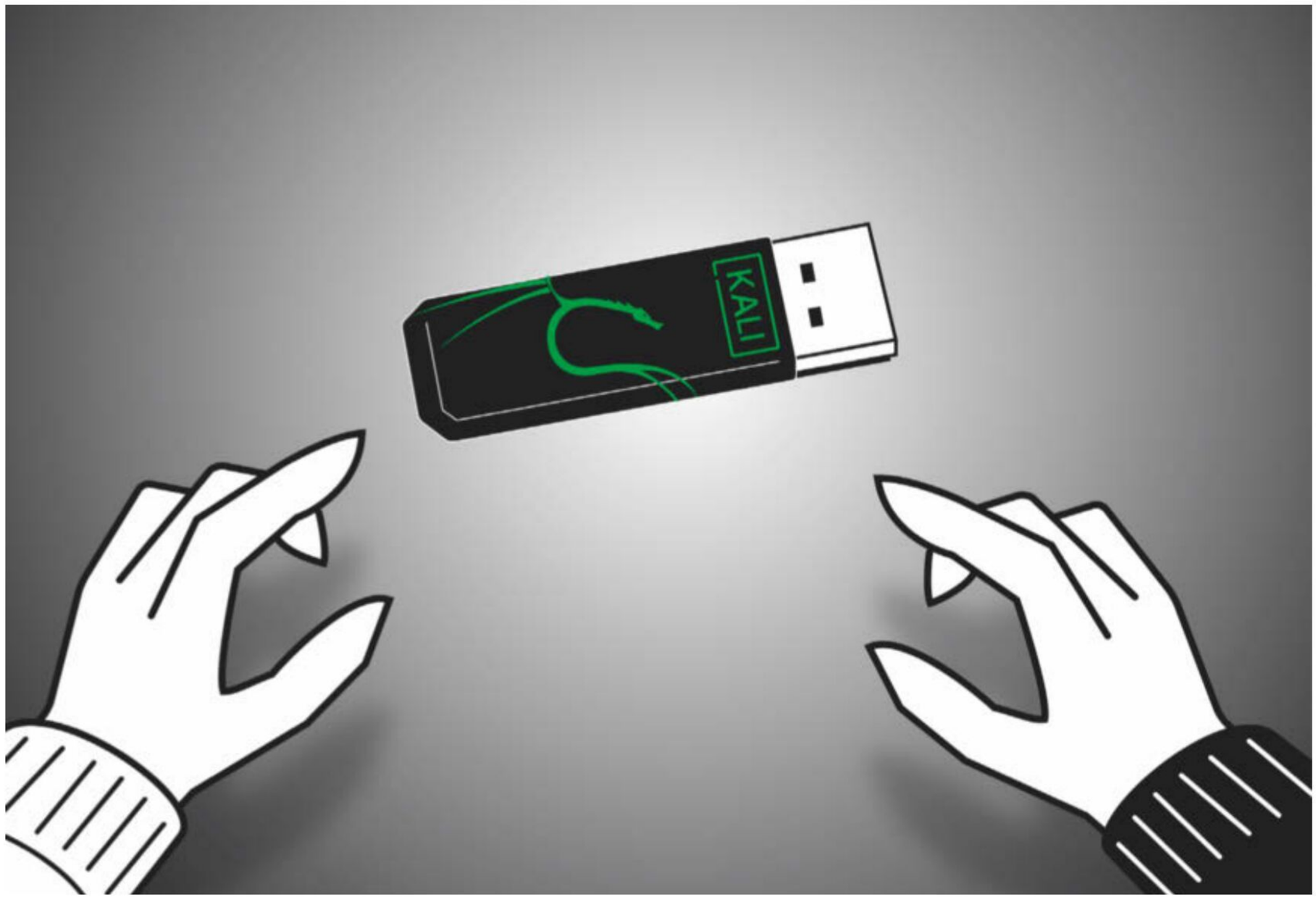


Bild: Sven Hauth

Kali Linux auf USB-Stick einrichten

Mit Kali Linux können Sie etliche Hacking-Tools ohne Installation ausprobieren. Auf einem USB-Stick haben Sie es immer dabei.

Von **Ronald Eikenberg**

Kali Linux ist in vielen Lebenslagen ein nützlicher Helfer: Es enthält etliche Hacking-Tools, die man sofort ausprobieren kann. Die oftmals umständliche Einrichtung der Programme fällt weg. Damit spüren Sie nicht nur Sicherheitsprobleme auf, die mitgelieferten Werkzeuge eignen sich auch zum Daten retten und für vieles mehr. Mit wenig Aufwand erstellen Sie sich einen bootfähigen USB-Stick, mit dem Sie sich selbst davon überzeugen können.

Als Grundlage dient ein Debian, das perfekt auf die Bedürfnisse der Hacking-Community zugeschnitten wurde. Deshalb ist Kali genauso wie einst sein Vorgänger BackTrack Linux seit Jahren die erste Wahl bei Security-Experten und Hackern. Kali lässt sich wie jedes Betriebssystem installieren, doch das ist zum

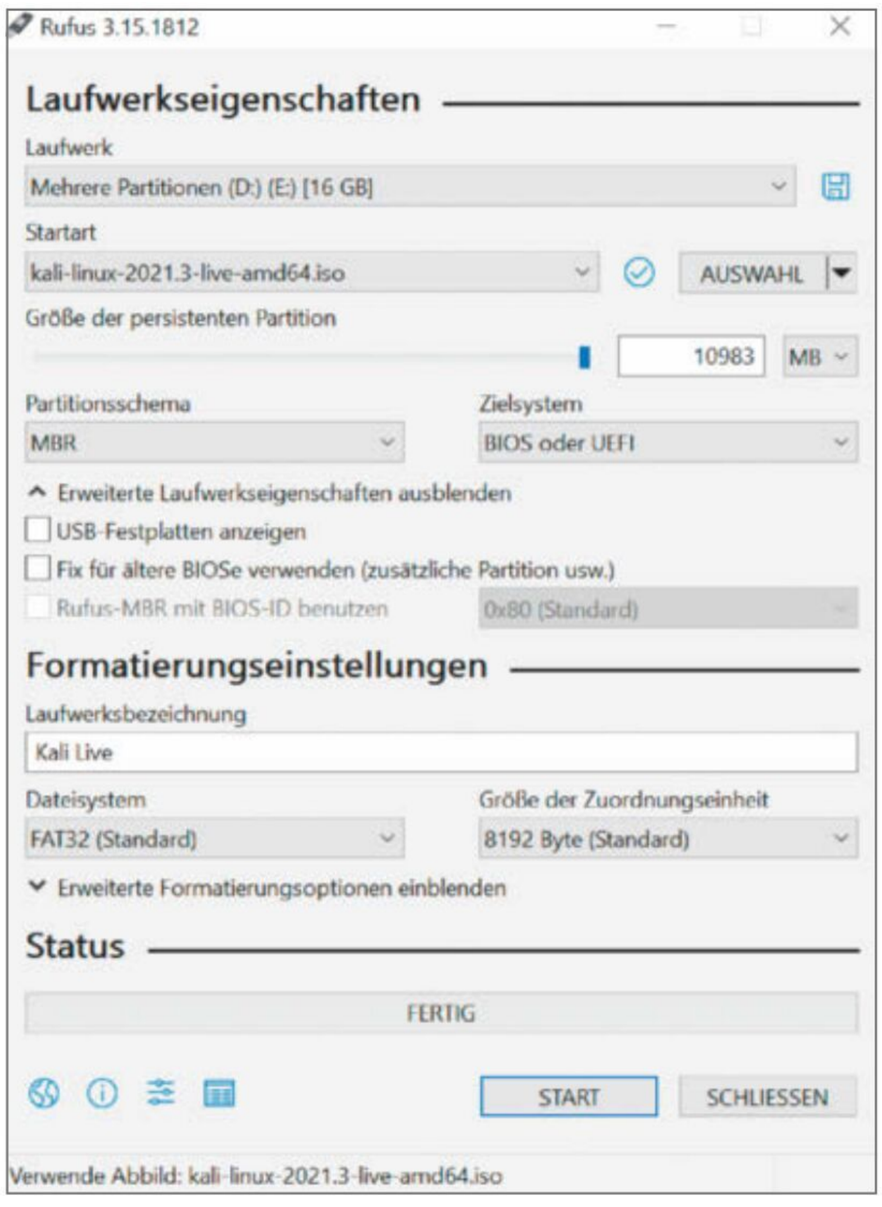
Ausprobieren gar nicht nötig. Im einfachsten Fall läuft das Hacker-Linux als Live-Betriebssystem vom USB-Stick – auf Wunsch auch mit Datenpartition, in der man dauerhaft Daten bunkern kann. Zudem gibt es allerhand virtuelle Maschinen sowie Images für Raspis und das mit Windows 10 eingeführte „Windows-Subsystem für Linux“ (WSL). Kurzum: Wer Kali testen möchte, der hat viele Optionen.

Kali-on-a-Stick

Dieser Artikel zeigt Ihnen das Einrichten eines Kali-Live-Sticks, den Sie universell einsetzen können, sowie die ersten Schritte, damit Sie komfortabel damit arbeiten können. Gegenüber einer virtuellen Maschine hat so ein Live-Stick den Vorteil, dass sein Betriebssystem direkt auf die Hardware des Rechners zugreifen kann. Das ist in Situationen wichtig, in denen ein hardwarenahes Hacking-Tool beispielsweise Direktzugriff auf Netzwerkkarte, USB-Geräte oder GPU benötigt.

Auf der Download-Seite der „Live Boot“-Variante (siehe ct.de/wn63) finden Sie zwei Kali-Versionen: Die stabile und getestete Snapshot-Version (etwa Kali 2021.3) und einen automatisch erstellten Weekly-Build, mit dem Sie näher am Puls der Zeit sind. Er enthält aktuellere Versionen der Komponenten, wodurch der erste Updatelauf schneller über die Bühne geht. Wenn Sie auf Nummer sicher gehen möchten, ist jedoch der Snapshot die bessere Wahl.

Live-Betriebssysteme sind üblicherweise vergesslich. Alle Änderungen am System landen lediglich im RAM und sind nach dem Herunterfahren verloren. Wenn Sie nicht jedes Mal bei Null anfangen möchten, können Sie eine Persistence-Partition anlegen, in der Kali sämtliche Änderungen speichert, einschließlich Einstellungen, Home-Verzeichnis und Updates. Nutzen Sie am besten einen modernen USB-3-Stick, da mit der Geschwindigkeit des Speichers auch die Performance des Live-Systems steht und fällt. Ältere Stick-Semester bremsen das System unnötig aus und haben nicht selten Probleme beim Einsatz als Bootmedium. Moderne und flotte USB-Sticks bekommen Sie bei den bekannten Onlinehändlern bereits für weniger als 10 Euro. Der Stick sollte mindestens 8 GByte fassen.



Klick, Klick, Stick: Rufus erstellt nach ein paar Mausklicks einen bootfähigen Kali-Stick samt Persistence-Partition, in der Sie Daten dauerhaft ablegen können.

Live-Linux mit Gedächtnis

Über das Anlegen der Persistence-Partition müssen Sie sich nicht den Kopf zerbrechen, denn das erledigen Sie beim Beschreiben des USB-Sticks nebenbei. Kali Linux erwartet eine ext3-Partition namens „persistence“, die sich über den gesamten überschüssigen Speicher Ihres Sticks erstrecken kann. Eine hohe Kapazität zahlt sich also aus. Bei einem 8-GByte-Stick kann sich der Speicherbereich für Ihre Daten immerhin bereits auf mehr als 3 GByte entfalten. Damit Kali die Partition erkennt, muss auf ihr eine Datei „persistence.conf“ mit dem Inhalt `/ union` gespeichert sein.

Sie könnten die Partition mit einem Partitionierer Ihrer Wahl (zum Beispiel GParted oder MiniTool Partition Wizard Free) von Hand anlegen, nachdem Sie den Stick mit dem Kali-Image bespielt haben. Doch warum kompliziert, wenn es auch einfach geht? Bei uns hat sich das Windows-Tool Rufus (siehe ct.de/wn63) bewährt, das dem USB-Stick nicht nur das Kali-Image verpasst, sondern im gleichen Arbeitsgang auch eine geeignete Persistence-Partition.

Um einen Persistence-Stick mit Rufus zu erstellen, starten Sie das Tool und wählen ganz oben den angeschlossenen USB-Stick als Schreibziel aus. Anschließend speisen Sie über „Auswahl“ das Kali-ISO ein, zum Beispiel „kali-linux-2021.3-live-amd64.iso“.

Achten Sie darauf, dass der Dateiname „live“ enthält, um sicherzustellen, dass Sie es mit der richtigen Datei zu tun haben – die „installer“-Versionen eignen sich ausschließlich zur Installation, sie enthalten keinen Livemodus.

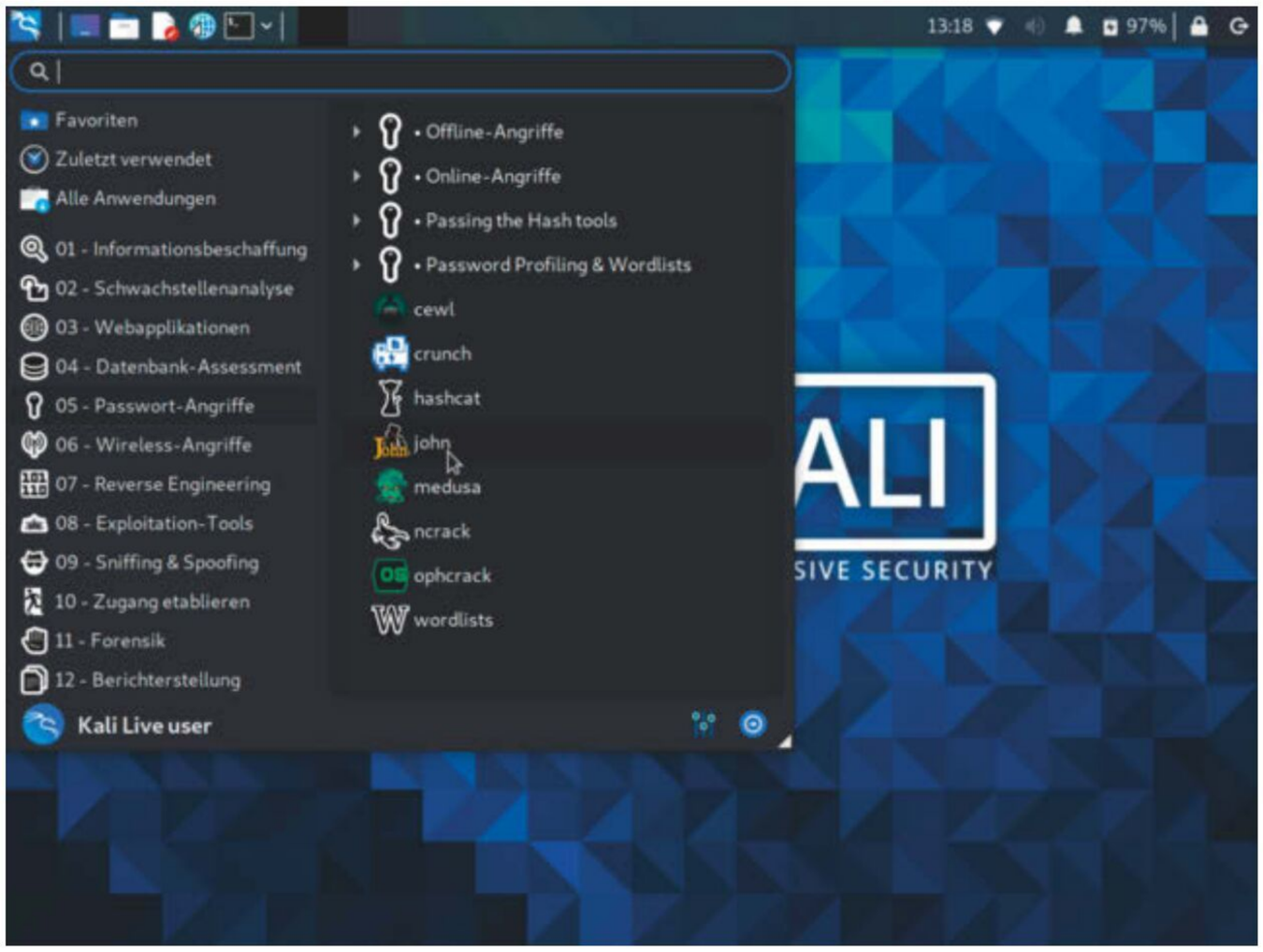
Danach kümmern Sie sich um die Persistence-Partition. Ziehen Sie gleich darunter den Schieberegler „Größe der persistenten Partition“ ganz nach rechts, damit der Persistence-Bereich so groß wie möglich wird. Ändern Sie rechts daneben die Speichergrößeneinheit von „GB“ auf „MB“ und ziehen Sie den Schieberegler erneut nach rechts, um noch ein paar MByte extra herauszuquetschen. Den Rest können Sie auf den Vorgabewerten belassen. Klicken Sie dann auf „Start“ und bestätigen Sie etwaige Rückfragen. Nach einigen Minuten, abhängig von der Schreibgeschwindigkeit Ihres USB-Sticks, ist Kali startklar.

Für Linux und macOS gibt es Rufus leider nicht, Sie können Ihr Glück mit UNetbootin versuchen (siehe ct.de/wn63), das ähnlich funktioniert. Bei uns war es etwas wählerischer bei der Auswahl des Schreibziels, wir konnten aus ungeklärten Gründen nicht jeden USB-Stick damit bespielen. In vielen Fällen hat es jedoch erfolgreich einen bootfähigen Kali-Stick samt Persistence-Partition erzeugt. Wählen Sie unter „Abbild“ einfach das Kali-ISO aus und in das Eingabefeld neben „Platz um Dateien zwischen Neustarts zu erhalten (nur Ubuntu)“ tragen Sie irgendeine Zahl größer Null als Wunschgröße für die Datenpartition ein.

Die eingetippte Zahl wurde bei uns übrigens stets ignoriert, UNetbootin hat stattdessen die maximal mögliche Partitionsgröße genutzt. Abschließend starten Sie das Bespielen mit dem Ok-Knopf. Falls Sie den Stick lieber per Shell vorbereiten möchten, hilft Ihnen die offizielle Kali-Dokumentation weiter (siehe ct.de/wn63). Dort erfahren Sie auch, wie Sie die Partition mit LUKS verschlüsseln, um sie vor unbefugten Zugriffen zu schützen.

Auf Probefahrt

Zeit für eine ersten Testfahrt! Wenn Sie ein aktuelles Windows nutzen, können Sie Ihren Rechner einfach über die erweiterten Startoptionen anweisen, vom Stick zu booten: Öffnen Sie über eine Startmenü-Suche „Optionen für den erweiterten Start ändern“ und klicken Sie unter „Erweiterter Start“ auf „Jetzt neu starten“. Nach dem Neustart wählen Sie die Option „Ein Gerät verwenden“ und anschließend den USB-Stick.



Die Kali-Installation enthält etliche Security-Tools, die man ohne Installation ausprobieren kann.

Es sollte der Grub-Bootmanager im Kali-Design erscheinen, der Ihnen diverse Startkonfigurationen anbietet. Wählen Sie „Live USB Persistence“, damit die Datenpartition des Sticks korrekt eingebunden wird. Falls Sie das nicht wünschen, wählen Sie mit dem obersten Eintrag den regulären Livemodus, der jedes Mal mit einem frischen System startet und nach der Nutzung sämtliche Änderungen vergisst.

Falls Sie den erweiterten Start nicht nutzen können, etwa weil Sie ein anderes Betriebssystem einsetzen, können Sie Ihren Rechner auch regulär vom Stick booten, indem Sie das System mit angeschlossenem Kali-Stick einschalten. Mit etwas Glück klappt der Start sofort, andernfalls müssen Sie im BIOS die Bootreihenfolge ändern oder, falls vorhanden, den Bootmanager des BIOS nutzen, um das System vom Stick zu starten.

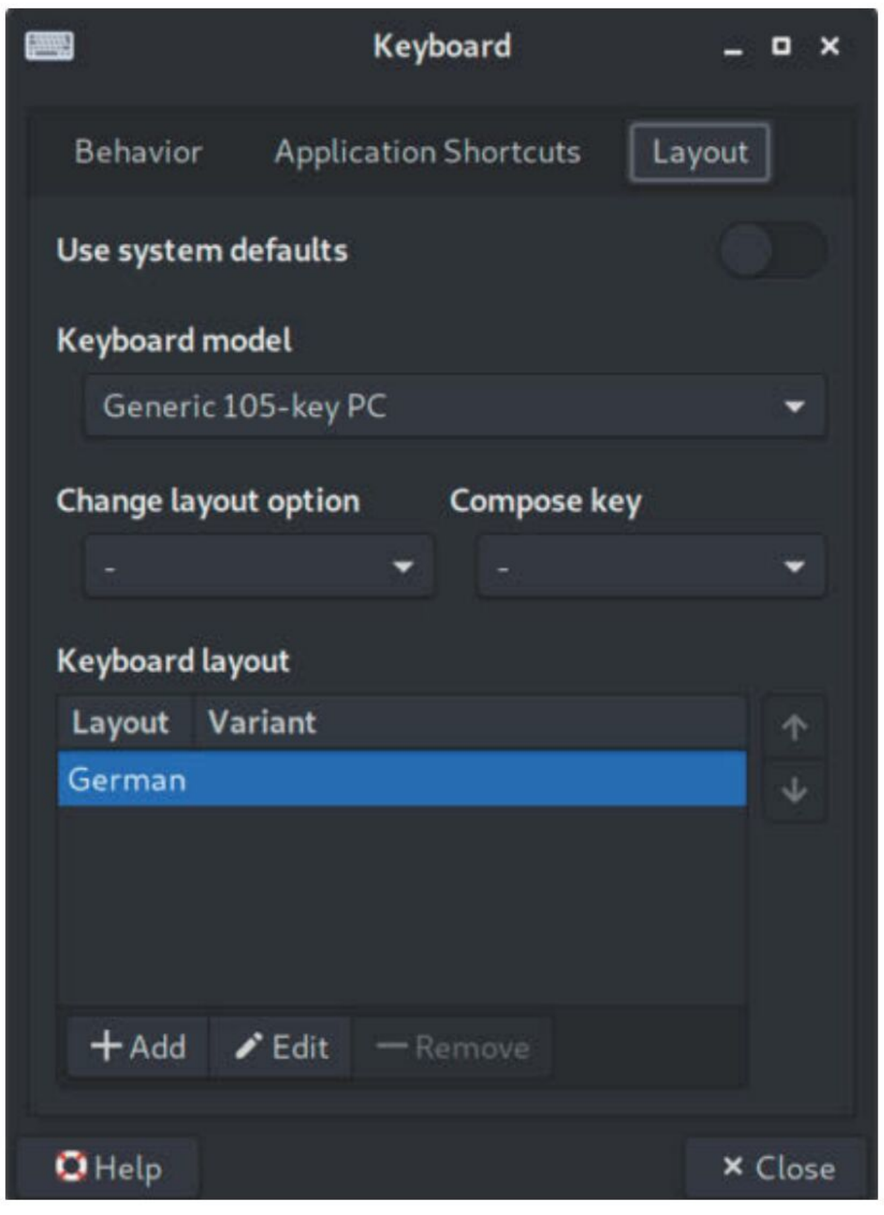
Hierzu drücken Sie direkt nach dem Einschalten des Rechners eine bestimmte F-Taste. Welche genau, erfahren Sie in der Dokumentation des Herstellers oder über eine Google-Suche. Hier kocht jeder Hersteller sein eigenes Süppchen. Bei Asus beispielsweise öffnet sich das BIOS über die F2-Taste, mit F8 erreicht man die temporäre Auswahl des Bootmediums. Falls Sie den Rechner weiterhin nicht

vom Stick starten können, probieren Sie am besten erst eine andere USB-Buchse, sonst einen anderen Stick aus.

Wenn Secure Boot in Ihrem Rechner aktiv ist, müssen Sie es zumindest vorübergehend im BIOS deaktivieren, da die Signaturüberprüfung an Kalis UEFI-Bootloader scheitert. Bei Surface-Geräten kann das Abschalten von Secure Boot dazu führen, das Sie später einmalig den Bitlocker-Wiederherstellungsschlüssel eingeben müssen, den Windows bei der Ersteinrichtung im Microsoft-Konto für Sie speichert.

Erste Schritte

Hat alles geklappt, bootet Kali nach kurzer Zeit automatisch bis zum Desktop durch, die Eingabe eines Passworts ist nicht nötig. Falls sich Kali nach einiger Zeit der Inaktivität sperrt, erlangen Sie mit dem vorgegebenen Nutzernamen `kali` und dem gleichnamigen Passwort `kali` wieder Zugriff.



Erste Amtshandlung: Im Live-Modus sollte man zunächst das Tastaturlayout ändern.

Die Xfce-Desktopumgebung macht Ihnen den Einstieg in die Kali-Welt leicht: Das Bedienkonzept unterscheidet sich nicht von anderen modernen Betriebssystemen. Ein wichtiger Dreh- und Angelpunkt ist das Kali-Menü, das Sie über das Logo oben links und über die Windows-Taste erreichen. Hier finden Sie die Einstellungen und alle wichtigen Hacking-Tools, die bereits installiert sind. Die Kategorien wie „Password Attacks“ und „Wireless Attacks“ helfen Ihnen, sich zurechtzufinden und nützliche Werkzeuge zu entdecken.

Darunter befinden sich Klassiker wie Wireshark, Nmap, OWASP ZAP, Metasploit, aber auch exotischere Spezialtools, die nur für ganz bestimmte Aufgaben nützlich sind. Falls Sie schon wissen, wonach Sie suchen, können Sie einfach das Suchfeld ganz oben benutzen, um das gewünschte Tool aufzuspüren und zu starten. Eine Auswahl interessanter Hacking-Tools und Tipps zur Bedienung finden Sie auf Seite 114.

Nach dem ersten Start sind noch ein paar Handgriffe nötig, um komfortabel arbeiten zu können, denn das System läuft mit einer Standardkonfiguration und ist noch nicht an die hiesigen Bedürfnisse angepasst. So ist etwa das QWERTY-Tastaturlayout eingestellt, was unter anderem die Eingabe von Shell-Befehlen erschwert. Solche Einstellungen werden normalerweise während der Installation abgefragt, die Sie mit dem Livesystem gewissermaßen übersprungen haben. Doch das ist schnell korrigiert.

Tastaturlayout ändern

Starten Sie die Tastatureinstellungen im Kali-Menü über „Settings / Keyboard“ und wechseln Sie auf den Registerreiter „Layout“. Deaktivieren Sie ganz oben den Schalter „Use system defaults“, um die darunterliegenden Einstellungen zu entsperren. Anschließend klicken Sie auf den „Add“-Button und wählen „German“ aus. Die Untervarianten hiervon können Sie ignorieren. Nach dem Hinzufügen können Sie „English“ über „Remove“ entfernen, da es nicht länger benötigt wird.

Falls Sie die Bedienoberfläche auf Deutsch umstellen möchten, öffnen Sie einfach den Terminal Emulator und tippen dort den folgenden Befehl ein: `sudo localectl set-locale LANG=de_DE.UTF-8`. Sobald Sie sich über den Abmelden-Knopf in der rechten oberen Ecke des Bildschirms ausloggen („Log Out“) und wieder anmelden (mit kali / kali), spricht Kali Deutsch. Selbst die Tool-Kategorien im Kali-Menü sind übersetzt, was die ersten Schritte erleichtert.

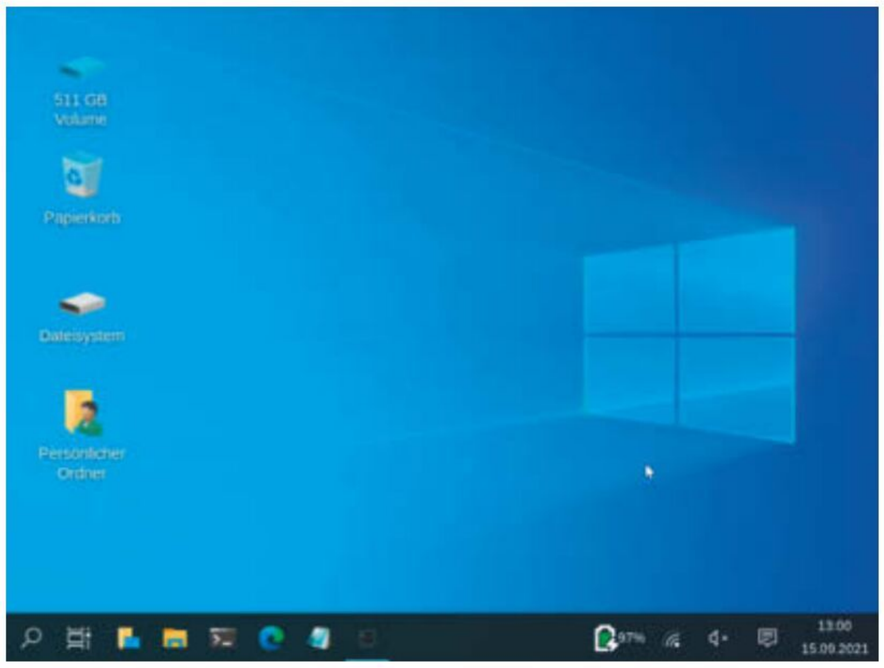
Wenn Sie mögen, ändern Sie jetzt noch das Anzeigeformat der Uhr oben rechts nach einem Rechtsklick übers Eigenschaften-Menü von 12 auf 24 Stunden. Rechts neben der Uhrzeit finden Sie das Network-Manager-Applet, über das Sie eine WLAN-Verbindung zum Router schaffen können – zum Beispiel für Updates. Dazu gleich mehr.

Falls Sie ein Notebook oder Display mit hoher Auflösung auf verhältnismäßig kleiner Fläche nutzen, zum Beispiel ein 15-Zoll-Notebook mit 4K-Display, dann wird Ihnen die dargestellte Kali-Bedienoberfläche möglicherweise winzig vorkommen. Mehr Bedienkomfort gibt es im HiDPI-Modus, der fast alles auf 200 Prozent skaliert, wie man es zum Beispiel von Windows kennt. Suchen Sie im Kali-Menü nach dem „Kali HiDPI Mode“ und starten Sie ihn. Die Änderung ist sofort aktiv. Auf dem gleichen Weg können Sie auch den ursprünglichen Skalierungsmodus wiederherstellen. Auf grafische Anwendungen, die als root gestartet werden, hat der HiDPI-Modus derzeit leider keine Auswirkungen. Über das Menü „Anzeige“ können Sie die Darstellung weiter verfeinern, etwa durch Ändern der Auflösung oder individuelle Skalierungsstufen (dabei sind auch negative Werte erlaubt).

Die Shell ist Dein Freund

Auch wenn viele Tools eine grafische Oberfläche haben: Der Dreh- und Angelpunkt ist das Terminal. Mit Kali nutzen Sie die moderne Z-Shell (ZSH), mit der die Eingabe der Befehle so bequem wie möglich ist. Sie erfahren bereits beim Tippen, ob Sie auf dem richtigen Weg sind: Solange Ihre Eingabe rot gefärbt ist, würde die Ausführung zu einem Fehler führen. Bekannte Befehle erscheinen grün und mit der Tabulatortaste können Sie die aktuelle Eingabe von der Shell vervollständigen lassen. So genügt es oft, die ersten Zeichen eines Kommandos einzugeben und Tab zu drücken. Genauso einfach hängen Sie Dateipfade an einen Befehl an, zum Beispiel, wenn Sie eine Datei mit Hashes in den Passwortknacker John the Ripper (siehe Seite 111) speisen möchten. Mit Strg+Alt+T öffnen Sie jederzeit ein neues Terminalfenster, Strg+Umschalt+T öffnet ein neues Tab in einem existierenden Terminal.

Wenn Sie Kali (oder seinen Vorfahren BackTrack) von früher kennen, wird Ihnen auffallen, dass Sie im System nicht länger als root mit uneingeschränkten Rechten unterwegs sind, sondern als „kali“. Manche Tools benötigen jedoch weiterhin Superuser-Rechte, zum Beispiel bestimmte Betriebsmodi des Netzwerkscanners Nmap (siehe S. 115). Für solche Fälle starten Sie das Tool einfach mit einem vorangestellten `sudo` als root. Dies ist auch für viele Eingriffe ins System nötig, etwa zur Installation von Paketen und Updates. Hilfe zur Nutzung der Tools und Befehle erhalten Sie meist über `man befehl` oder, indem Sie `-?` oder `--help` an den Befehl anhängen.



Kali tarnt sich auf Wunsch als Windows 10.

Kali frischmachen

Mit den folgenden Befehlen bringen Sie Kali und die Tools auf den aktuellen Stand:

```
sudo apt update

sudo apt full-upgrade
```

Kali aktualisiert zunächst die Paketlisten und installiert anschließend die Updates. Je nachdem, wie aktuell Ihre Kali-Installation ist, kann dabei viel Zeit ins Land ziehen. Auch die Schreibgeschwindigkeit Ihres USB-Sticks spielt eine große Rolle. Möchten Sie ausschließen, dass der Upgrade-Vorgang zwischendurch darauf wartet, dass Sie Rückfragen beantworten, können Sie ein `-y` an den zweiten Befehl hängen, um alle Fragen im Vorfeld pauschal mit „Ja“ zu bestätigen.

Tools nachrüsten

Falls Ihnen mal ein Tool fehlt, dann können Sie es wahrscheinlich aus dem Kali-Repository nachinstallieren. Sie können zum Beispiel nach Zenmap suchen, der grafischen Oberfläche für den Netzwerkscanner nmap: `apt search zenmap`

Danach installieren Sie den einzigen Suchtreffer zenmap-kbx mit `sudo apt install zenmap-kbx`. Das ist eines der ersten Tools, die als Kaboxer-Paket (Kali Applications Boxer) angeboten werden, was Sie an dem Namensbestandteil -kbx erkennen. Es handelt sich dabei um ein neues Containerformat, durch das sämtliche Abhängigkeiten in den passenden Versionen mitgeliefert werden können, ohne dass sie separat installiert werden müssen – ähnlich wie bei einem Docker-Container.

Damit löst das Kali-Team das alte Problem, dass manche Tools aufgrund Ihrer Abhängigkeiten umständlich zu installieren sind oder sich mit anderen Tools in die Quere kommen. Ist der Vorgang abgeschlossen, können Sie das neue Tool über das Kali-Menü oder per Shell starten, in diesem Fall mit `sudo zenmap-kbx`.

Entdecke die Möglichkeiten

Mit Ihrem Kali-Stick steht Ihnen eine prall gefüllte Werkzeugtasche zur Verfügung, die Ihnen in vielen Situationen gute Dienste leistet. Die meisten Tools lassen sich zwar in die Oberkategorie „IT-Security“ einsortieren, doch Kali kann viel mehr. Wenn die Systemplatte streikt, können Sie mit TestDisk von Ihrem Stick einen Reparaturversuch starten und mit PhotoRec retten Sie verloren geglaubte Dateien. GParted ist ein leistungsfähiges grafisches Partitionierungsprogramm und Guymager erstellt Datenträgerabbilder, die sogar den Ansprüchen von Forensikern genügen. Falls Sie das Thema Forensik vertiefen möchten, sei Ihnen auch die Bootoption „forensic mode“ ans Herz gelegt: In diesem Betriebsmodus nimmt Kali keine Änderungen am System vor, was primär bedeutet, dass Laufwerke nie automatisch eingehängt werden. So kann man zum Beispiel ein Abbild der Festplatte ziehen, ohne Ihren Ist-Zustand zu verändern.

Zu guter Letzt sei noch der Undercover-Mode von Kali erwähnt, der mehr als eine Spielerei ist: Wenn Sie die Verknüpfung „Kali Undercover Mode“ über das Kali-Menü starten, verkleidet sich das Hacker-Linux kurz darauf als Windows 10. Die Taskleiste wandert Windows-typisch nach unten, als Hintergrundbild erscheint das blaue Windows-Bild. Das ist nicht nur witzig, es erlaubt Kali-Nutzern auch, im Alltag abzutauchen – und verhindert lästige Fragen neugieriger Mitmenschen.

Es gibt viel zu entdecken. Nehmen Sie sich etwas Zeit, um die zahllosen Möglichkeiten von Kali zu erkunden. Manchmal ist etwas Einarbeitung nötig, doch Sie erlernen wertvolles Hintergrundwissen darüber, wie die Dinge funktionieren und können fortan hinter die Kulissen blicken: Sorgt die neue Smart-Home-Kamera für mehr Sicherheit oder lässt sie auch Einbrecher in Ihr Wohnzimmer blicken? Wie lange hält Ihr WLAN einem Angriff stand? Ist Ihre WordPress-Installation ausreichend gegen Hacker geschützt? Mit Kali finden Sie es heraus. Inspiration liefert Ihnen der Artikel auf Seite 114, der viele wichtige und nützliche Tools detailliert vorstellt. (rei) c't

Kali-Download & Tools

ct.de/wn63

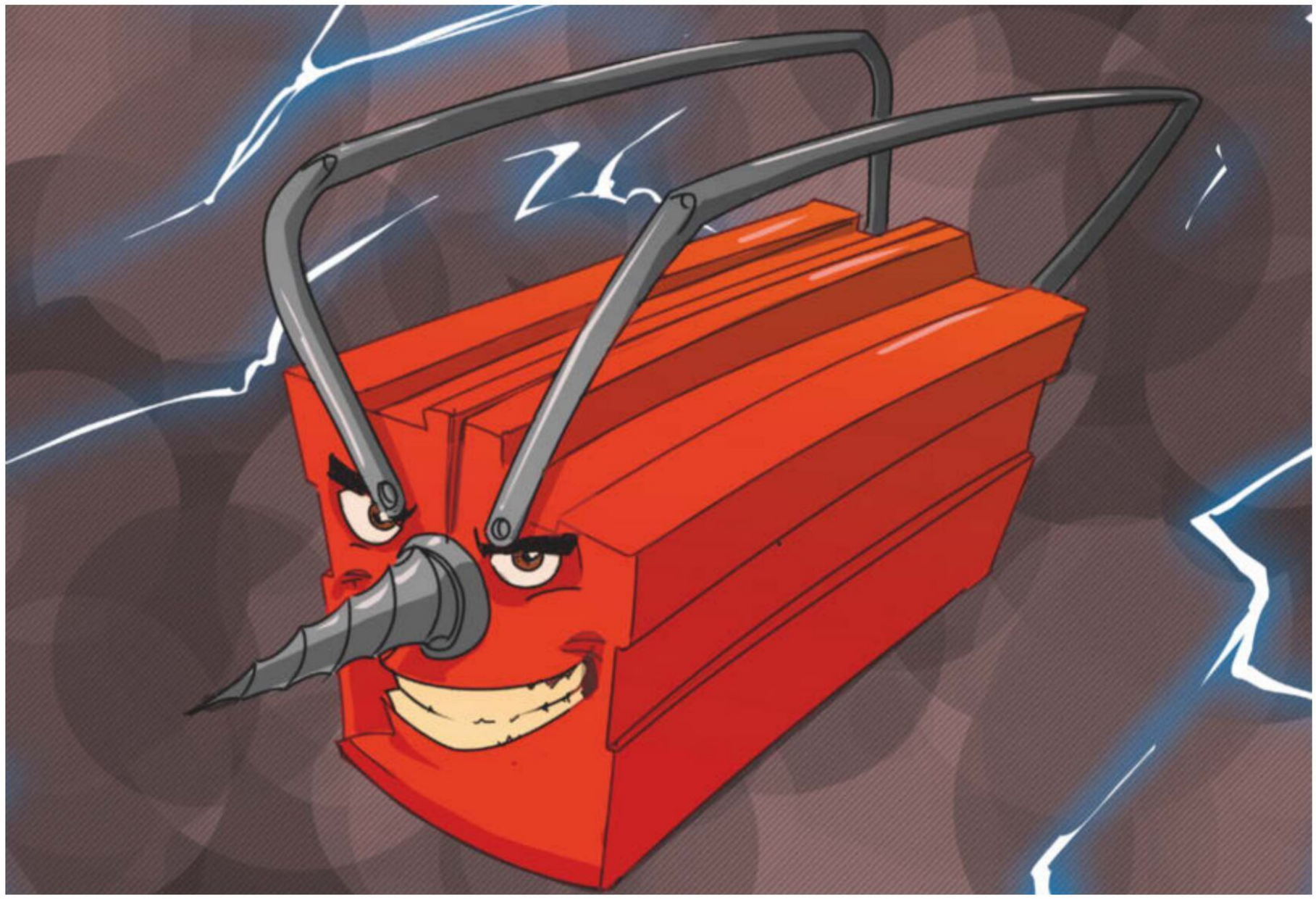


Bild: Thorsten Hübner

Rechtliche Aspekte bei Hacking-Tools

Um Schwachstellen im eigenen Netz zu suchen und Datenflüsse zu überwachen, nutzen Administratoren vielfach die gleichen Softwarehilfsmittel wie Angreifer, die illegale Ziele verfolgen. Was sagt das deutsche Recht dazu? Steht jemand, der mit trickreichen Analyse- und Spähtools arbeitet, mit einem Bein vor Gericht?

Von **Verena Ehrl**

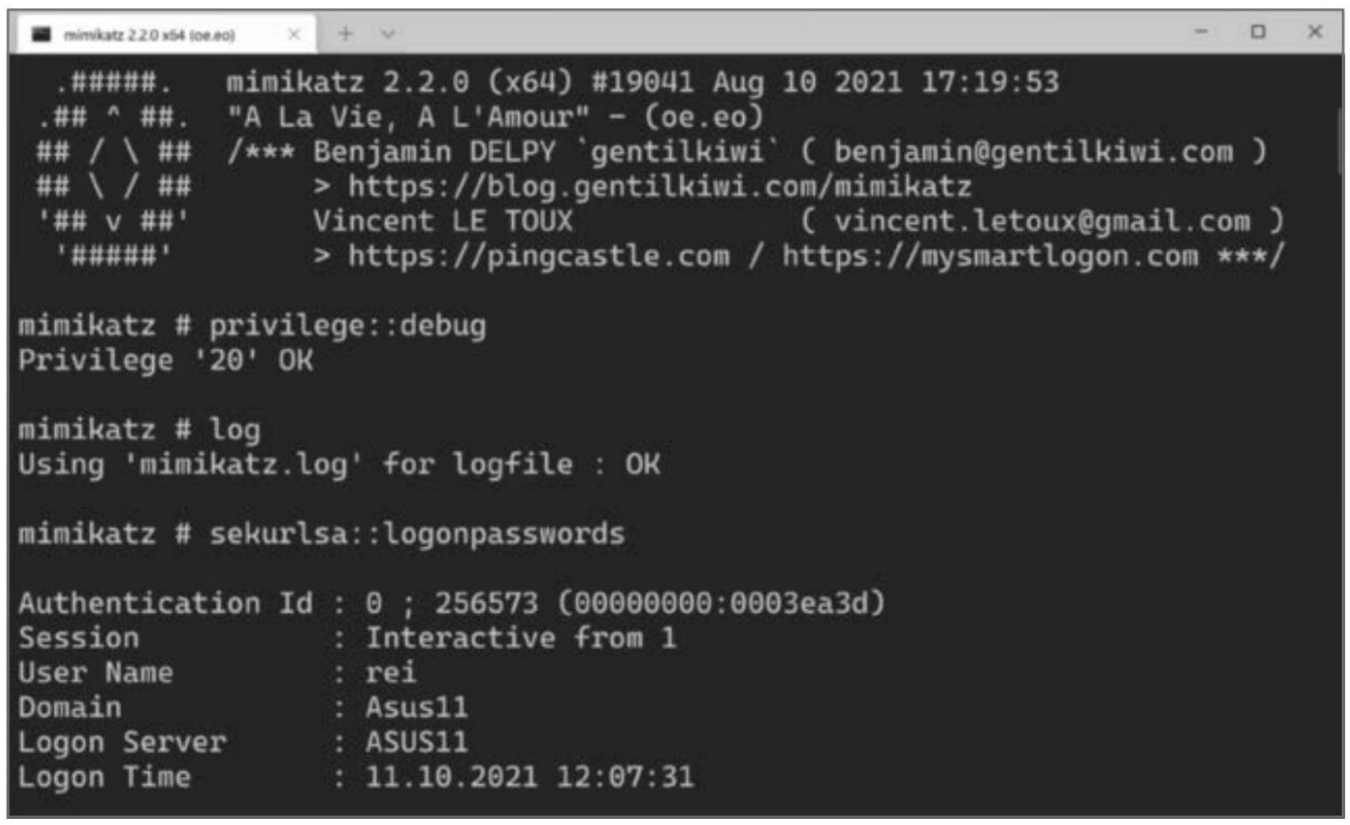
Der Theaterautor und Sprachliebhaber Hans-Joachim Haecker brachte die Dual-Use-Problematik bereits 1968 in einem Gedichtchen seines Bandes „Insonderheit“ unter dem Eindruck des internationalen Wettrüstens scherzhaft auf den Punkt: „Insonderheit die Abwehrwaffen sind für die Abwehr wie geschaffen. Auch kann man mit geschickten Händen sie für den Angriff gut verwenden.“

Die Waffen, mit denen Akteure innerhalb der IT-Welt hantieren, eignen sich zum Eindringen in Systeme, zum Überwinden von Sicherungsmaßnahmen, zum Spionieren und Manipulieren. Dieselben Werk-

zeuge können aber dazu dienen, unterschiedliche Ziele zu erreichen. In der Hand eines Administrators, der ein System, für das er verantwortlich ist, Penetration Tests („Pentests“) aussetzt, kann etwa das Software-Tool „Mimikatz“ legalen Einsatz finden (S. 114). Es ebnet allerdings ebenso gut Angreifern den Weg bei illegalen Aktionen, indem es ihnen Zugangsdaten für die Übernahme eines Netzwerks offenbart. Auf diese Ambivalenz bezieht sich das Schlagwort „Dual Use“ im Zusammenhang mit Hackerausrüstung.

Nicht immer erscheinen die Werkzeuge, um die es geht, so spektakulär wie die Hacking-Gadget-Hardware, mit der c’t sich bereits in vergangenen Jahren befasst hat [1, 2]. Sehr oft steht vielmehr bloße Software im Mittelpunkt, die loggt, sucht, entschlüsselt, ausliest, analysiert und speichert (S. 104, 106, 114, 122). Die rechtlichen Fragen, vor die ein Anwender gestellt ist, sind jedoch grundsätzlich die gleichen wie bei den Spionagegerätchen [3]: Wo liegt die rote Linie, jenseits der man sich auf illegalem Terrain bewegt? Was sagt das geltende Recht zum Umgang mit potenziell gefährlichen und schadenträchtigen Tools?

Dass es „Güter mit doppeltem Verwendungszweck“ gibt, die sich gleichermaßen für legales und illegales Tun eignen, beschäftigt nicht zuletzt den europäischen Gesetzgeber. Am 9. September 2021 ist die Neufassung der sogenannten Dual-Use-Verordnung in Kraft getreten [4].



Mimikatz ist ein typisches Beispiel für ein Hackerwerkzeug, das auch verantwortungsvollen Admins wertvolle Dienste leistet, wenn es ums Aufspüren von Schwachstellen im eigenen Netz geht.

Sie betrifft „Güter einschließlich Datenverarbeitungsprogramme (Software) und Technologie, die sowohl für zivile als auch für militärische Zwecke verwendet werden können“. Es gibt durchaus Softwareentwicklungsprojekte, die man mit etwas Fantasie in den Betrachtungshorizont der Verordnung rücken kann.

Ziel der Dual-Use-Verordnung ist die Exportkontrolle. Die kann bereits relevant werden, wenn Forschung und Produktentwicklung mit Partnerunternehmen in bestimmten außereuropäischen Ländern stattfinden und dabei schadenträchtige Software im Spiel ist.

Neu im Blick der europäischen Rechtssetzungsorgane und der zur Umsetzung verpflichteten Mitgliedsstaaten sind Länder, welche die Todesstrafe praktizieren oder in denen Menschenrechtsverletzungen wie Folter auf staatliches Geheiß stattfinden. Wer etwa potenziell gefährliche Software ins nichteuropäische Ausland transferieren will, braucht dazu eine vorherige Genehmigung des Bundesamts für Wirtschaft und Ausfuhrkontrolle (BAFA). Diese Behörde entscheidet in jedem Einzelfall, ob der Transfer zulässig ist oder nicht.

Zweierlei Paar Schuhe

Abseits der von der Verordnung erfassten Transferproblematik sind Dual-Use-Softwarewerkzeuge rechtlich schwer zu fassen. Weder ihr Erwerb noch ihr Besitz ist grundsätzlich untersagt. Straf- und Zivilrecht melden sich erst dann, wenn jemand diese Tools einsetzt, um Rechtsbrüche zu begehen. Derjenige riskiert dann eine Strafe oder er sieht sich zivilrechtlichen Ansprüchen ausgesetzt – oft droht ihm beides.

Nicht alles, was jemand rechtswidrig tut, ist auch strafbar. Mit dem Strafrecht geht der Staat gegen von ihm untersagtes Verhalten vor. Dabei sind Strafermittlungsbehörden im Spiel, es gibt Beschuldigung und Anklage. Im Zivilrecht stehen hingegen gleichberechtigte Streitparteien einander gegenüber. Dabei gibt es Kläger und Beklagte, die Gerichte entscheiden über Ansprüche, welche die Parteien gegeneinander geltend machen. Vertragspflichten und Schadenersatzansprüche sind typisches zivilrechtliches Geschäft.

Durch Software kann ein Anwender sich Ärger in beiden Rechtsbereichen einhandeln. Ein gutes Beispiel für die rechtliche Gratwanderung dabei sind die bereits angesprochenen Pentests. Sie haben die Aufgabe, Schwachstellen in Konfiguration, Hard- und

Software von Servern, Routern und Arbeitsplätzen im Netz aufzuzeigen. Ein Mitarbeiter, der einen solchen Test im Auftrag eines zuständigen Entscheiders für das betroffene Netz durchführt, bewegt sich damit auf der legalen Seite. Wenn allerdings etwa ein Cybersecurity-Dienstleister einen Pentest unaufgefordert und ohne Erlaubnis bei einem potenziellen Kunden durchführt, um diesen als Auftraggeber zu gewinnen, setzt er sich strafrechtlicher Verfolgung wegen Datenveränderung oder Computersabotage aus.

Wesentlich sind dabei die Paragrafen 303a und 303b des Strafgesetzbuchs (StGB), die sich mit virtueller Sachbeschädigung befassen. Damit hat der Gesetzgeber 1986 eine Regelungslücke beim Straftatbestand der Sachbeschädigung (§ 303 StGB) geschlossen. Die klassische Sachbeschädigung setzt einen körperlichen Gegenstand voraus – das lässt Daten und beispielsweise Festplatten, die funktionsfähig bleiben, aber deren Inhalt gelöscht oder verschlüsselt wurde, außen vor.

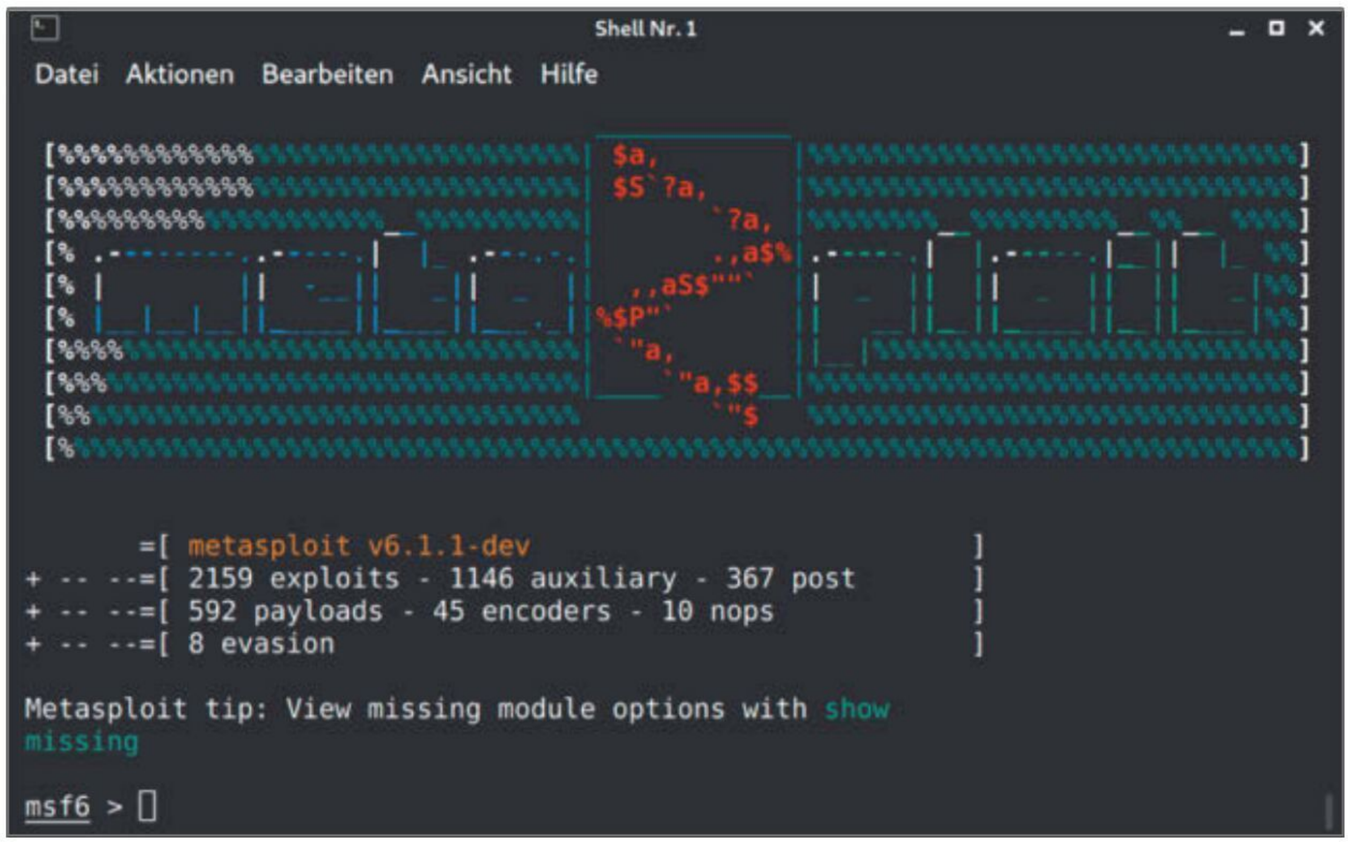
§ 303a StGB stellt die unbefugte Veränderung von Daten unter Strafe. Dort heißt es in Absatz 1: „Wer rechtswidrig Daten (§ 202a Abs. 2) löscht, unterdrückt, unbrauchbar macht oder verändert, wird mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft."

Bereits der Versuch ist strafbar; dasselbe gilt wie beim Ausspähen (§ 202a StGB) und Abfangen von Daten (§ 202b StGB) auch fürs „Vorbereiten" einer rechtswidrigen Datenveränderung – beispielsweise durch Bereitstellen von Software, deren „Zweck die Begehung einer solchen Tat ist" (§ 202c Abs. 1 Nr. 2 StGB). Hierbei sind nicht Dual-Use-Werkzeuge im Blick, sondern Spezialsoftware, die eindeutig auf den Zweck ausgerichtet ist, damit eine Straftat zu begehen.

Als „Daten" im Sinne der hier genannten Paragrafen gelten nach § 202 StGB „nur solche, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden", also nicht etwa Papiernotizen.

§ 303b StGB, der sogenannte Hackerparagraf, ist der Computersabotage gewidmet. Er steht in direktem Zusammenhang mit seinem Nachbarn, der die Datenveränderung betrifft, und lautet: „Wer eine Datenverarbeitung, die für einen anderen von wesentlicher Bedeutung ist, … erheblich stört, … wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft."

Wenn es um die Datenverarbeitung eines Unternehmens respektive einer Behörde geht, stehen



Das modulare Pentesting-Tool Metasploit ist bei Security-Experten beliebt, es lässt sich aber auch für echte Angriffe missbrauchen.

Freiheitsstrafen bis zu fünf Jahren im Raum. In besonders schweren Fällen riskieren Täter sogar bis zu zehn Jahren Gefängnis. Der Paragraf grenzt die Wege, auf denen die strafbare Datenverarbeitungsstörung bewirkt wird, näher ein: Unter Nr. 1 fasst er die Störung durch Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern von Daten (siehe § 303a Abs. 1). Unter Nr. 2 erscheint die Dateneingabe und Datenübermittlung mit der Absicht, jemand anderem einen Nachteil zuzufügen. Unter Nr. 3 schließlich geht es darum, dass eine Datenverarbeitungsanlage oder ein Datenträger zerstört, beschädigt, unbrauchbar gemacht, beseitigt oder verändert wird. Auch hierbei sind wie bei der Datenveränderung bereits Versuch und Vorbereitung strafbar.

Dass es nur ums Stören von Datenverarbeitungen von „wesentlicher Bedeutung" geht, soll Bagatellfälle aus dem Blick der Strafjustiz nehmen.

Erpressungstrojaner vor Gericht

Im April 2021 hat der Bundesgerichtshof (BGH) einen Fall entschieden, der die Verteilung von Ransomware betraf – also das Einschleusen von Verschlüsselungstrojanern zu Erpressungszwecken [5]. Dabei stufte das Gericht unter anderem das Anbringen einer Eintragung in der Windows-Registry, die das automatische Laden einer Schadsoftware beim Rechnerstart

bewirkte, als strafbare Datenveränderung ein. Zugleich sah der BGH in diesem Fall auch eine Computersabotage nach § 303b StGB.

Der Angeklagte war Mitglied einer Cybercrime-Bande mit Sitz in der Ukraine. Diese hatte mit ihren Ransomware-Angriffen von 2013 bis 2016 über 200 Millionen Rechnersysteme infiziert und von den geschädigten Computernutzern mehr als neun Millionen Euro erpressen können.

Schadsoftware ähnlicher Art mit einer vorgesehenen Entsperrmöglichkeit hätte aber auch im Rahmen eines Pentests in einem lokalen Netz durchaus legal verwendet werden können. Ein Unternehmen hätte damit etwa seine Mitarbeiter auf deren Vorsicht testen können, was das Anklicken unbekannter Inhalte betrifft.

Computersabotage am Arbeitsplatz

Das mutwillige Stören des Datenverarbeitungsbetriebs kann nicht nur strafrechtliche, sondern auch arbeitsrechtliche Auswirkungen haben. Mitarbeiter, die aus Wut oder infolge von Rachegedanken gegen ihren Arbeitgeber Datenvandalismus im Unternehmensnetz betreiben, riskieren eine fristlose Kündigung.

In der Hand von Angreifern kann auch der Fern Wifi Cracker, mit dem man Drahtlosnetze auf Sicherheitslücken abklopft, zum Werkzeug für eine Straftat werden.

Das geschah 2019 einem als Key-Account-Manager beschäftigten Arbeitnehmer nach einer heimlichen Löschaktion auf dem Unternehmensserver seines Arbeitgebers. Nach einer Abmahnung war ihm zuvor ein Aufhebungsvertrag angeboten worden. Daraufhin löschte er 8 GByte an Daten, darunter Kalkulationssoftware, Umsatzmeldungen, Vorlagen für Preislisten und Wettbewerbsanalysen für bestimmte Produkte. Die Daten konnten später wiederhergestellt werden. Der Verdacht fiel auf ihn. Gegen die fristlose Kündigung , die er wenig später erhielt, wehrte er sich zunächst erfolgreich. In der Berufungsinstanz jedoch unterlag er vor dem Landesarbeitsgericht (LAG) Baden-Württemberg im September 2020 [6]. Sein Arbeitgeber hatte einen 93-seitigen Vergleich des Datenbestands im fraglichen Verzeichnis vor und nach der Löschaktion vorgelegt.

Das Gericht sah die fristlose außerordentliche Kündigung als begründet an: Das unbefugte vorsätzliche Löschen betrieblicher Daten auf EDV-Anlagen des Arbeitgebers tauge ebenso wie das Vernichten von Verwaltungsvorgängen grundsätzlich als „wichtiger Grund“ für eine solche Kündigung im Sinne des § 626 Abs. 1 BGB. Dabei komme es nicht unbedingt darauf an, ob sich der Arbeitnehmer nach § 303a StGB oder § 303b StGB strafbar gemacht habe. Es sei auch nicht entscheidend, ob und mit welchem Aufwand ein Teil der gelöschten Daten wiederhergestellt werden konnte oder ob der Arbeitgeber diese Daten für den weiteren Geschäftsablauf tatsächlich benötigte. Vielmehr gehöre es zu den vertraglichen Nebenpflichten eines Arbeitsverhältnisses im Sinne des § 241 Abs. 2 BGB, dass der Arbeitnehmer seinem Arbeitgeber den Zugriff auf betriebliche Dateien nicht verwehre oder unmöglich mache.

Wenn der Admin spioniert

Dass es bei der strafrechtlichen Bewertung von Hacker-Aktivitäten nicht so sehr um die benutzten Werkzeuge als vielmehr um Zweck und Absicht des Einsatzes geht, illustriert auch ein Fall, den 2020 der BGH in letzter Instanz entschied [7]. Zwei Männer mussten sich wegen des Ausspähens von Daten (§ 202a StGB) verantworten. Einer davon leitete die Stabsstelle eines Apothekerverbandes und betrieb daneben ein gesundheitspolitisches Informationsportal im Internet. Der zweite Angeklagte arbeitete als

Systemadministrator am Berliner Standort des Bundesgesundheitsministeriums (BMG) und war nebenbei als Callboy tätig – daher rührte auch die Bekanntschaft der beiden Männer.

Der Admin hatte jahrelang Zugriffsrecht auf alle E-Mail-Accounts seiner Dienststelle und versorgte den Portalbetreiber mit so gewonnenen Interna aus dem Ministerium. Nachdem das Ministerium den unbeschränkten Mailzugriff der Administratoren im Hause als Sicherheitsmangel erkannt hatte, wurde es für den Mann schwieriger – er verlegte sich schließlich auf einen unter den Admins bekannten Notfalltrick, mit dem er sich selbst von Fall zu Fall die nötigen Zugriffsrechte verschaffte. Er lieferte dem Portalbetreiber auf Datenträger kopierte E-Mail-Inhalte nach Wunsch und kassierte dafür insgesamt rund 1000 Euro. Sein Kunde war besonders an E-Mails der Minister und Staatssekretäre sowie einiger Abteilungs- und Referatsleiter interessiert. In den weitergereichten Mails ging es unter anderem um Gesetzesvorhaben, die für das Publikum des Portals besonders interessant waren.

Das Landgericht (LG) Berlin verurteilte die Männer im April 2019 wegen gemeinschaftlichen Ausspähens von Daten nach § 202a StGB und sah in der Manipulation der Zugriffsrechte auf die einzelnen E-Mail-Konten zudem die Überwindung einer Zugangssicherung nach § 202a Abs. 1 StGB. Die gegen das landgerichtliche Urteil eingelegte Revision wies der BGH weitgehend ab, lediglich den einzuziehenden Geldbetrag setzte er niedriger an als die Vorinstanz.

Die Bundesrichter beschäftigten sich vor allem damit, ob Daten im Sinn des §202a Abs. 1 StGB überhaupt als gesichert gelten können, wenn ein Admin mithilfe seiner Kenntnisse darauf zugreifen kann. Die Antwort: Es genüge, wenn getroffene Vorkehrungen den Zugriff auf Daten zumindest deutlich erschweren. Die Sicherung von E-Mail-Accounts durch Passwörter reiche aus. Dabei brauche der Systembetreiber nur den Zugriff Unbefugter zu berücksichtigen, aber nicht die Zugriffsmöglichkeit durch Eingeweihte oder Experten. Es sei nicht erforderlich, dass die Sicherung gerade gegenüber dem Täter wirkt – wenn dieser etwa ein Administrator ist, der den tatsächlichen Zugriff auf die Daten hat.

Als Überwinden der Zugangssicherung nach § 202a StGB können dem Gericht zufolge auch Handlungen gelten, die nicht besonders anspruchsvoll oder aufwendig sind. Wenn jemand durch Insiderkenntnisse oder Ähnliches eine Absicherung schnell und leicht ausschalten kann, zähle das rechtlich ebenso, als hätte sich jemand durch raffinierte technische Werkzeuge Zugriff verschafft. Nur wenn eine Durchbrechung des Schutzes für jedermann ohne Weiteres möglich sei, werde der Tatbestand nicht erfüllt.

Wer den Schaden hat …

Wie bereits gesagt, ist strafrechtliche Verfolgung nicht das Einzige, was der illegale Einsatz von Hacking-Tools nach sich ziehen kann: Wenn dabei ein Schaden entsteht, hat der Geschädigte einen Anspruch auf Schadenersatz gegen den Verursacher. Schäden durch IT-Störmanöver können sehr hoch sein – wenn etwa durch den Ausfall von Unternehmensservern Arbeitsprozesse lahmgelegt werden. Auch der Ausfall der Netzkommunikation kann enorme Umsatzeinbußen und damit hohe wirtschaftliche Schäden bedeuten. Für Anspruchsteller im Zivilrecht ist wichtig, dass jede Streitpartei alles, was für ihre Sache spricht, selbst gerichtsfest beweisen muss. Das kann bei Schäden durch Hackertools etwa den Nachweis eines Hackerangriffs und die zweifelsfreie Benennung des Angreifers betreffen. Außerdem ist auch nachzuweisen, dass der Angriff tatsächlich den geltend gemachten Schaden hervorgerufen hat.

Wenn ein Täter bereits strafrechtlich wegen einer Computerstraftat zulasten eines Geschädigten verurteilt worden ist, hat jener es anschließend vergleichsweise leicht, seine Ansprüche gegen den Verurteilten zivilrechtlich geltend zu machen: Das Urteil des Strafgerichts hat selbst bereits Indizwirkung, zudem kann der Kläger die im Strafverfahren erhobenen Beweise zu seinen Gunsten nutzen.

Ein dritter, bislang noch nicht genannter Bereich, der durch unrechtmäßigen Einsatz von Hackertools berührt werden kann, ist der Datenschutz. Wo bei einem Angriff personenbezogene Daten im Spiel sind, geht es nicht bloß um wirtschaftliche Schäden, sondern möglicherweise auch um die massenhafte Verletzung des informationellen Selbstbestimmungsrechts der Betroffenen. Wer es also als Pentester mit realen Datenbeständen zu tun hat, tut gut daran, die Bestimmungen der europäischen Datenschutzgrundverordnung (DSGVO) sorgfältig zu beachten. Darüber hinaus sollten Admins, die im Auftrag des eigenen Arbeitgebers mit Hacking-Werkzeugen arbeiten, zur eigenen Absicherung auf einer möglichst konkret gefassten schriftlichen Vereinbarung über Umfang und Grenzen dieses Auftrags bestehen. Ebenso wichtig ist es, die Schritte dieser Arbeit genau zu protokollieren. (psz) c't

Literatur

[1] Ronald Eikenberg, David Wischnjak, **Böse und billig: Hacking-Gadgets**, Gefahr durch angriffslustige Hardware, c't 18/2017, S. 62 und S. 64: ct.de/wu3e

[2] Ronald Eikenberg, **c't testet die Tools der Hacker**, c't Security 2020, S. 172

[3] Verena Ehrl, **Elektronische Übeltäter**, Rechtliche Aspekte im Zusammenhang mit Spionage- und Sabotage-Gadgets, c't 18/2017, S. 78: ct.de/wu3e

[4] Verordnung (EU) 2021/821 des Europäischen Parlaments und des Rates vom 20.5.2021 über eine Unionsregelung für die Kontrolle der Ausfuhr, der Vermittlung, der technischen Unterstützung, der Durchfuhr und der Verbringung betreffend Güter mit doppeltem Verwendungszweck: heise.de/s/N76o

[5] BGH, Beschluss vom 8.4.2021, Az. 1 StR 78/21: heise.de/s/rmDJ

[6] LAG Baden-Württemberg, Urteil vom 17.9.2020, Az. 17 Sa 8/20: heise.de/s/MXBL

[7] BGH, Beschluss vom 13.5.2020, Az. 5 StR 614/19: heise.de/s/Zvpw

secIT by Heise
SPECIAL

Jetzt Kombi-Rabatt sichern
und **über 30 % sparen!**

Die Online-Konferenzen zur secIT by Heise

secIT Special
IT-Security im Fokus

Vertiefen Sie in einer spannenden Keynote sowie in 3 interaktiven Vorträgen Ihr Wissen rund um IT-Security. Jedes secIT Special präsentiert Ihnen ein exklusives Thema.

DIE TERMINE

IR, SOC und SIEM

Verteidigungschinesisch (nicht nur) für Anfänger!
Im Kombi-Ticket als Aufzeichnung erhältlich

Cybersicherheit für KMU

Kaufen, mieten oder selber machen?
Im Kombi-Ticket als Aufzeichnung erhältlich

9. Dezember 2021

Hacking for Security

Was Sicherheitstests für Unternehmen bringen!

JETZT ANMELDEN
https://konferenzen.heise.de/secit-special

UNSERE PARTNER

G DATA ADVANCED ANALYTICS
Increase Your Skills
SONICWALL
SOPHOS Die Evolution der Cybersecurity

NitroPC: Mini-PC mit Security-Plus

Dank Open-Source-Firmware und deaktivierter Management Engine ist der flinke NitroPC vertrauenswürdiger als andere Rechner – und damit prinzipiell auch sicherer. Seine SSD ist standardmäßig verschlüsselt.

Von **Ronald Eikenberg und Christof Windeck**

Der kompakte NitroPC des Berliner Herstellers Nitrokey ist nur äußerlich eine Black Box: Innerlich geht es transparent zu, denn nicht nur das vorinstallierte Linux ist Open Source, auch die UEFI-Firmware. Das ist durchaus eine Seltenheit, denn fast alle anderen Rechner sind mit einem proprietären (UEFI-)BIOS ausgestattet, über das man keine Kontrolle hat. Auch die Management Engine (ME) der Intel-Chipsätze ist unkontrollierbar, beim NitroPC ist sie deshalb weitgehend abgeschaltet.

Dies soll den NitroPC besonders vertrauenswürdig machen, wodurch er sich sogar als Hochsicherheitsrechner in Unternehmen und Behörden sowie als Arbeitsrechner für investigative Journalisten eig-

nen soll. Wer möchte, kann die Open-Source-Firmware, eine Kombination aus Coreboot und TianoCore, selbst kompilieren und flashen. Der Hauptvorteil ist jedoch, dass ihr Code öffentlich einsehbar ist. Jeder kann ihn auf Sicherheitslücken und Backdoors abklopfen, allerdings mit Ausnahme einiger proprietärer Binärkomponenten von Intel – sogenannte BLOBs –, etwa dem Firmware Support Package (FSP), ohne die auch der NitroPC nicht auskommt.

Bei einem vollständig proprietären BIOS muss man hingegen darauf vertrauen, dass der Hersteller alles richtig gemacht hat, denn unabhängige Code-Audits sind selten. Dieser Vertrauensvorschuss kann jedoch gefährlich werden: So musste etwa Dell kürzlich ein Sicherheitsloch stopfen, durch das Angreifer Code im Kontext des UEFI-BIOS ausführen konnten – und das ist nur eines von vielen Beispielen. Das BIOS gilt bei Hackern als heiliger Gral. Wer es schafft, sich darin einzunisten, hat das System weitreichend unter Kontrolle und muss nicht fürchten, dass die Infektion jemals vom Virenscanner entdeckt wird.

Das Gleiche gilt für die Management Engine (ME). Es handelt sich um einen Computer im Computer, der chipsatzspezifische Funktionen wie TPM und Hardware-Monitoring übernimmt, aber auch den Fernzugriff aufs System ermöglichen kann. Das öffentliche Wissen über ihre Funktionsweise stammt vor allem von unabhängigen Sicherheitsforschern, die durch Reverse Engineering auch schon diverse kritische Sicherheitslücken darin entdeckt haben. Nitrokey löst dieses Problem, so gut es geht: Wie alle modernen Intel-Systeme ist zwar auch der NitroPC mit der ME ausgestattet, sie ist jedoch so weit wie möglich deaktiviert. Der Hersteller nutzt hierfür das Open-Source-Tool me_cleaner (siehe ct.de/wcnv).

Diese Besonderheiten schränken die Konfigurierbarkeit ein wenig ein: Wer gerne an den BIOS-Setup-Einstellungen schraubt, macht beim NitroPC ein langes Gesicht. Drückt man beim Einschalten die Esc-Taste, kann man über das rudimentäre BIOS-Setup im Wesentlichen die Boot-Reihenfolge der physischen Datenträger ändern. Netzwerk-Boot beherrscht der Rechner nicht. Etwas mehr geht über die UEFI-Shell. Sie kann unter anderem detaillierte Informationen über Hardware und UEFI-Treiber ausgeben.

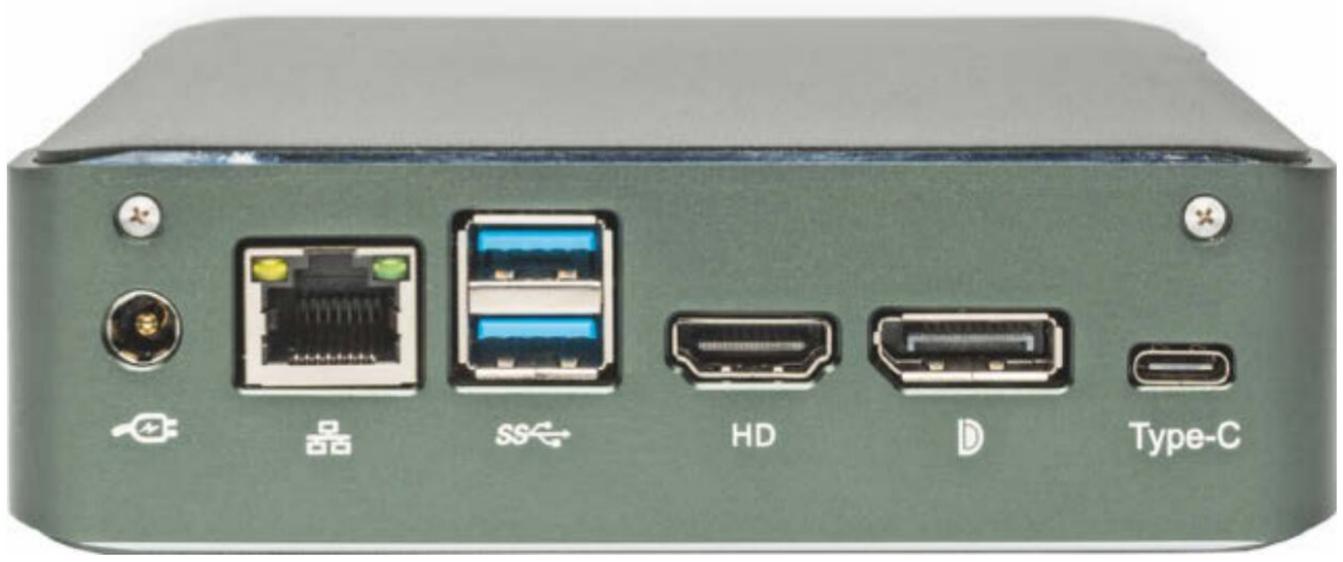
Auch die Management Engine ist funktional eingeschränkt: So fehlt das Trusted Platform Module (TPM), das unter Windows etwa für Measured Boot, FIDO2 und BitLocker nützlich ist. Dank der UEFI-Kompatibilität könnte man Windows 10 prinzipiell installieren, aber das wäre widersinnig, weil das Closed-Source-Betriebssystem mehr Risiken birgt, als die Open-Source-Firmware vermeidet. Wer gelegentlich auf ein Windows angewiesen ist, sollte es auf dem NitroPC besser in einer VM nutzen.

Anders als das NitroPad [1], einem durch Nitrokey modifizierten Lenovo Thinkpad, ist der NitroPC nicht mit der Custom-Firmware Heads ausgestattet. Heads startet dort nach dem Coreboot-BIOS und überprüft, ob das BIOS und wichtige Boot-Dateien manipuliert wurden. Dem NitroPC fehlt mit dem TPM der dafür nötige Vertrauensanker.

Bei der Bestellung im Online-Shop kann man zwischen Ubuntu, Debian und Linux Mint wählen. Gegen 45 Euro Aufpreis installiert Nitrokey auch Qubes OS, das durch seine Virtualisierungsschichten besonders sicher ist. Unser Testgerät war mit Ubuntu 20.04 LTS ausgestattet, dessen LUKS-Festplattenverschlüsselung bereits aktiv war. Ein Beipackzettel wies uns darauf hin, das vorgegebene Standard-

Nitrokey NitroPC

Sicherer Mini-PC mit Open-Source-Firmware ohne Intel ME	
Hersteller, URL	Nitrokey, nitrokey.com
Prozessor	Intel Core i7-10510U (4 Kerne, 8 Threads, 1,8–4,9 GHz, 15 W, Comet Lake (CML))
GPU / RAM	Intel UHD (integriert in CPU) / 16 GByte (2 × 8 GByte DDR4-2666, max. 64 GByte)
SSDs	1 × 1 TByte M.2 (PCIe 3.0 x4), optional 1 × SATA 2,5 Zoll bis 2 TByte
1 GBit/s-Ethernet / WLAN	1 × Realtek RTL8111 / Qualcomm QCA6174A (Wi-Fi 5, 2x2, BT 5.0, M.2)
Anschlüsse vorn	2 × USB-A 3.2 Gen 2 (10 GBit/s), 2 × USB-A 2.0. 1 × Audio-Klinke
Anschlüsse hinten	1 × HDMI 2.0, 1 × DP 1.2, 2 × USB-A 3.2 Gen 2, 1 × USB-C 3.2 Gen 2x2 (20 GBit/s), 1 × Stromversorgung, 2 × WLAN-Antennen
Betriebssystem	Ubuntu 20.04 LTS
Netzteil	Chicony A13-040N3A (19 V/40 W)
Abmessungen Gehäuse	12,8 cm × 3,8 cm × 12,8 cm (ohne Stecker)
mitgeliefertes Zubehör	VESA-Montageadapter
Messwerte (Linux, 4K-Display, USB-Tastatur/-Maus)	
Blender 2.82a, Szene Blender	705 s
7-zip (Ver-/Entschlüsseln)	20.852 / 17627 MIPS
PCIe-3.0-SSD (lesen / schreiben)	2,2 / 1,8 GByte/s
USB-A 3.2 Gen 2 (lesen / schreiben)	1,0 / 1,0 GByte/s
USB-C 3.2 Gen 2x2 (lesen / schreiben)	2,2 / 2,0 GByte/s
WLAN-Durchsatz 2,4 / 5 GHz	nah: 140 / 518 MBit/s, 20 Meter: 13 / 105 MBit/s
Leistungsaufnahme Soft-off	0,7 W
Leerlauf / Volllast CPU	4,9 / 26 W (kurzzeitig 40 W)
Geräusch im Leerlauf / CPU-Volllast	< 0,1 sone / 0,3 sone
Preis Testgerät / Garantie	867 € / Gewährleistung 24 Monate



Anschlussfreudig: Der NitroPC bietet zahlreiche Ports, darunter USB-C mit USB 3.2 Gen 2x2.

passwort „PleaseChangeMe“ zu ändern. Vorinstalliert war lediglich die Nitrokey-App zur Verwaltung der gleichnamigen Krypto-Sticks, die der Hersteller ebenfalls verkauft. Ubuntu lief während unseres Tests flink und zuverlässig auf dem Mini-PC, an der Linux-Kompatibilität der Hardware hatten wir nichts auszusetzen.

Hardware

Der NitroPC ist weitgehend baugleich mit dem etwas teureren Librem Mini v2 der US-Firma Purism [2]. Die Hardware fertigt ein ungenannter chinesischer OEM-Hersteller; sehr ähnliche Geräte findet man bei AliExpress etwa unter der Marke Hystou, allerdings mit „normalem“ UEFI-BIOS.

Im Mini-PC rechnet der 2019 vorgestellte Intel-Mobilprozessor Core i7-10510U aus der 14-Nanometer-Generation „Comet Lake“. Seine vier Kerne takten kurzzeitig mit bis zu 4,9 GHz, unter Last sind es eher 4,3 GHz. Die Rechenleistung gleicht der eines zwei Jahre alten Notebooks der 1000-Euro-Klasse und genügt auch für anspruchsvollere Aufgaben, zumal Nitrokey für das Gerät bis zu 64 GByte RAM anbietet. Unser Testgerät war mit 16 GByte RAM und einer NVMe-SSD mit 1 TByte bestückt. Gegen Aufpreis bekommt man auch eine 2-TByte-SSD und sogar eine zweite (SATA-)SSD mit ebenfalls bis zu 2 TByte.

Am Betriebsgeräusch gibt es nichts zu meckern: Im Leerlauf hört man den Lüfter praktisch nicht und selbst unter Volllast bleibt der NitroPC sehr leise. Auch die Leistungsaufnahme ist mit knapp 5 Watt im Leerlauf ziemlich niedrig. Kurzzeitig schluckt der Mini – wie viele andere auch – bis zu 40 Watt, was an der Grenze der Belastbarkeit des beigelegten Netzteils liegt; dabei zeigten sich aber keine Probleme.

Gute Noten verdient sich der Mini-PC bei den Datentransferraten. Zwar gibt es noch schnellere PCIe-SSDs und WLAN-Adapter, in der Praxis hat das aber wenig Bedeutung. Die USB-C-Buchse schafft sogar USB 3.2 Gen 2x2, überträgt aber leider keine Displaysignale. Es gibt noch sechs weitere USB-Buchsen, aber keinen Kartenleser.

Der NitroPC startet ohne Speicher bei 599 Euro und liegt damit ungefähr auf dem Preisniveau eines ähnlich ausgestatteten Intel NUC. Betriebsbereit mit 8 GByte RAM und 256-GByte-SSD gibt es ihn für 679 Euro, die Maximalausstattung mit 64 GByte RAM und 2-TByte-SSD kostet über 1400 Euro. Eine zweite SSD und Qubes OS kosten noch mal extra. Auf Wunsch verschickt Nitrokey den Mini-PC für 50 Euro auch mit versiegelten Schrauben in einem ebenfalls versiegelten Beutel. So können Käufer nachvollziehen, ob das Gerät auf dem Transportweg geöffnet und potenziell manipuliert wurde.

Fazit

Wer einen kompakten Linux-PC sucht und sich nicht um die Installation und etwaige Hardware-Inkompatibilitäten kümmern möchte, bekommt mit dem NitroPC ein rundes Gesamtpaket zu einem fairen Einstiegspreis. Obendrauf gibts durch das quelloffene UEFI-BIOS und die reduzierte Management Engine ein Plus an Vertrauenswürdigkeit – und damit im Prinzip auch an Sicherheit. Das könnte für manche Zielgruppen kaufentscheidend sein. Der Mini-PC ist sehr leise und flink genug für die meisten Einsatzzwecke, als Spielerechner ist das Linux-System mit seiner Onboard-Grafik jedoch ungeeignet. Der NitroPC ist eine gute Alternative zum Librem Mini v2, der nicht nur etwas teuer ist, sondern auch aus den USA verschickt wird und demzufolge durch den Zoll muss. (rei) c't

Literatur

[1] Ronald Eikenberg, **Hochsicherheits-Notebook**, Linux-Notebook Nitrokey NitroPad X230, c't 7/2020, S. 96

[2] Johannes Merkert, **Freiheits-Notebook**, Das Librem 15 mit PureOS und quelloffenem Coreboot, c't 23/2017, S. 114

Firmwarequellen, Herstellershop

ct.de/wcnv

Hoch hinaus...

Wie Cloud-Dienste die Arbeit erleichtern

Heft + PDF mit 29 % Rabatt

Das c't-Sonderheft zeigt Ihnen Wege, wie Sie sich die Arbeit mit Servern aus der Cloud erleichtern und Neues ausprobieren können:

- Einstieg in Cloud-Konzepte und -Software
- Hilfreiche Dienste für Cloud-Server
- Mit Go für fast alle Plattformen programmieren
- Für Abonnenten portofrei
- Auch im Set mit Heft + PDF + Buch „Go – Das Praxishandbuch“

Heft für 14,90 € • PDF für 12,99 € • Bundle Heft + PDF 19,90 €

shop.heise.de/ct-cloud21

Generell portofreie Lieferung für Heise Medien- oder Maker Media Zeitschriften-Abonnenten oder ab einem Einkaufswert von 20 €.
Nur solange der Vorrat reicht. Preisänderungen vorbehalten.

heise Shop

IoT und Industrie ungeschützt im Netz

Angriffe auf die IT-Umgebungen von Unternehmen sind mitunter unglaublich einfach. Häufig kann man Daten abgreifen oder Industriesteuerungen übernehmen, ohne überhaupt Sicherheitsmechanismen umgehen zu müssen. Wir haben das Internet systematisch nach ungesicherten Servern durchsucht.

Von **Jan Mahn und Merlin Schumacher**

Dateifreigaben ungeschützt im Netz	138
IoT ungesichert im Netz	142
Hintertür zu Wordpress	148
Newsletter als Spam-Schleudern	152
Unachtsamer Phisher enttarnt	156
Datenlecks bei Test- und Impfterminen	160
Ransomware-Attacke gezielt vereiteln	166

Paradiesische Zustände müssen das gewesen sein, als die Vorläufer des Internets erfunden wurden: Das gesamte Netzwerk bestand aus einer handvoll freundlich gesinnter Nutzer aus Forschungseinrichtungen und wer einen Dienst anbot, konnte mit Dankbarkeit und gutgemeinten Ratschlägen rechnen. Dass das im heutigen Internet anders aussieht, hat sich mittlerweile herumgesprochen – sollte man zumindest annehmen. Im Internet tummeln sich längst nicht nur freundliche Zeitgenossen und schon als gewöhnlicher Nutzer muss man ständig auf der Hut sein.

Ungleich aufmerksamer muss man sich aber verhalten, wenn man selbst einen Dienst im Internet veröffentlichen möchte. Immer dann, wenn man die Konfigurationsoberfläche des eigenen Routers öffnet und eine Portweiterleitung einrichtet, sollte man sich bewusst machen, welche Verantwortung man jetzt trägt. Ein handelsüblicher Router, der nebenbei als Firewall arbeitet, lehnt alle Anfragen von außen grundsätzlich ab und schützt die Geräte im Netz vor Anfragen aus dem Internet. Mit einer Portweiterleitung bohrt man gezielt ein Loch in diese Firewall und legt fest, welcher Port zu welchem Gerät im privaten Netz weitergeleitet werden soll. Das kann ein Webserver sein, die Steuerung des Smart-Homes oder ein Mailserver. Wichtig ist jetzt: Der veröffentlichte Dienst muss unbedingt mit einer Anmeldung versehen, verschlüsselt und die verwendete Software stets aktuell sein. Vor allem aber sollte man die Finger von Portweiterleitungen lassen, wenn man sich unsicher ist.

Planlos offen?

Wer unbedacht Ports aufreißt, der riskiert, dass ihm Daten gestohlen werden oder andere im privaten Netz umherspazieren und dort Schaden anrichten. Doch leider sind solche Fehlkonfigurationen keine Seltenheit. Immer wieder bekamen wir in der Vergangenheit Hinweise auf einzelne Fälle, die Hinweisgeber zufällig entdeckt haben. Besonders prominente Fälle waren eine Arztpraxis [1] und die Autovermietung Buchbinder [2], beiden wurden ungeschützte Dateifreigaben zum Verhängnis. Doch sind solche Probleme Einzelfälle oder eher die Regel? Um das herauszufinden, haben wir das Internet systematisch unter die Lupe genommen. In diesem und den folgenden Artikeln stellen wir eine Auswahl unserer Erkenntnisse vor. Die Fälle stehen exemplarisch für viele weitere Funde – gleichzeitig geben wir Ratschläge, wie Sie als Administrator solche Fehler vermeiden können.

In diesem Artikel beschreiben wir, wie wir vorgegangen sind, und zeigen beispielhaft am Protokoll SMB, welche Folgen eine Fehlkonfiguration haben kann. Ab Seite 142 befassen wir uns gezielt mit Industriesteuerungen und dem IoT-Protokoll MQTT – in Industrieanlagen können offene Systeme in kurzer Zeit besonders viel Schaden anrichten. Quasi nebenbei stießen wir bei unseren Recherchen auf weitere Konfigurationsfehler: Unschöne Probleme kann man sich auch als Betreiber von Newsletter-Formularen eintreten. Ab Seite 152 erfahren Sie, wie man durch Unachtsamkeit Spammern und Phishern einen erfolgreichen Arbeitstag garantiert. Allzu kommunikativ sind auch falsch konfigurierte Wordpress-Umgebungen – mehr ab Seite 148.

IPs sind nicht geheim

Viele unfreiwillige Dienstanbieter sitzen einem gewaltigen Irrtum auf, den man auch immer wieder in Foren und Blogs als gut gemeinten Ratschlag liest: Solange man keine Domain einrichte, die per DNS auf die Adresse auflöst, sei eine IP-Adresse in den Weiten des Internets quasi geheim. Es gebe schließlich über 4 Milliarden Adressen, daher sei es unmöglich, einen veröffentlichten Dienst unter einer beliebigen Adresse zu erraten.

Diese Erzählungen gehören definitiv ins Reich der Mythen. Schon die vermeintlichen 4,2 Milliarden IP-Adressen existieren nur in der Theorie. Abziehen kann man zunächst alle Broadcast-Adressen sowie sämtliche reservierten Adressbereiche, zusammen rund 600 Millionen. Die verbliebenen rund 3,6 Milliarden IPv4-Adressen reichen keinesfalls aus, damit ein Dienst anonym bleiben kann.

Möchte man offene Ports im Internet finden, muss man nur systematisch danach suchen. Ein bewährtes Werkzeug unter Sicherheitsforschern ist die Suchmaschine shodan.io. Deren Betreiber haben Server mit Portscannern eingerichtet – ein solcher Portscanner probiert nacheinander die Ports an einer Adresse durch und protokolliert, auf welchen Ports er eine Antwort bekommen hat. Will man das gesamte Internet durchsuchen, muss man das 3,6 Milliarden mal wiederholen. Shodan geht dann noch einen Schritt weiter und stellt für zahlreiche Protokolle eine Verbindung her und speichert die Antworten in seiner Datenbank. Über eine Weboberfläche kann man gezielt nach Protokollen oder Antworten suchen. Einen ähnlichen Dienst gibt es bei censys.io. Ganz einfache Suchen sind kostenlos, für kommerzielle Nutzung und Filter muss man zahlen.

Über 63 000 SMB-Server fanden wir weltweit im Internet. Auf viele konnte man ohne Zugangsdaten zugreifen.

Gezieltes Vorgehen

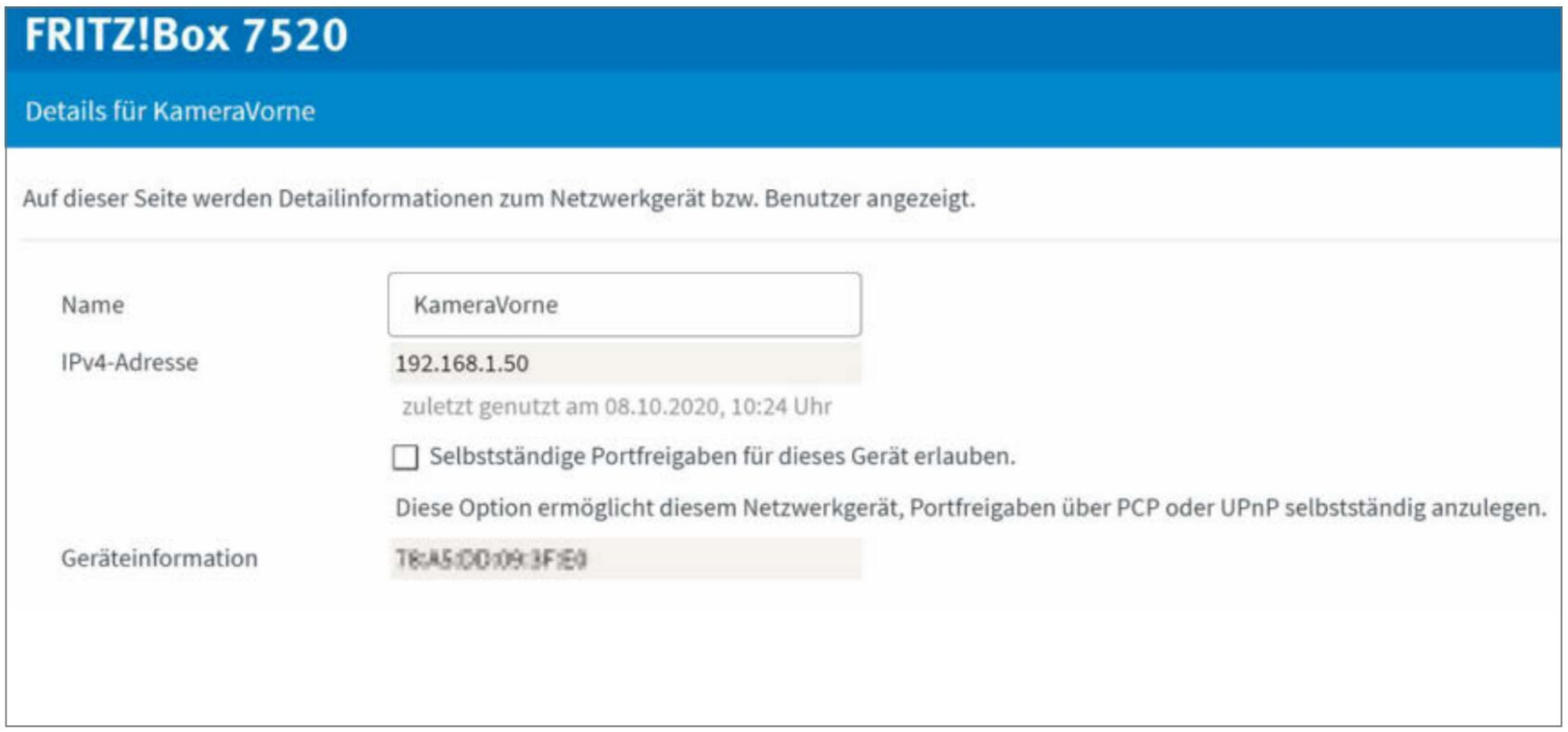
Für unseren Sicherheitsreport wollten wir uns aber nicht auf gefilterte und aufbereitete Datensätze von anderen verlassen. Solche Suchmaschinen bringen die Funde in eine eigene Reihenfolge und finden einige Adressen gar nicht. Stattdessen entschieden wir uns, selbst ein System zum systematischen Scannen des gesamten IPv4-Internets vorzubereiten. Dafür mussten wir das Rad nicht neu erfinden. Grundlage für unseren automatischen Scanner ist das Open-Source-Kommandozeilenwerkzeug ZMap. Das scannt das gesamte Internet und schreibt alle IP-Adressen mit einem offenen Port in eine Datei. Bemerkenswert ist die Geschwindigkeit, die ZMap an den Tag legt: Ein Scan für einen Port über alle Adressen dauert nach Angaben der Entwickler nur 5 Minuten, wenn man eine 10-GBit/s-Leitung nutzen würde. Wir entschieden uns, die Scans auf angemieteter Hardware bei einem Hoster zu starten, und drosselten ZMap auf unter 25 MBit/s. So mussten wir teilweise einige Tage auf einen kompletten Scan des Internets warten.

Netzlaufwerke für alle

Den ersten Scan starteten wir auf SMB-Port 445. Windows-Nutzer kennen das Protokoll von den Windows-Dateifreigaben, aber auch Linux-Maschinen und NAS können SMB anbieten. Die Liste der Ergebnisse war lang. Bei etwa 63 000 IPs meldete sich ein SMB-Dienst. Auf diese Liste ließen wir ein Skript los, das einen SMB-Verbindungsaufbau ohne Zugangsdaten probierte.

Die meisten Server brachen die Verbindung ab oder verlangten ein Login. Etwa 1500 Server antworteten bereitwillig auf unsere Anfragen und listeten die verfügbaren Freigaben. Einige Server boten sogar noch SMB 1 an, für das seit Jahren Exploits bekannt sind. Uns interessierten – schon um jeden rechtlichen Ärger zu vermeiden – aber nur die Freigaben, die ohne jede Anmeldung les- und oder beschreibbar waren. Davon gab es viele: So fanden wir die gesamte Buchhaltung zweier südamerikanischer Baufirmen und eines mittelamerikanischen Urlaubsclubs, Verträge, Rechnungen und Beschlüsse einer asiatischen Regionalverwaltung und viele NAS-Geräte.

Bei den NAS handelt es sich um ein systematisches Problem und nicht immer hat der Nutzer die Portweiterleitung per Hand im Router aktiviert. Viele Router gestatten es Geräten im Netzwerk, per UPnP eine solche Weiterleitung selbst einzurichten. Öffnet das NAS Port 445 in der Firewall, ist die Katastrophe perfekt. Deaktivieren Sie daher UPnP-Freigaben in Ihrem Router. Die Fritzbox listet unter „Internet / Freigaben / Portfreigaben“ alle Geräte mit offenen Ports



Möchte man verhindern, dass das NAS per UPnP ein Loch in die Firewall bohrt und Daten ungewollt mit der Welt teilt, muss man die Funktion im Router deaktivieren.

auf. Entfernen Sie hier alle Haken in der Spalte „Selbstständige Portfreigabe“ und klicken Sie auf „Übernehmen“.

Manche NAS bieten Freigaben für Apples Backup-System Time Machine an, die grundsätzlich ohne Anmeldung erreichbar sind. Im lokalen Netz mag das praktisch sein, um den Mac zu sichern, in Kombination mit einer Portfreigabe ist das verheerend. Wir fanden zahlreiche Komplett-Backups von Apple-Nutzern weltweit. Bei vielen NAS waren wir auch nicht die ersten Besucher. Hier hatten schon Verschlüsselungstrojaner zugeschlagen.

Auch ein grober Schnitzer aus Deutschland war dabei, zur Abwechslung mal kein NAS. Ein nordrhein-westfälischer Büromöbelhändler hatte seinen Windows-Server ins Netz gestellt, damit die Mitarbeiter bequem auf die Daten zugreifen können – leider konnte das auch jeder nicht angemeldete Besucher. Die gesamte Unternehmenskommunikation war per SMB für jedermann zugänglich, darunter Rechnungen der letzten Jahre, Kundenlisten, Umsatzauswertungen, Kostenvoranschläge. Wir haben den Anbieter darauf aufmerksam gemacht und er hat die Lücke zügig geschlossen und zugesichert, den zuständigen Landesdatenschutzbeauftragten zu informieren. Die Freigaben lagen auch nicht auf einer Maschine im eigenen Netz, sondern auf einer virtuellen Maschine bei einem Hoster. Die haben oft keine separate Firewall, sodass man sich unbedingt darum kümmern muss, die Firewall des Betriebssystems einzurichten. Im Gespräch war der IT-Verantwortliche des kleinen Unternehmens überrascht, dass die Freigabe in den Weiten des Netzes gefunden werden konnte. Den Vorfall nahm er zum Anlass, eine VPN-Lösung bei einem Dienstleister in Auftrag zu geben.

Was tun?

All diese Freigaben fanden wir mit einem oberflächlichen Scan, wir mussten keine Zugangssicherungen überwinden. Eine Absicherung der Freigaben per Authentifikation ist zwar schon ein Schritt mehr, reicht gegen Angreifer aber nicht aus. SMB gehört zu den sehr geschwätzigen Protokollen. Auch wenn man von außen nicht auf die Freigaben selbst, sondern nur auf die Übersicht zugreifen kann oder Details zur verwendeten Software sieht, ist das schon zu viel. Aus unserer Sicht gehört SMB ins lokale Netz, nicht ins Internet! Wer Netzwerkfreigaben braucht, muss ein VPN einrichten.

Alternativ können Sie über eine selbstgehostete Nextcloud-Instanz nachdenken (sofern Sie Admin-Erfahrungen mitbringen). Und selbst Server von Google, Amazon und Microsoft sind immer noch ein datenschutzfreundlicherer Ort als eine laienhaft ins Internet gehängte SMB-Freigabe. (jam) c't

Literatur

[1] Ronald Eikenberg, **Dr. Datenleck**, Warum eine komplette Arztpraxis offen im Netz stand, c’t 25/2019, S. 16

[2] Hartmut Gieselmann, Ronald Eikenberg, Christian Wölbert, Joerg Heidrich, **Daten-GAU bei Buchbinder**, Persönliche Informationen von 3 Millionen Kunden der Autovermietung Buchbinder offen im Netz, c’t 4/2020, S. 12

Bild: Andreas Martini

IoT ungesichert im Netz

Vernetzte Anlagen können in der Industrie viele Probleme lösen. Hängt man sie ungeschützt ins Internet, schafft man sich aber eine Menge neue. Bei unserer Suche nach schlampigen Konfigurationen wurden wir allzu häufig fündig.

Von **Jan Mahn**

Wenn Privatpersonen versehentlich ihr Smart-Home ungeschützt ins Internet hängen, ist der Schaden überschaubar. Schlimmstenfalls können Scherzbolde aus der Ferne das Licht abschalten oder die Rollläden schließen. Richtig unangenehm wird es aber, wenn Industrieunternehmen ihre vernetzte oder „smarte“ Fabrik mit der ganzen Welt teilen. Das Potenzial für Erpressungen und Sabotage ist riesig. Was passiert, wenn Angreifer eine Chemiefabrik oder eine Ölraffinerie fernsteuern, möchte

man sich nicht ausmalen. Eigentlich sollte man davon ausgehen, dass solche Unternehmen eigene IT-Sicherheitsexperten beschäftigen oder Expertise einkaufen und sich nach dem Stand der Technik gegen Angriffe schützen. Eigentlich.

Auf die Idee, die Sicherheit von Industrieanlagen mal systematisch zu untersuchen, brachte uns ein Tippgeber, der durch Zufall einen offenen MQTT-Server im Internet gefunden hatte. MQTT ist ein Protokoll, über das Sensoren und Aktoren einander Nachrichten schicken. Dabei läuft die Kommunikation nicht direkt von Gerät zu Gerät, sondern immer über einen MQTT-Broker, bei dem andere die Nachrichten abonnieren können. Das Protokoll haben wir bereits ausführlich vorgestellt [1] und nutzen es in Kombination mit Node-Red im c't Smart-Home (siehe ct.de/wke5). Hat man gute Gründe dafür, kann man MQTT durchaus im Internet veröffentlichen – dafür verwendet man aber unbedingt MQTT über TLS auf Port 8883 und richtet für alle Endgeräte Benutzerkonten ein. Anmelden können Sie sich entweder per Passwort oder noch besser mit einem Zertifikat.

Unseren Scanner haben wir nur auf ungeschützte Broker angesetzt. Zunächst ließen wir ihn eine Liste aller Server generieren, die auf Port 1883, also mit unverschlüsseltem MQTT antworten. Die Treffer haben wir dann darauf geprüft, ob sie Verbindungen ohne Anmeldedaten zulassen – über 10 000 Adressen landeten so in unserer Liste.

Private Freizügigkeit

Am Anfang schauten wir uns einige Treffer stichprobenartig an. Abonniert man auf einem MQTT-Broker alle Topics, kann man bereits ganz brauchbar abschätzen, für was der Server genutzt wird. Nicht gerade überraschend waren die vielen Smart-Homes, die wir rund um den Globus von Berlin bis Sidney fanden. Topics wie `livingroom/lights/center` verraten allzu eindeutig, wofür der Broker gedacht ist. Bei solchen privaten Umgebungen sahen wir häufig dasselbe Muster: Wer MQTT ohne Schutz veröffentlichte, hatte oft auch etwas auf Port 80 freigegeben – gerne die Konfigurationsoberfläche des Routers oder Schaltsteckdosen mit der Open-Source-Firmware Tasmota. Beide gehören definitiv nicht ins Internet.

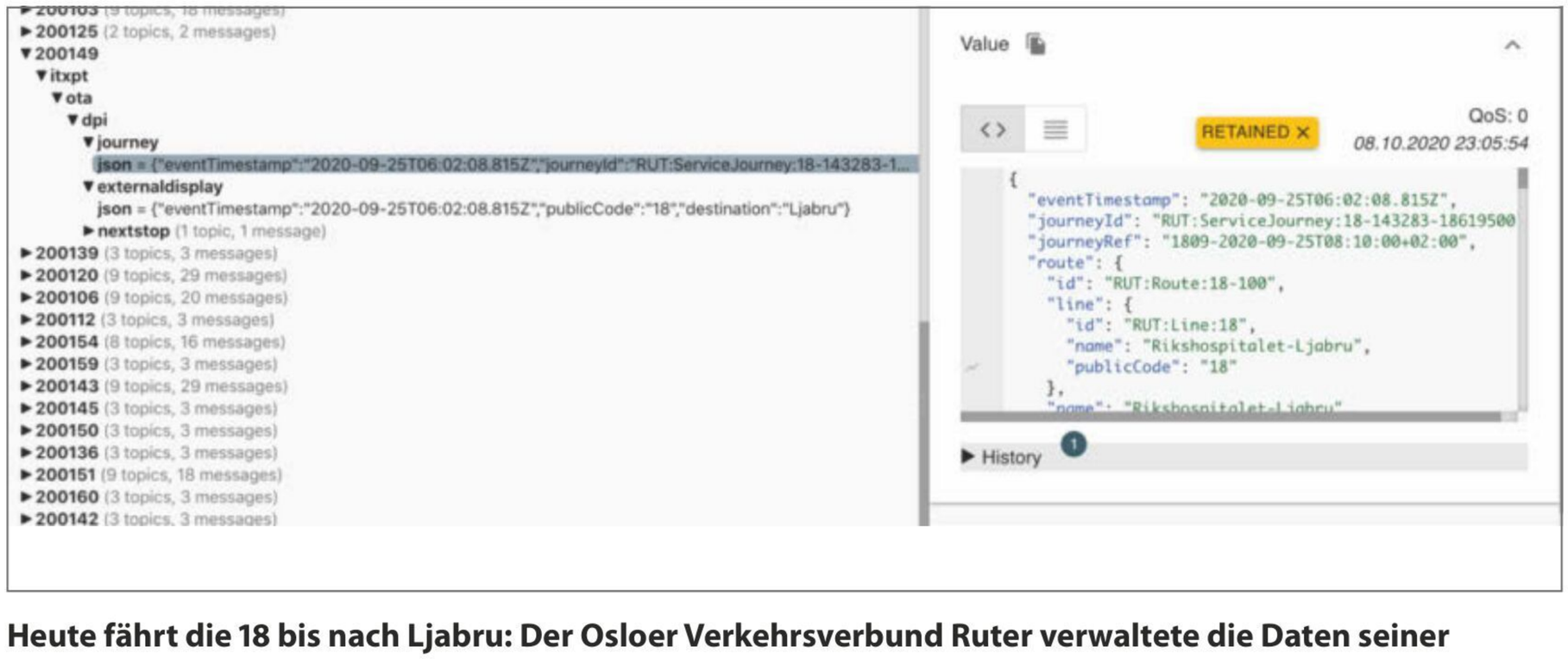
Sehr häufig fanden wir Daten der Software Owntracks in den MQTT-Topics offener Server. Die App installiert man auf dem Smartphone und gibt ihr Zugangsdaten für einen MQTT-Server. Diesem sendet sie dann regelmäßig den aktuellen Standort des Telefons. Diese Information kann man zum Beispiel nutzen, um die Heizung abzuschalten, wenn niemand zu Hause ist. Viele Smart-Home-Bastler wollen sich damit eine datenschutzfreundliche Alternative zu kommerziellen Location-Trackern bauen. Wer dafür aber einen ungesicherten MQTT-Server nutzt, erreicht leider genau das Gegenteil. Häufig konnte man aus den Topics leicht alle Familienmitglieder identifizieren (`peter_phone` und `marie_iphone`). Leichter kann man es Kriminellen nicht machen, den perfekten Zeitpunkt für einen Einbruch zu planen. Wo immer wir Hinweise auf den Betreiber finden konnten, informierten wir diesen. Owntracks kommt gut mit TLS und Authentifizierung klar, man muss sie nur aktivieren.

Industrielle Probleme

Die Smart-Homes waren aber nur Beifang auf der Suche nach Industrieanlagen. Um die unzähligen Treffer etwas einzugrenzen, suchten wir gezielt nach statischen IP-Adressen, die nur selten zu Privatkundenanschlüssen gehören. Heraus kam eine bunte Sammlung an „professionellen" MQTT-Brokern mit Fehlkonfigurationen – voller Lese- und Schreibzugang für alle. Ein Hersteller von Snack-Automaten aus Italien teilte die Statusinformationen mit der ganzen Welt, ein portugiesischer Hersteller von Brandmeldeanlagen ließ über 5000 Anlagen fast sekündlich den Status auf einen öffentlichen Server schreiben.

In Nordland in Norwegen fanden wir einen Server mit Live-Telemetriedaten von 70 Fahrzeugen, offensichtlich Busse, die Fahrzeugdaten und Positionen an den Server verschickten. Denselben Fehler machte auch ein Dienstleister für öffentlichen Nahverkehr aus Westdeutschland. Auf dessen Server fanden wir Telemetriedaten für Busse mehrerer Nahverkehrsunternehmen. Wir kontaktierten den Anbieter und er aktivierte nach kurzer Zeit Authentifizierung und Verschlüsselung, stattete die Geräte mit Zugangsdaten aus. Die Versuchung, für Fahrzeugtelemetrie auf Authentifizierung zu verzichten, ist groß – schließlich spart man sich die Arbeit, Kennwort oder Zertifikat in jedem Fahrzeug zu hinterlegen.

Dieser Versuchung konnte man auch beim Nahverkehrsverbund „Ruter" in Oslo nicht widerstehen. Dort betrieb man einen MQTT-Broker, der die Positionen und Routen aller Straßenbahnen verwaltet. Eigentlich eine praktische Sache. Aus den Daten kann man Displays an Haltestellen, in und an den Bahnen sowie Apps und eine Webseite speisen. Die Daten selbst sind vorbildlich dokumentiert, es gibt mehrere öffentliche GitHub-Repositories des Betreibers,



Heute fährt die 18 bis nach Ljabru: Der Osloer Verkehrsverbund Ruter verwaltete die Daten seiner Straßenbahnen auf einem öffentlich les- und beschreibbaren MQTT-Server.

in denen das System erklärt wird (siehe ct.de/wke5). Die Adresse wird dort aus nachvollziehbaren Gründen nicht veröffentlicht.

Weil wir wegen Einreisebeschränkungen nicht selbst nach Oslo reisen konnten, kontaktierten wir einen Hackerspace in Oslo und fanden einen Kontakt, mit dessen Hilfe wir die Lücke bestätigen wollten. Das Ergebnis der Testfahrt: Bei den Daten auf dem Server handelte es sich um Echtzeitdaten, alle Fahrzeugnummern, die nächsten Haltestellen und die GPS-Positionen stimmten mit der Realität überein. Das System funktioniert allerdings nur in eine Richtung – die Daten aus den Bahnen werden zur Weiterverarbeitung auf dem MQTT-Server gesammelt. Zwar gestattete der Server Schreibzugriff, es gelang aber nicht, die Anzeigesysteme in den Zügen per MQTT fernzusteuern. Wer die Adresse des Servers kennt, kann aber womöglich interne Systeme gehörig durcheinanderbringen. Im Anschluss an das Experiment kontaktierten wir Ruter.

Geheime URL verpetzt

Besonders ungeschickt konfigurierten auch die Betreiber von Verkehrsüberwachungskameras in Taiwan ihren Server. Wir fanden einen MQTT-Broker, der Teil einer Bilderkennungsinfrastruktur ist. Ein KI-System wertet die Bilder von Verkehrsüberwachungskameras aus und notiert alle erkannten Regelverstöße in JSON-Objekten, zum Beispiel so:

```
{
"o_types": "Taxi",
"event_type":"IllegalTemporaryParking",
"report_type": "incident",
[...]
}
```

Zusätzlich zu den erkannten Ereignissen landeten aber auch die URLs zu den RTSP-Videostreams der Kameras auf dem MQTT-Server. Diese Adressen waren nicht für die Öffentlichkeit bestimmt und wären nicht zu erraten gewesen. So technisch beeindruckend die Bilderkennung funktionierte, so dilettantisch war die Einrichtung des Servers. Mit den Links kann man zum Beispiel im VLC-Mediaplayer das Geschehen auf den Straßen live verfolgen.

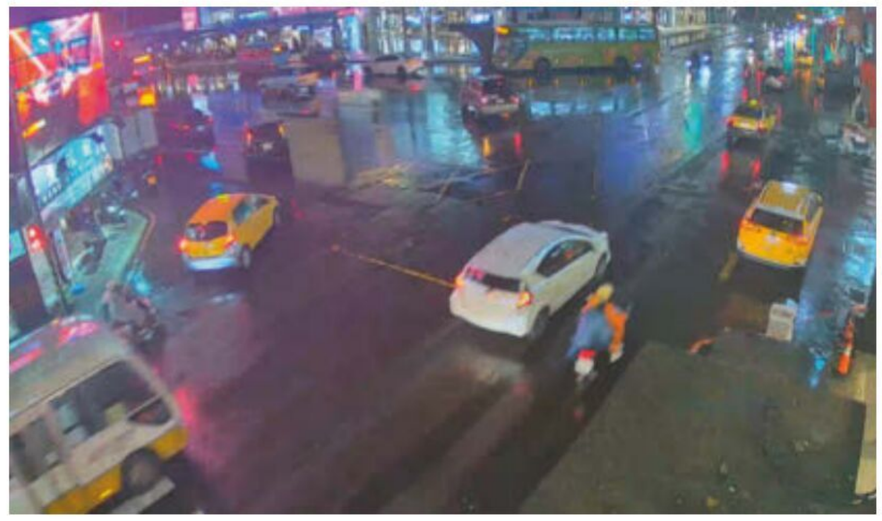
S7 für alle

Auf der Suche nach weiteren Industriesteuerungen recherchierten wir zunächst gängige Steuerprotokolle. Die Wahl fiel auf das Fernwartungsprotokoll ISO-TSAP, über das man Siemens-SIMATIC-Anlagen über das Netzwerk verwalten kann. Solche Anlagen sind in allen Industriezweigen weit verbreitet, die Chancen auf Treffer sollten dementsprechend hoch sein. Laut Dokumentation arbeitet das Protokoll auf Port 102 und ist ausdrücklich nur für lokale, abgeschottete Netze gedacht, in denen nur SIMATIC-Geräte miteinander sprechen. Weder Authentifizierung noch Verschlüsselung sind überhaupt vorgesehen. Ein solches Protokoll ins Internet zu hängen, ist daher eine ganz miserable Idee.

Wenig überraschend wurde unser Scanner im Internet aber schnell fündig. Offenbar antworteten

zahlreiche Steuerungen auf die Anfragen. Weil wir die passende Software zur Fernwartung nicht zur Hand hatten, probierten wir das Naheliegendste und öffneten die gefundenen IP-Adressen im Browser. Schon nach wenigen Versuchen begrüßte uns eine Weboberfläche mit der Bezeichnung „IBH Link S7++“. Dabei handelt es sich um ein Gateway eines deutschen Anbieters, mit dem man ältere Siemens-Anlagen mit einem (lokalen) Netzwerk verbinden kann. Der Betreiber, laut IP-Geodatenbank vermutlich aus der Ölindustrie im Nahen Osten, hatte kein Kennwort für den Admin-Zugang gesetzt. Kriminelle können das leicht ausnutzen: In der Oberfläche kann man die per PROFIBUS angeschlossenen Geräte nicht nur auslesen, sondern auch umkonfigurieren oder das System komplett vom Netz nehmen. Je nach Anlagentyp kann das verheerende Folgen haben.

Nach diesem ersten Fund gingen wir systematisch vor und prüften die Liste noch einmal automatisiert. Uns interessierten alle Adressen, unter denen sowohl Port 102 als auch Port 80 (für die Weboberfläche) offen waren. Auf Port 80 ließen wir ein Skript das HTML-Dokument auf eine Zeichenkette aus der Oberfläche untersuchen. Heraus kam eine Liste mit über 100 offenen Steuerungen, laut IP-Geodatenbank teilweise auch aus Deutschland. Ein Admin-Kennwort war nirgends gesetzt worden.



Die Überwachungskamera in Taiwan, die diese Aufnahme machte, war nur über eine nicht zu erratende Adresse erreichbar. Die lag allerdings ungeschützt auf einem MQTT-Server.

MIT Technology Review
Das Magazin für Innovation von Heise

Die Welt verstehen, wie sie morgen sein wird.

2 Ausgaben inklusive Prämie nach Wahl:

mit-tr.de/testen

40 % Rabatt

leserservice@heise.de +49 541/80 009 120 trvorteil.de/testen

Offen für alle: Eine von Dutzenden Industriesteuerungen, die ohne Schutz im Internet hängen. Gedacht sind die Geräte ausschließlich für lokale Netze.

Jeden einzelnen Betreiber ausfindig zu machen, ist unmöglich. Anhand einer IP-Adresse herauszufinden, wem ein Anschluss gehört, funktioniert leider nicht so einfach. Um welche Anlagentypen es sich handelt, kann man ebenfalls nicht genau feststellen. Von Ampelsteuerungen bis hin zu Fertigungsanlagen oder Pipelines kann alles dabei sein. Die Konfigurationsoberfläche enthält auch keinerlei Informationen, die auf den Besitzer hindeuten, sodass wir uns entschieden, den deutschen Hersteller IBHsoftec zu kontaktieren. Er bestätigte uns, die Gateways in die ganze Welt zu verkaufen. Gedacht sei das Gerät für lokale Netze und nicht für die Veröffentlichung im Internet. Nach Angaben des Herstellers findet sich im Handbuch der Hinweis, dass man unbedingt ein Kennwort vergeben müsse. Aufgrund unseres Hinweises kündigte man zusätzlich an, in einer zukünftigen Version der Software einen Warnhinweis in die Oberfläche einzubauen, solange das Kennwort nicht gesetzt wurde. Andere vernetzte Geräte des Herstellers zeigen diesen Hinweis bereits.

Die Verantwortung tragen in diesem Fall ganz klar die Anwender und der Fehler ist mehr als einfach zu verhindern: Möchte man die Anlage von unterwegs warten oder nicht für jedes kleine Problem zur Pipeline in den Nahen Osten reisen, sollte man sich dringend einen VPN-Server einrichten. Das kann ein Hardware-VPN-Gateway genauso übernehmen wie ein Raspberry Pi (für Industriekunden gibt es den auch für die Hutschienenmontage) mit Wireguard. Weder ISO-TSAP noch die Konfigurationsoberflächen von Steuerungen haben etwas im Internet verloren. Selbst wenn man ein Admin-Kennwort vergeben hat, kann man nicht sicher sein, dass die Software vor Angriffen wie Brute-Force-Attacken ausreichend geschützt ist.

Versuchung widerstehen

Die Beispiele zeigen, wie einfach es sowohl Hobby-Admins als auch fahrlässige Profis potenziellen Angreifern machen. In vielen Fällen können sie sich Exploits, Werkzeugkästen und Hintertüren sparen und einfach durch den Vordereingang spazieren.

Sollten Sie selbst für ein Unternehmen oder ein Smart-Home verantwortlich sein: Widerstehen Sie den Versuchungen der vermeintlich einfachen Lösungen. Geräte, die für private Netzwerke gedacht sind, gehören nicht per Portfreigabe ins Internet. Um unangenehme Überraschungen zu vermeiden, sollten Sie sich ein paar Stunden Zeit nehmen und mal die Position der Gegenseite einnehmen – untersuchen Sie Ihr eigenes Netzwerk von außen und suchen Sie nach offenen Ports und unverschlüsselten Diensten. Dabei helfen Portscanner auf der Kommandozeile (wie der Klassiker `nmap`) oder der Online-Scanner bei heise Security (siehe ct.de/wke5). Für jeden offenen Port brauchen Sie einen triftigen Grund. Ein VPN ist immer die beste Wahl; ist das nicht sinnvoll oder umsetzbar, gilt: Verschlüsseln und Authentifizieren ist Pflicht. (jam) c't

Literatur

[1] Jan Mahn, **Weltsprache**, Das Protokoll MQTT für robusten Datenaustausch in Industrie und Hausautomation, c't 6/2018, S. 164

Dokumente und Werkzeuge

ct.de/wke5

inside agile

AGILE LEADERSHIP CONFERENCE

So werden agile Teams besser

9. Dezember 2021 ONLINE

Jetzt Tickets sichern!

Sind in einem Unternehmen Scrum, Kanban oder andere Ansätze auf Teamebene eingeführt, stehen Führung und Management vor neuen Herausforderungen:

- Wie führt man selbstorganisierte Teams im Gegensatz zu Einzelpersonen?
- Wie kann man Mitarbeitende beurteilen, wenn die Teamleistung im Fokus steht und die Individualleistung von außen kaum erkennbar ist?
- Braucht es überhaupt noch disziplinarische Führungskräfte? Wenn ja, in welcher Menge und mit welchen Aufgaben?

Die Agile Leadership Conference bietet einen fundierten, praxisorientierten Überblick, was agiles Arbeiten für die Führung in Unternehmen bedeutet.

Veranstalter heise Developer · dpunkt.verlag

in Kooperation mit it-agile

+++ Außerdem Online-Workshops am 14. Dezember · 12. und 13. Dezember +++

alc.inside-agile.de

Hintertür zu Wordpress

Wordpress gilt als vielseitiges und einfach zu wartendes CMS. Doch viele Admins vergessen, die mächtigen Schnittstellen zu schützen, und ermöglichen so ungewollt den Zugriff auf nicht öffentliche Inhalte und Dateien.

Von **Mirko Dölle und Jan Mahn**

Wordpress ist das weltweit wohl meistgenutzte CMS, es kommt in großen Konzernen genauso zum Einsatz wie bei privaten Homepages. Viele Provider bieten Wordpress als Komplettpaket inklusive Webserver an, und für die grundlegende Bedienung braucht es kein Informatikstudium. Doch das System hat Tücken: So erlauben viele Wordpress-Installationen über die Hintertür Zugriff auf Daten, die der Betreiber eigentlich gar nicht veröffentlichen wollte.

Die Ursache für die ungeplante Geschwätzigkeit ist die Programmierschnittstelle, das JSON-API, über das man Wordpress mit anderen Programmen verbinden kann. Dass diese Schnittstelle ohne weitere Maßnahmen nicht gegen lesende Zugriffe geschützt ist, verrät die offizielle Dokumentation leider nicht an prominenter Stelle.

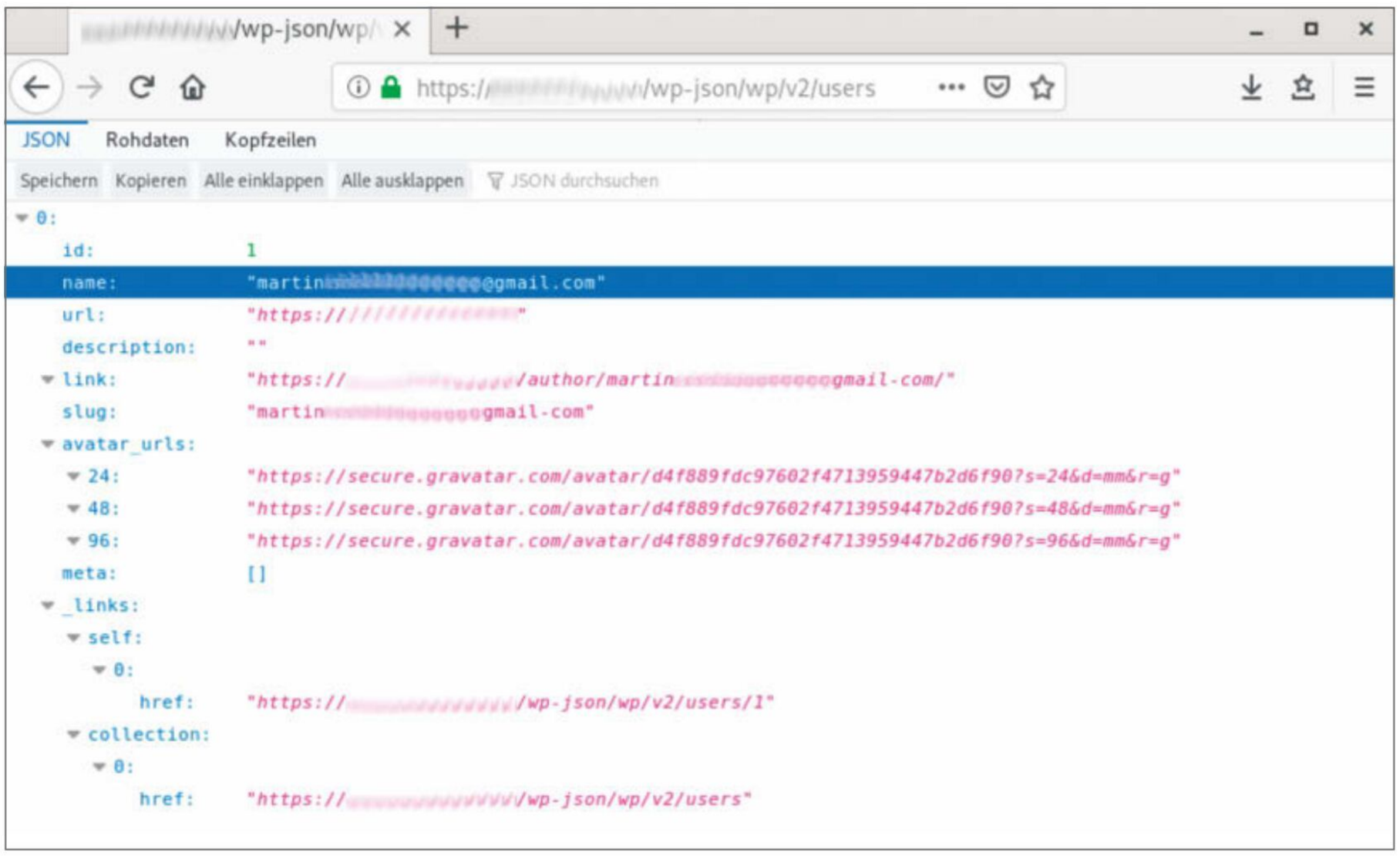
Ausgeplaudert

Über diesen Kanal können Neugierige leicht Musiktitel noch vor dem geplanten Veröffentlichungstermin herunterladen oder gelangen sogar an streng vertrauliche interne Dokumente. Die Hintertür erlaubt es aber Angreifern auch, vorab und ohne rechtliche Risiken wertvolle Informationen über das CMS zu sammeln, die sie dann zum Beispiel für Brute-Force-Angriffe auf Passwörter einsetzen können. Für effizientes Brute-Force kommt gern die zweite Schnittstelle mit dem Namen XML-RPC zum Einsatz.

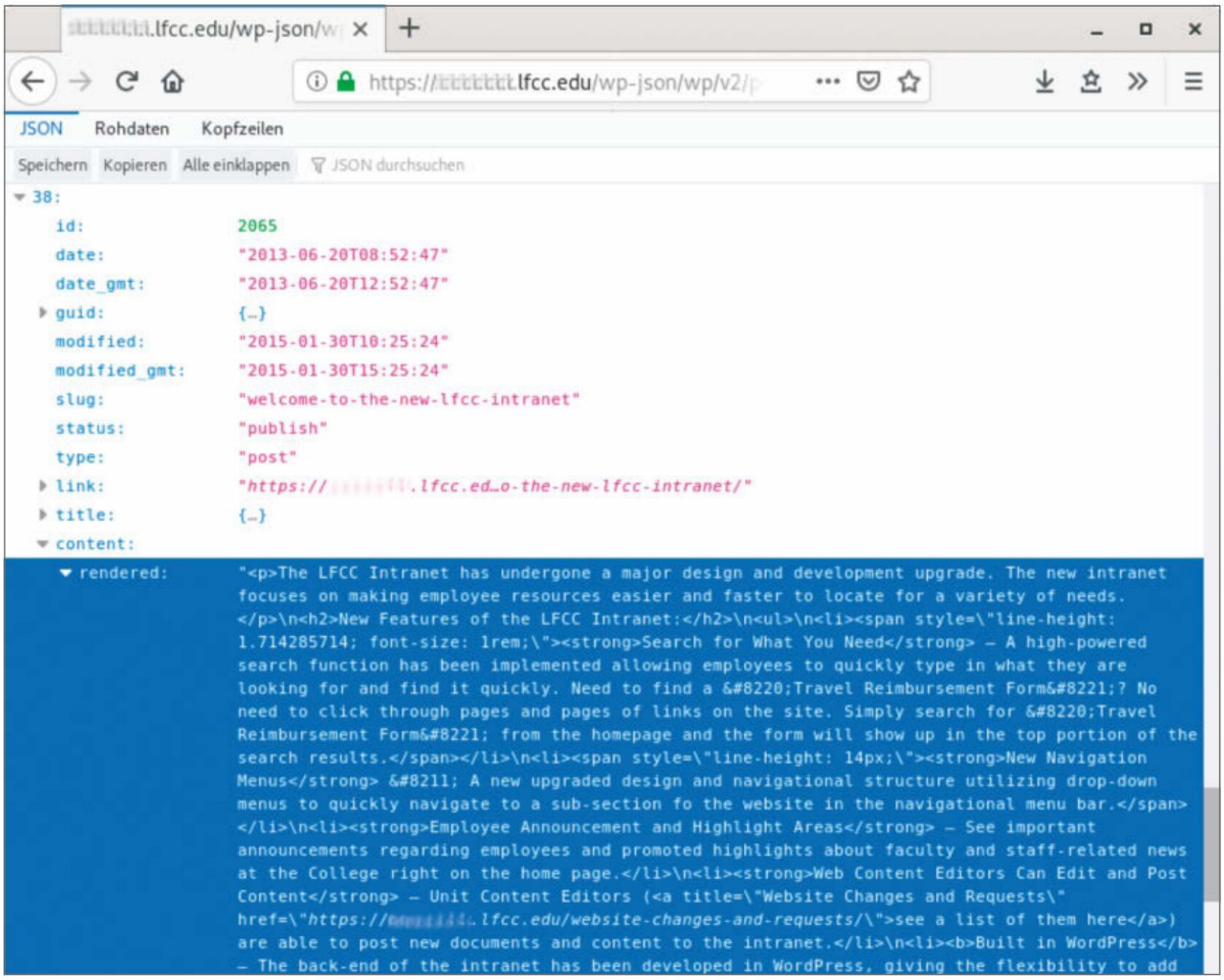
Verwundbare Wordpress-Installationen zu finden ist kinderleicht. Die IoT-Suchmaschine Shodan.io zum Beispiel hat eine eigene Kategorie für Wordpress. Für die Suche braucht man allerdings einen kostenpflichtigen Account. Alle anderen suchen stattdessen bei gewöhnlichen Suchmaschinen nach den Begriffen „wp-content“, „wp-include“ oder „wp-login“ – alle drei sind untrügliche Anzeichen dafür, dass die Website Wordpress verwendet. Möchte man herausfinden, ob eine Webseite von Wordpress ausgeliefert wird, reicht meist ein Blick auf die URL eines eingebetteten Bildes. Enthält diese „wp-content“, ist das ein sicheres Zeichen.

Offene Hintertüren

Ob die Admins vergessen haben, die API-Hintertüren zu schließen, finden Sie ganz einfach mit dem Browser heraus, indem Sie das Unterverzeichnis „/wp-json“ ansurfen. Wird Ihnen hier eine JSON-Struktur angezeigt, ist das API meist komplett offen. Wenn das JSON-API nicht unter „wp-json“ antwortet, muss man an anderen Stellen danach suchen. Hinweise findet man oft im HTML-Quelltext.



Verwendet der Admin E-Mail-Adressen als Benutzernamen für Wordpress, wird das ungeschützte JSON-API zum maschinenlesbaren Selbstbedienungsladen für Spammer.



Schönes neues Intranet: Der Server des Lord Fairfax Community College ist nicht nur aus dem Internet erreichbar, über das ungeschützte JSON-API von Wordpress hat jedermann Zugriff auf über 2500 Dokumente, Scans, Dienstpläne und Mailverteiler.

Auf der Website der US-Sängerin Laura Brehm etwa, die für ihre Zusammenarbeit mit dem deutschen EDM-Musiker TheFatRat bekannt geworden ist, befindet sich das API unter „/index.php/wp-json“. Das findet man leicht heraus, indem man im ausgelieferten HTML-Code der Seite nach „wp-json“ sucht.

Hat man das API lokalisiert, kann man sich per Browser weiter umsehen. Ein Blick in „/index.php/wp-json/wp/v2/media“ förderte ein paar vergessene, sehr hoch auflösende Bilder der Sängerin zutage. Dies ist ein Standardproblem von so gut wie allen Wordpress-Installationen, die wir im Rahmen unserer Recherche abgeklopft haben: Oft werden Bilder in Originalauflösung mit mehreren Megapixeln hochgeladen, die Wordpress dann in mehrere Standardauflösungen herunterrechnet. Eingebunden werden dann die verkleinerten Bilder, doch wenn man die Originale nicht löscht, findet man sie über das JSON-API und kann sie ungeschützt herunterladen.

Erkundet man das JSON-API weiter, findet man unter „/index.php/wp-json/wp/v2/users“ auf der Seite von Laura Brehm heraus, dass es bei dieser Wordpress-Installation nur einen einzigen Benutzer mit dem Namen „laura“ gibt – eine wichtige Information,

mit der Angreifer anschließend über die ebenfalls offene XML-RPC-Schnittstelle eine Brute-Force-Attacke auf das Passwort mit mehreren Hundert Versuchen pro Aufruf starten könnten.

Andere Wordpress-Seiten verwendeten die E-Mail-Adresse der Benutzer als Benutzernamen oder als Wordpress-Slug, darunter auch eine Seite, die sich mit der asiatischen Poker-Variante Teen Patti beschäftigt. Die Nachlässigkeit macht den Endpunkt „wp/v2/users“ des JSON-API zu einem Selbstbedienungsladen für Spammer.

Blankopass

Richtig verhängnisvoll wurde der Einrichtungsfehler für das Lord Fairfax Community College in den USA. Dort hat man versucht, auf dem von außen erreichbaren Intranet-Server einen geschützten Bereich zu errichten, indem man die Seite per Plug-in mit einer verpflichtenden Anmeldung versah. Dieses sorgte aber lediglich dafür, dass man zum Wordpress-Login umgeleitet wird, wenn man Inhalte über das Frontend abruft. Das JSON-API wurde nicht per Umleitung gesichert, sodass jedermann darauf zugreifen und so über den Link „/wp-json/wp/v2/pages“ sämtliche Seiten, über „/wp-json/wp/v2/posts“ sämtliche Forumsbeiträge und über „/wp-json/wp/v2/comments“ sämtliche Kommentare lesen kann; über „/wp-json/wp/v2/media“ sind sämtliche Dateien erreichbar.

Auf diese Weise hat jedermann freien Zugriff auf über 2500 interne Protokolle, Mailing-Listen, Dienstpläne der Admin-Rufbereitschaft, Telefonverzeichnisse, Dropbox-Links, Links auf Google-Docs-Dokumente und archivierte Akten aus den Jahren 2008 bis heute.

Fundgrube

Bei vielen offenen Wordpress-Installationen ist die Mediendatenbank eine große Fundgrube: Sie wird in Firmen häufig auch als Datenhalde für den internen Datenaustausch missbraucht. Dahinter steckt auch die falsche Annahme, dass Inhalte, die in keinem öffentlichen Post verlinkt werden, für Dritte nicht auffindbar wären. Für das Frontend der Seite stimmt das auch, denn schließlich kann man nicht einfach ein Directory-Listing des Verzeichnisses „/wp-content“ abrufen.

Diese Auflistung findet sich aber in der Mediendatenbank, die man über das API erreicht. Bei unseren Recherchen fanden wir interne Fotos von Firmen, bei verschiedenen Musikern Musikdateien, Bilder und Videos von künftigen Projekten und in einem Fall sogar ein Backup des kompletten Webservers als Zip-Datei. Das passiert nicht nur kleinen Unternehmen. Die italienische Consulting-Firma MediaEngine, die für etliche namhafte Firmen wie Red Bull, Armani, Continental, BMW, Maserati, Allianz, UniCredit und Virgin arbeitet, betreibt ebenfalls ein Wordpress-CMS mit offenem JSON-API. Dort fanden wir in den Posts und in der Mediendatenbank unter anderem Konzepte und Entwürfe für künftige Website-Auftritte, die vermutlich nicht für die Öffentlichkeit bestimmt waren.

Ein Paradebeispiel dafür, wie Wordpress interne Informationen ausplaudert, war die Website der schweizerischen Firma Akiro. Als wir bei unseren Recherchen darauf stießen, bestand sie scheinbar nur aus dem Firmenlogo und den Impressumsangaben, sonst gab es keine Informationen. Über das offene JSON-API fanden wir jedoch heraus, dass noch ein Produktkatalog und etliche ältere Seiten veröffentlicht waren. Darunter befand sich auch ein Kontaktformular, das sich zu allem Überfluss auch noch für Spam und Phishing missbrauchen ließ (siehe Seite 152) – und am 3. September 2020 auch tatsächlich zum Massenversand von Werbung für eine zwielichtige Lotterie benutzt wurde.

Abhilfe

Um das API für Externe abzuklemmen, gibt es mehrere Wege. Einige empfehlen, es komplett abzuschalten. Das funktioniert aber nicht, wenn man den modernen Editor Gutenberg benutzt, der auf das API zugreift. Stattdessen sollten Sie eine Authentifizierung verlangen.

Eine Möglichkeit ist es, alle Pfade unterhalb von „/wp-json“ direkt vom Webserver mit HTTP-Basic-Auth sichern zu lassen. Einfacher ist es, sich mit Wordpress-Bordmitteln zu helfen. Öffnen Sie dazu die Datei functions.php im verwendeten Theme. und fügen Sie dort die Funktion add_filter() ein, die wir Ihnen über den Link ct.de/wqhw zum Download bereitgestellt haben.

Natürlich haben wir vorab alle Betreiber der in diesem Artikel genannten Wordpress-Installationen über die bestehenden Probleme und die anstehende Veröffentlichung informiert, im Fall des College bemühten wir zusätzlich den Support-Chat. Trotzdem waren die JSON-APIs bei Redaktionsschluss weiterhin erreichbar – offenbar sehen die Betreiber keinen Handlungsbedarf. (mid) c't

Code zum Absichern

ct.de/wqhw

Bild: Andreas Martini

Newsletter als Spam-Schleudern

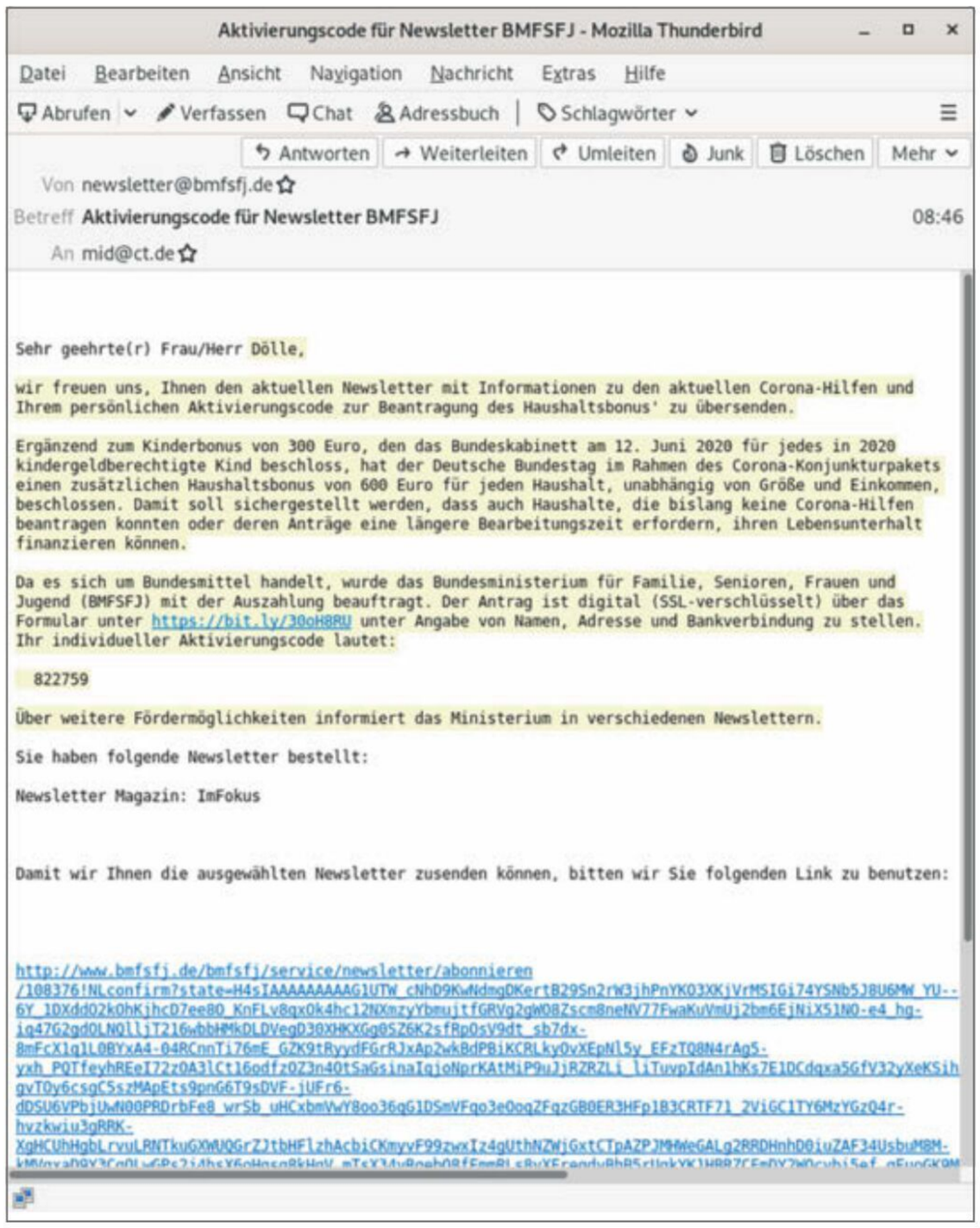
Newsletter-Anmeldungen und Kontaktformulare auf bekannten Internetseiten sind für Spammer und Phisher eine willkommene Möglichkeit, ihre Mails an Spamfiltern und Internet-Schutzprogrammen vorbei an den Mann zu bringen. Die Website-Betreiber riskieren dabei schlimmstenfalls ihre Existenz.

Von **Mirko Dölle**

Willkommen, noch ein Klick Herr Viagra Super Cheap http://bit.ly/30oH8RU – ehe man sich versieht, ist man auch schon in die Spam-Falle getappt. Im Kampf gegen immer schärfere Spamfilter missbrauchen Spammer und Phisher Anmeldeformulare von Newslettern, indem sie sie automatisiert mit Mail-Adressen aus Spammer-Datenbanken füttern und anstelle des Namens ihre Potenzmittelwerbung unterbringen. Manche Newsletter- und Kontaktformulare eignen sich sogar für Phishing-Attacken, weil sie ungeprüft formatierte Texte akzeptieren.

Dabei missbrauchen Spammer bevorzugt Websites von Regierungseinrichtungen und namhaften Firmen oder Organisationen, da diese ein hohes Ansehen genießen und nicht ohne triftigen Grund auf Spam-Blacklists der großen Mail-Provider landen. Mit Erfolg, wie c't durch verschiedene Missbrauchsfälle und Stichproben herausfand.

Außerdem bekommen die Mails auch einen höchst offiziellen Anstrich: Gut gemachte Fälschungen kann der Empfänger kaum mehr erkennen. Besonders perfide ist diese Methode, wenn die betroffene Behörde oder Firma bereits E-Mail-Authentifizierung per SPF oder DKIM verwendet und die Phishing-Mail nachweislich von einem autorisierten Server stammt oder mit dem korrekten kryptografischen Schlüssel signiert ist. Wer soll da noch misstrauisch werden?



Durch die völlig ungeprüfte Verwendung von Benutzereingaben aus dem Newsletter-Anmeldeformular (gelb) ließen sich über den Webserver des Bundesfamilienministeriums Phishing-Mails verschicken, die kaum als solche zu erkennen waren.

Ungeprüft und ungefiltert

Dabei entscheidet die Sorgfalt der Programmierer des Newsletter- oder Mail-Backends darüber, ob und inwiefern sich das Anmelde- oder Kontaktformular missbrauchen lässt. Gefahr besteht immer dann, wenn Eingaben aus dem Formular, etwa der Name, in eine Verifizierungs- oder Bestätigungs-Mail übernommen, aber nicht ausreichend geprüft werden.

Oft wird bei Newsletter-Formularen nur die Länge der Namensfelder beschränkt, eine inhaltliche Prüfung findet nicht statt – schließlich will man die Interessenten nicht damit vor den Kopf stoßen, dass etwaige Sonderzeichen in ihrem Namen nicht akzeptiert werden. Ein solches Newsletter-Formular lässt sich immer für Spam missbrauchen, indem Angreifer etwa den Vornamen „Viagra Super Cheap“ und als Nachnamen „http://bit.ly/30oH8RU“ eintragen – fertig ist der Potenzmittel-Spam. Fehlt ein Captcha, werden die Felder des Anmeldeformulars tausendfach automatisch per Skript befüllt; die Mail-Adressen der Opfer gibt es für wenig Geld auf dem Schwarzmarkt.

Dass ein Anbieter URLs oder Mailadressen aus den Namensfeldern entfernt, haben wir bei Stichproben nicht feststellen können; wann immer unsere Eingaben in der Bestätigungsmail auftauchten, konnten wir dort auch Links unterbringen. Lediglich HTML-Tags wurden meist generell entfernt, immerhin.

Fundgrube

Um Server mit angreifbaren Formularen zu finden, benötigt man weder Spezialwissen noch besondere Werkzeuge. Ob Google Web-Suche oder DuckDuckGo – wenn man nach den Begriffen „Newsletter“ und „Name“ oder „Vorname“ sucht, findet man unzählige Newsletter-Anmeldeformulare aus aller Welt, bei der man zusätzlich zur E-Mail-Adresse auch den Namen eingeben kann.

Im zweiten Schritt abonniert man den Newsletter und schaut sich die Bestätigungs-Mail an: Manche Newsletter-Anbieter wollen besonders kundenfreundlich erscheinen und deshalb die Interessenten schon in der ersten E-Mail mit ihrem Namen ansprechen – weshalb sie kurzerhand die Eingaben aus dem Anmeldeformular dort einbetten. Für Angreifer das Einfallstor, um Werbung oder Phishing-Nachrichten einzuschleusen.

Eine andere beliebte Schwachstelle sind Kontaktformulare mit der Option, eine Kopie der Anfrage an sich selbst zu schicken. Hier haben Angreifer nahezu Narrenfreiheit, schließlich gibt es hier Eingabefelder, die für große Mengen Text vorgesehen sind – sofern es denn überhaupt eine Längenbeschränkung gibt.

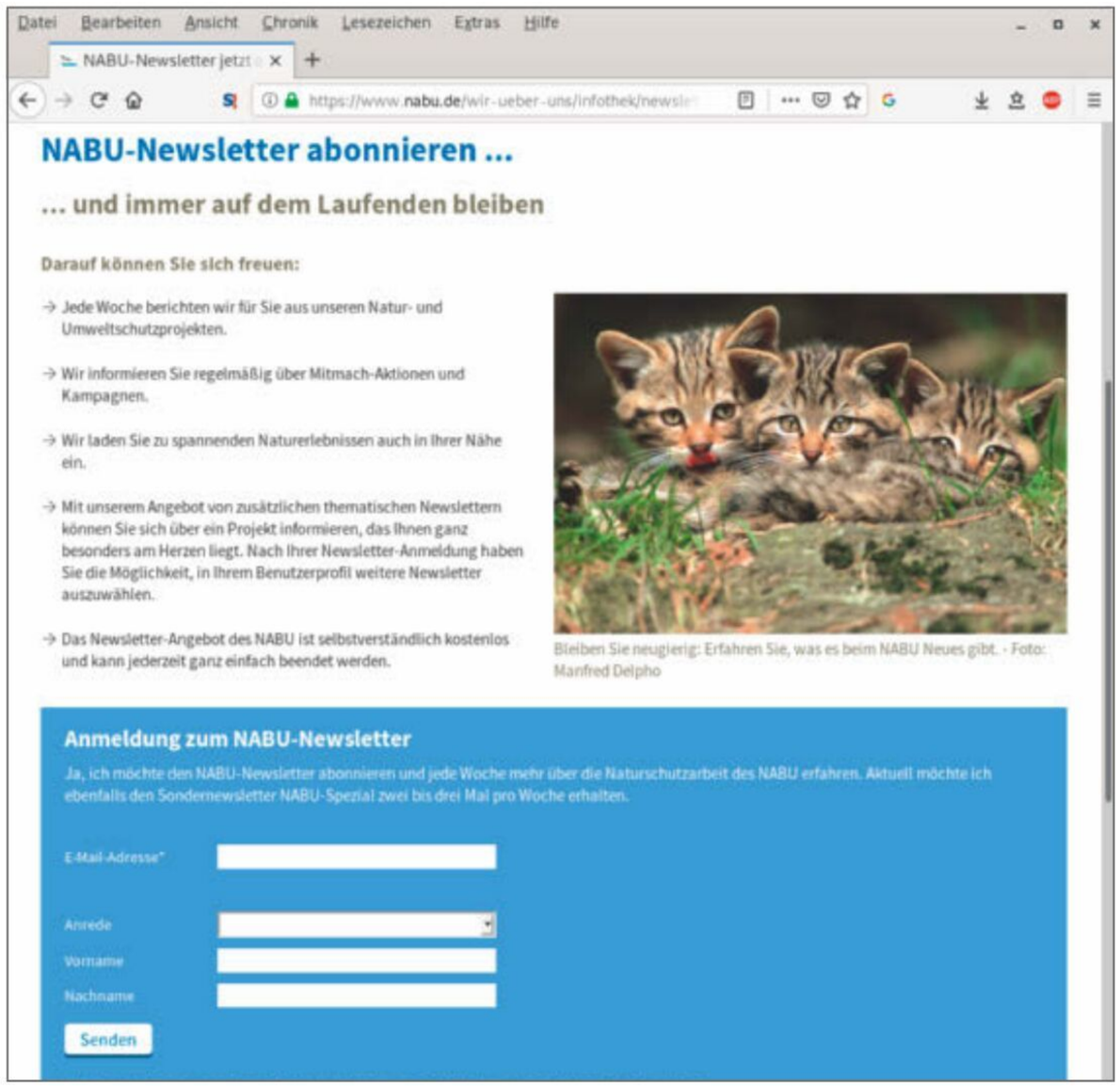
Vertrauensfragen

Ein lascher Umgang mit Benutzereingaben birgt noch ein zweites Risiko: Viele Newsletter-Backends speichern die Angaben in einer Datenbank. Werden die Namensfelder ungefiltert durchgereicht, entsteht schnell eine SQL-Injection-Lücke – mit der Gefahr des Diebstahls sämtlicher Daten. Überprüfen konnten wir so etwas im Rahmen unserer Recherche nicht, das wäre strafbar.

Für Phisher sind vor allem Behörden und große IT-Unternehmen interessant, genießen diese doch ein hohes Vertrauen bei den Opfern – was eher sie dazu verleiten könnte, ihre Daten auf der präparierten Seite einzugeben. Die Anfang August von uns entdeckte Spam- und Phishing-Lücke beim Bundesfamilienministerium [1] war deshalb so brisant, weil sich die Bestätigungsmail mangels Eingabeprüfungen sehr weitreichend umgestalten ließ und auch mehrere Kilobyte formatierten Text klaglos verarbeitete. Die Empfänger hätten kaum eine Chance, einen solchen Phishing-Versuch zu erkennen – schließlich stammte die Mail tatsächlich von einem Server des Bundesfamilienministeriums.

Eine ähnliche Lücke fanden wir im Newsletter-Anmeldeformular des Naturschutzverbands NABU. Auch hier wurden Vorname und Nachname abgefragt und ungeprüft in die Verifizierungsmail übernommen. Außerdem fehlte ein Captcha oder sonstiger Schutz vor automatisiertem Missbrauch, wodurch Spammer nach Auskunft des NABU in der Nacht vom 26. auf den 27. August 2020 gut 250 000 Newsletter-Verifizierungsmails mit Werbung für Porno-Seiten verschicken konnten.

Nachdem die ungewöhnlichen Aktivitäten durch das Server-Monitoring bemerkt wurden, sei die Newsletter-Anmeldung unverzüglich deaktiviert worden, schreibt der NABU in seiner Stellungnahme gegenüber c't. Das ist plausibel, da unsere Honeypots nur eine solche Newsletter-Spam-Mail erreichte, während wir vom Bundesfamilienministerium mehrere erhielten. Die neue Newsletter-Anmeldeseite des NABU ist nun durch ein Captcha vor massenhaftem Missbrauch geschützt und überträgt abgesehen von der Mailadresse keine Angaben mehr in die Verifizierungsmail.



Auch die Anmeldeseite des NABU-Newsletters übertrug Vor- und Nachnamen in die Verifizierungsmail und war nicht etwa durch ein Captcha geschützt, weshalb Spammer sie am 27. August für den massenhaften Versand von Porno-Werbung missbrauchen konnten.

Auch wenn eine persönliche Ansprache als besonders kundenfreundlich gilt, sollte man lieber unpersönlich bleiben, als den Empfänger der Newsletter-Verifizierung zu gefährden. Die Alternative ist, die Benutzereingaben stark zu begrenzen und aufwendig auf unerwünschte Inhalte zu überprüfen, bevor man sie verwendet.

Pleite durch Spam

Ein solcher Missbrauchsfall ist nicht nur für das Ansehen schädlich, es kann Firmen die Existenz kosten, wenn ihre Server und Domains aufgrund des massenhaften Spam-Versands auf der Blacklist von Spamhaus und in anderen Anti-Spam-Datenbanken landen. Die Nutzung und automatische Aktualisierung solcher Datenbanken mit bekannten Spamversendern ist in Firmen weit verbreitet, E-Mail-Anbieter bauen solche

Datenbanken sogar selbst anhand eingehender Spam-Mails an ihre Kunden auf. Das kann innerhalb weniger Stunden dazu führen, dass ein Unternehmen keinerlei E-Mails mehr versenden kann, weil die E-Mail-Anbieter die Annahme aller Nachrichten eines Servers verweigern, Mails von dort generell als Spam brandmarken oder gar nicht zustellen.

Damit fällt für das gesamte Unternehmen das Kommunikationsmedium E-Mail von einem Moment auf den anderen aus. Bis man herausgefunden hat, in welche Anti-Spam-Datenbanken man aufgenommen wurde und die Betreiber davon überzeugt hat, den Eintrag zu entfernen, weil das Problem inzwischen behoben ist, können Wochen vergehen. Teilweise werden solche Einträge auch nur gegen eine Geldzahlung und erst nach einer gewissen Zeitspanne wieder gelöscht.

Ein ungeschütztes Kontaktformular, dessen Inhalt man sich in Kopie an seine Mailadresse schicken lassen kann, fanden wir zufällig bei unseren Recherchen zu WordPress (siehe Seite 148) bei der schweizerischen Firma Akiro. Wie beim Bundesfamilienministerium ließ sich auch im Kontaktformular von Akiro kilobyteweise formatierter Text unterbringen und an eine beliebige E-Mail-Adresse verschicken. Der Webserver von Akiro wurde am 3. September 2020 für eine groß angelegte Spam-Aktion missbraucht, er hätte aber auch für Phishing genutzt werden können, etwa um falsche Auftragsbestätigungen mit Links zu infizierten Office-Dokumenten an andere Firmen zu verschicken. Auch hier gilt: Ein einfaches Captcha hätte ausgereicht, um der Spam-Aktion einen Riegel vorzuschieben. Phishing lässt sich so aber nicht unterbinden.

Überlastungsschutz

Newsletter-Anmeldungen, die nicht etwa durch Captchas vor automatisierter Nutzung geschützt sind, lassen sich unter Umständen auch gezielt für DoS-Angriffe auf die Mailserver von Firmen oder Einzelpersonen missbrauchen. Dazu müssen allerdings mehrere Faktoren zusammenkommen: Für die Bestätigung der Newsletter-Anmeldung genügt es, einen in der E-Mail enthaltenen Link aufzurufen. Außerdem muss das Opfer ein Viren- oder Trojaner-Schutzprogramm verwenden, das die in E-Mails enthaltenen Links vorab auf Schadsoftware überprüft. Solche Programme werden in Firmen als Emotet-Schutz verwendet, sie können aber auch Bestandteil eines Antivirus- oder Internet-Schutzprogramms für private Anwender sein.

Ob ein Unternehmen oder eine Einzelperson einen solchen URL-Checker verwendet, kann der Angreifer leicht herausfinden: Dazu verschickt er außerhalb üblicher Bürozeiten zum Beispiel über ein angreifbares Kontaktformular einer Website eine Test-Mail, die einen individuellen Link zu einem Webserver des Angreifers enthält. Findet er kurze Zeit später im Log des Webservers einen oder mehrere Abrufe dieser URL, kann er davon ausgehen, dass Links automatisch überprüft werden.

Um das Mailsystem zu überlasten, meldet der Angreifer möglichst viele Mitarbeiter bei möglichst vielen Newslettern aus aller Welt an. Das Ergebnis ist eine Mailflut aus allen Richtungen mit Bestätigungen und anschließend den Newslettern. Wir haben das exemplarisch mit dem Newsletter des „eco Verband der Internetwirtschaft“ ausprobiert.

Massen-Rückläufer

Da die Mailadressen-Datenbanken der Spammer auch viele falsche oder veraltete Adressen enthalten, kommt es beim Missbrauch von Newsletter-Anmeldungen außerdem zu einer erheblichen Menge an Rückläufern (Backscatter) an die Absenderadresse der Newsletter-Verifizierung. Das bestätigte uns der NABU, bei dem Missbrauchsfall Anfang September 2020 seien über 17 500 Mails als nicht zustellbar oder mit anderen Statusmeldungen zurückgekommen – das ist ein Anteil von sieben Prozent. Dank der schnellen Reaktion der Admins war das im Fall des NABU noch überschaubar. Gelingt den Spammern jedoch der Versand einiger Millionen Mails, kann Backscatter durchaus den Mailserver überlasten, was einer Denial-of-Service-Attacke gleichkommt.

Newsletter-Anbieter sollten automatisierten Missbrauch deshalb aus eigenem Interesse unterbinden, etwa indem sie ein Captcha einbinden. Das muss nicht der bekannte Google-Dienst sein, dessen Einsatz datenschutzrechtlich mehr als heikel ist, es gibt auch etliche lokal nutzbare Captchas.

Indem Newsletter-Anbieter außerdem ein interaktives Element auf der Bestätigungsseite einbinden, das vom Newsletter-Abonnenten angeklickt werden muss, verhindern sie auch, dass die Virenscanner und Emotet-Schutzprogramme ein vermeintliches Newsletter-Abo automatisch bestätigen oder den Newsletter immer wieder automatisch abbestellen, weil sie den am Ende des Newsletters eingebetteten Abmelde-Link auf Schadsoftware überprüfen. So werden echte Interessenten des Newsletters nicht gegen ihren Willen wieder hinausgeworfen. (mid) c't

Literatur

[1] Mirko Dölle, **Staatliche Phishing-Hilfe**, Bundesministeriums-Website ermöglichte Spamming und Phishing, c't 18/2020, S. 40

Bild: Thorsten Hübner

Unachtsamer Phisher enttarnt

Phishing und Spamming sind eigene kriminelle Industriezweige, die Hand in Hand arbeiten. Weil sich ein Phisher einen dummen Fehler leistete, erfuhren wir mehr über ihn, als ihm lieb sein konnte.

Von **Jan Mahn**

Eine verdächtige Mail mit einer noch verdächtigeren URL landete in einem Spam-Filter, den einer unserer Leser betreut. Beruflich kümmert er sich um IT-Sicherheit und so war ihm sofort klar, dass es sich bei der vermeintlichen Aufforderung des Mailanbieters, sich aus Sicherheitsgründen sofort an der Webmail-Oberfläche anzumelden, um einen Phishing-Versuch handeln musste. Der Link in der Mail zeigte zu einer Subdomain von web.core.windows.net und enthielt am Ende als Query-Parameter die Mailadresse. Neugierig schaute sich der Leser die Seite an und fand ein anschauliches Beispiel für eine Phishing-Attacke – und eine Sicherheitslücke zu Ungunsten des Phishers.

In einer virtuellen Maschine probierten wir den Link aus und tauschten die Mailadresse im Link durch eine Beispiel-Adresse beim deutschen Mail-Hoster Web.de aus. In der Mitte erschien vor grauem Hintergrund ein stark deformiertes Login-Fenster, das nur entfernt an das Original von Web.de erinnerte. Wer dort bereitwillig sein Kennwort eingab, musste schon sehr naiv sein.

Ein Blick in die Entwicklerwerkzeuge des Browsers enthüllte, was sich der Phisher eigentlich überlegt hatte: Per Iframe sollte hinter dem Fenster die echte Web.de-Seite von https://web.de eingebettet werden, darüber sollte das selbstgebaute Login-Fenster schweben. Das hätte die Täuschung zumindest etwas besser gemacht und die Erfolgsquote sicher erhöht. Doch daraus wurde nichts: Weil die Betreiber von Web.de schon länger mit Phishing gegen ihre Nutzer zu tun haben, haben sie ihre Server so konfiguriert, dass sie folgenden Header mitschicken:

```
content-security-policy: frame-ancestors 'none'
```

Moderne Browser weigern sich dann, die Seite im Iframe darzustellen – es bleibt eine unattraktive graue Fläche. Eine kleine Einstellung im Server, die Phishing zumindest etwas erschwert. Wer selbst Login-Seiten betreibt, ist gut beraten, diesen Header zu aktivieren.

Die Phishing-Seite war so programmiert, dass sie dynamisch auf unterschiedliche Mailhoster reagierte: In der URL wurde die Mailadresse des Opfers übergeben, die Phishing-Links müssen also in einer Art Serienbrief personalisiert generiert und verschickt werden. Je nach Mailadresse versucht die Seite, unterschiedliche Mail-Anbieter per Iframe einzubinden und stellt das Favicon der Seite als Logo im Login-Fenster dar. Eine kleine Versuchsreihe zeigte aber, dass die gängigsten Mail-Provider Iframe-Einbindungen per Header unterbunden und die meisten Opfer wohl eine graue Fläche gesehen haben.

Das Phishing-Manöver wirkte etwas verzweifelt. Geplant vom Phisher war, dass im Hintergrund die echte Login-Seite per Iframe eingebunden wird. Das verhindern jedoch die Sicherheitsmaßnahmen moderner Browser.

Passwortversand

Neben Iframe und gefälschtem Login-Fenster fanden wir JavaScript auf der Seite. Die Analyse hatten die Entwickler aber deutlich erschwert und den Code mit einem sogenannten Obfuskator etwas unkenntlich gemacht. Ein solches Werkzeug ersetzt möglichst viel aussagekräftigen Klartext (Strings, Funktions- und Variablennamen) durch andere Zeichen, in diesem Fall durch hexadezimale Zeichen. So wird es zwar nicht unmöglich, den Code zu verstehen, aber immerhin mühsam (als Gegenmittel gibt es wiederum De-Obfuskatoren).

Aber auch ohne JavaScript-Code im Klartext konnten wir beobachten, was beim vermeintlichen Anmelden geschah. Die Entwicklerwerkzeuge aller Browser haben einen Reiter „Netzwerk“, der HTTP-Aufrufe mit Anfrage- und Antwortdaten protokolliert und darstellt. Für gewöhnlich wird das Kennwort per HTTP an den Server geschickt und dort gespeichert. Doch dieser Fall war ungewöhnlich – und nicht gerade geschickt:

Sandte man das Formular ab, wurde eine Anfrage an den Endpunkt `sendMessage` von `https://api.telegram.org/` geschickt, in den Formulardaten das Kennwort, das man ins Kennwortfeld getippt hatte:

```
##+nEw+l0g+##
+----------------------+
max.muster@web.de+|+geheimes_passwort
+----------------------+
```

Im Messenger Telegram kann jeder einen Bot anlegen und mit ihm eine Kommunikation starten. Bots sind klar als solche gekennzeichnet und ganz hilfreich, um sich zum Beispiel Statusmeldungen seiner Server oder des vernetzten Zuhauses schicken zu lassen. Dafür reicht ein API-Aufruf, wie wir ihn gefunden haben. Der Phisher nutzte dieses Verfahren, um alle Kennworteingaben von Opfern sofort aufs Handy zu bekommen.

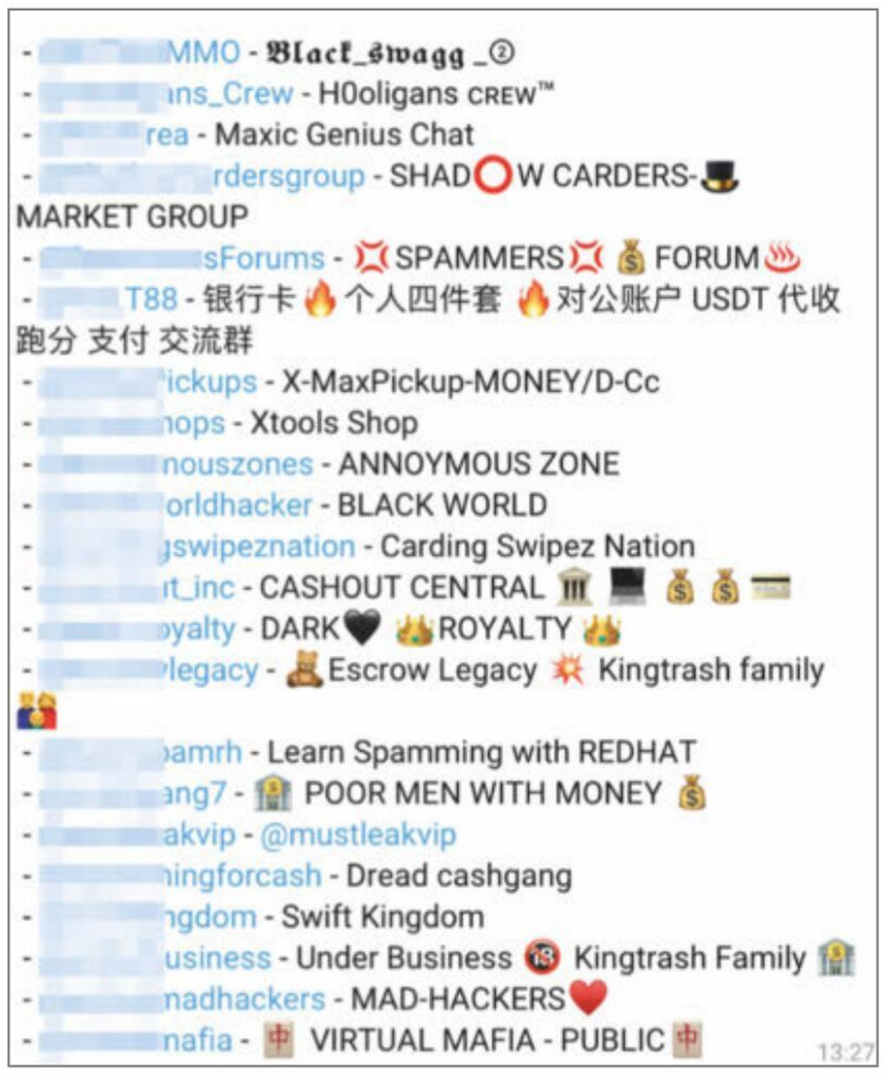
Um das API zu nutzen, generiert Telegram ein Token, auf das man gut aufpassen muss – keinesfalls darf man das API direkt per JavaScript aus einer öffentlichen Seite heraus ansprechen: Die URL zum

API enthält nämlich das Token, und wer das kennt, kann den Bot Nachrichten schicken lassen. Eigentlich legt man das Token daher auf einen Server und lässt ausschließlich diesen mit dem API sprechen, niemals den Browser.

Diese grundsätzliche Vorsichtsmaßnahme hatte der Phisher ignoriert und uns so das API-Token für seinen Bot präsentiert. Per API hätten wir ihn jetzt mit Nachrichten überhäufen können, doch damit nicht genug: In der HTTP-Antwort verrät das Telegram-API weitere Details: Vorname, Nachname und Telegram-Benutzername des Benutzers, dem der Bot eine Nachricht geschickt hat. So erfuhren wir, dass der Phisher offenbar Daniel heißt und hatten auch seinen Benutzernamen. Mithilfe des Werkzeugs TgScanRobot, das öffentliche Telegram-Gruppen systematisch durchsucht, fanden wir heraus, in welchen unsympathischen Kreisen er sich herumgetrieben hatte: Über 20 Gesprächs- und Handelsplattformen für Spamming, Hacking-Werkzeuge und Handel mit geklauten Kreditkarten. In einer dieser Gruppen hatte sich Daniel auch mal zu Wort gemeldet und wurde zurechtgewiesen, weil er sich nicht an die Regeln der Gruppe gehalten hatte.

Jetzt wollten wir mehr über Daniel wissen – zumindest seine Herkunft interessierte uns. Ein Gruppenname mit chinesischen Schriftzeichen deutete schon mal grob auf Asien hin. Um es genauer einzukreisen, stellten wir dem Phisher eine Falle: Mit seinem Token schickten wir ihm über seinen Bot eine Nachricht, dass eben dieser Bot wegen illegaler Aktivitäten gesperrt sei, und er einen Link bei Telegram zur Freischaltung klicken müsse. Statt einem Link zur Telegram-Seite enthielt unsere Nachricht einen Link des Dienstes Grabify – eine Art URL-Kürzer, der dem Ersteller nebenbei zahlreiche Details zu allen Nutzern anzeigt, die ihn angeklickt haben. Ob ein Phisher selbst auf eine solche Phishing-Nachricht hereinfällt?

Nur sechs Stunden später ging er ins Netz und klickte auf den Link: So erfuhren wir, dass Daniel einen aktuellen Firefox nutzt, seinen PC in der Zeitzone „Asia/Shanghai GMT+8“ mit englischer Oberfläche betreibt und über ein Microsoft-VPN im Internet surft, das in den USA endet.



Weil die Phishing-Seite den Telegram-Benutzernamen des Phishers offenbarte, konnten wir die Liste der öffentlichen Telegram-Gruppen extrahieren, in denen er Mitglied war. Der Cyber-Kleinkriminelle war gut vernetzt in Spammer- und Kreditkartenbetrügerkreisen.

Gehostet bei Microsoft

Damit Daniel keinen weiteren Schaden anrichten konnte, musste die Phishing-Seite schnell vom Netz. Gehostet wurde sie in Microsofts Azure-Cloud, genauer gesagt handelte es sich um eine statische Seite, wie sie jeder Azure-Kunde anlegen kann. Ungeschickt von Microsoft ist es, dafür Subdomains von windows.net zu vergeben. Phisher könnten damit eine weitaus wirksamere Phishing-Kampagne für Microsofts eigene Kunden aufsetzen: Wer aufgefordert wird, sein Windows-, Office-365-, oder Outlook.com-Konto einzugeben, wird angesichts einer windows.net-Seite zunächst nicht stutzig. Für die perfekte Täuschung bräuchten die Angreifer aber einen besseren Webdesigner als Daniel, der das originale Microsoft-Design ansehnlich nachbauen kann.

Wir entschieden uns, Microsoft Azure über das Formular im Microsoft Security Response Center über die Phishing-Seite zu informieren (siehe ct.de/w9bq). Wenige Tage später war die Seite verschwunden und wir erhielten eine Bestätigung von Microsoft. Dass Strafverfolger über Microsoft eine Chance hätten, den wirklichen Namen von Daniel zu erfahren, ist unwahrscheinlich – wer sich in Foren über geklaute Kreditkarten austauscht, wird sich nicht mit eigenen

Daten bei Microsoft anmelden – die Suche dürfte schnell im Sande verlaufen.

Professionelle Kampagnen

Wie ein großer Fisch in der Szene wirkt Daniel nicht, mehr wie ein recht unerfahrener Kleinkrimineller, der sich mit dem Verkauf von Mailadresse-Kennwort-Kombinationen verdingen oder über gekaperte Postfächer Kennwörter für Webshops zurücksetzen und in fremdem Namen einkaufen wollte. Unklar ist, ob er die Seite selbst gebaut hat, die Expertise in einer der Telegram-Gruppen eingekauft oder dort einen Schnellkurs „Phishing für Einsteiger“ belegt hat.

Microsoft Security Response Center

ct.de/w9bq

Zur Verwaltung von Spam-Vorlagen, Adressen und Zeitplänen betreiben Spammer umfangreiche Webanwendungen. Per Kennwort geschützt sind die Oberflächen nicht immer.

Doch wer kauft Benutzernamen und Kennwörter, die Kleinkriminelle mühsam sammeln? Diesen Teil der Wertschöpfungskette – sofern man das so bezeichnen möchte – decken professionellere Gruppen ab. Ihre Spuren fand ein Leser zufällig bei einem Port-Scan: Auf Port 80 lag eine umfangreiche Webanwendung, die offenbar zum Verwalten von Spam-Kampagnen gedacht war. Die Beschriftungen deuteten auf Betreiber in Osteuropa hin. Da Datenschutz unter kriminellen Spammern ohnehin kein allzu hohes Gut ist, hing die gesamte Anwendung aber ohne Kennwortschutz im Netz. Auf der einen Seite enthielt sie Textdateien mit einigen hundert Megabyte Benutzername-Kennwort-Kombinationen. Außerdem einen ausgeklügelten Manager für Spam-Kampagnen. Der erinnerte vom Aufbau an professionelle Werkzeuge für Newsletter- und Social-Media-Kampagnen – nur eben für Spam. Online konnte man Textvorlagen, Empfänger und Absender kombinieren und so zeitgesteuerte Spam-Wellen planen. Die Vorlagen wurden offenbar von einer Template-Engine verarbeitet, die per Zufall die Platzhalter mit einem der angegebenen Inhalte füllte:

```
I {want|desire|choose|wish} to
{ask|demand|inquire}...
```

Auf diese Weise kann man auch ausgeklügelte Inhaltsfilter an die Grenzen bringen, weil es ausreichend unwahrscheinlich ist, dass zwei identische Mails oder wiedererkennbare Muster entstehen.

Verschickt wurden die Spam-Mails über die legitimen Mailserver von Mail-Hostern – authentifiziert mit einem der Accounts aus der langen Liste von erbeuteten Kennwörtern. In solchen Fällen haben auch Blacklist-Filter und Verfahren wie SPF oder DKIM kaum eine Chance, weil die Mails ja von vertrauenswürdigen Absenderservern verschickt wurden.

Um zumindest diesen einen Sumpf stückweise trockenzulegen, haben wir den Betreiber der Website haveibeenpwned.com auf die öffentlich zugängliche Kennwortsammlung der Spammer hingewiesen. Das Projekt sammelt gefundene Benutzernamen und Kennwörter als Hashes und Anwender können sich informieren, ob ihre Zugangsdaten schon im Internet kursieren.

Wo die Spam-Profis so große Kennwortsammlungen überhaupt finden, kann man nur mutmaßen – ein Teil kommt aus Datenlecks bei Betreibern, die in einschlägigen Foren verkauft werden, ein weiterer Teil sicher über dubiose Marktplätze von Zulieferern wie dem kleinkriminellen Phisher Daniel. (jam) c't

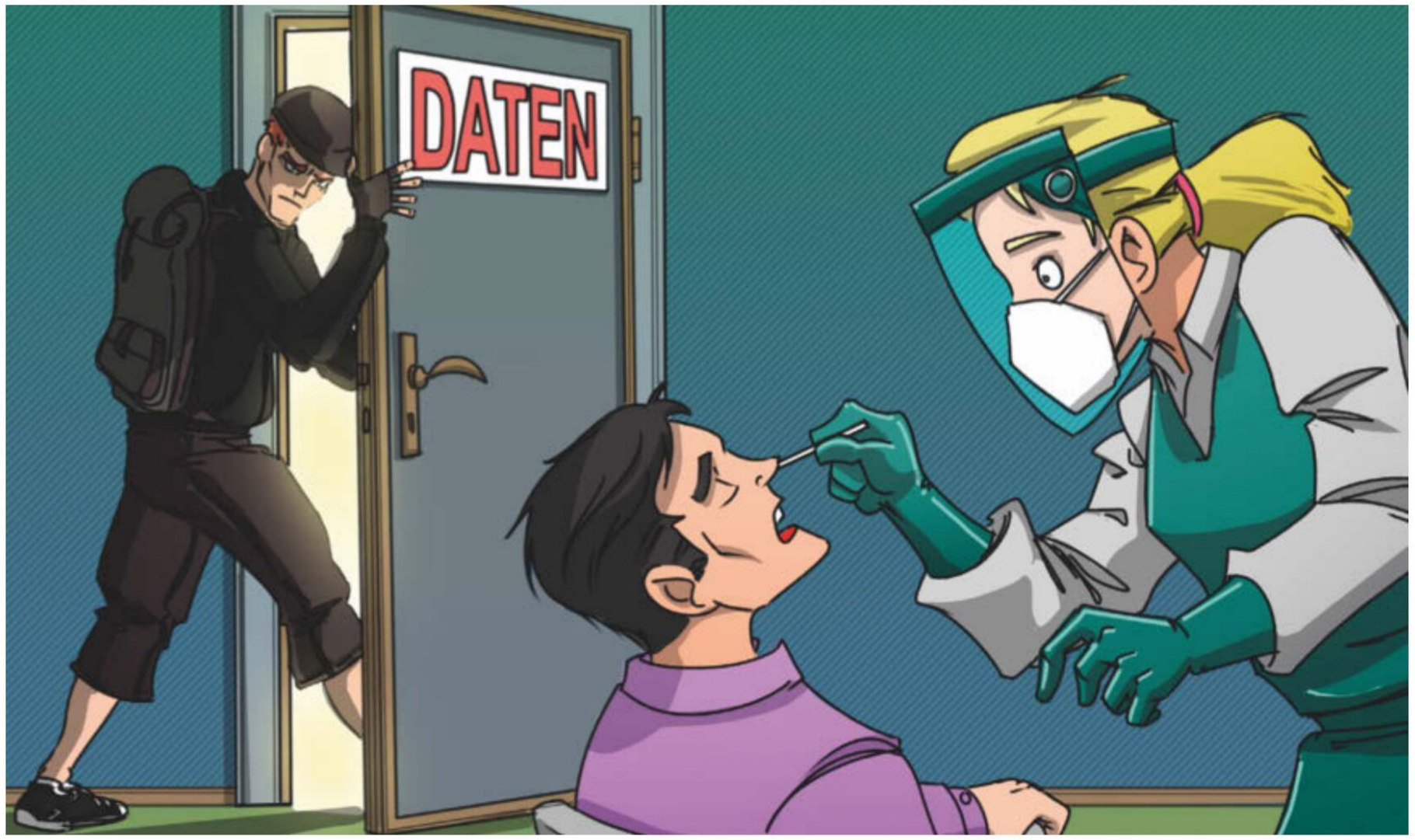


Bild: Thorsten Hübner

Datenlecks bei Test- und Impfterminen

Seitdem großflächig auf das Coronavirus getestet und in Arztpraxen geimpft wird, häufen sich die Datenlecks bei Test- und Impfterminvergabesoftware. Das Muster ist immer ähnlich – halbgare Software mit vermeidbaren Fehlern. Wie können Nutzer typische Probleme erkennen und Entwickler sie vermeiden?

Von **Jan Mahn**

Seit Anfang 2021 sammelt sich in den Postfächern der c't-Redaktion eine neue Kategorie von Zuschriften: „Datenschutzproblem bei Terminvergabe“ oder „Datenleck bei Impfportal?“ lauten häufige Betreffzeilen. Dahinter stecken Berichte von Lesern, die sich in einem Corona-Schnelltestzentrum oder bei einer Arztpraxis für einen Schnelltest oder eine spontane Impfung angemeldet haben: „Wenn ich das richtig sehe, könnte ich auf diesem Weg die Daten von Tausenden anderer Patienten einsehen.“

Für gewöhnlich reagieren wir auf solche Hinweise immer nach einem ähnlichen Schema: Zunächst versuchen wir, den Fehler nachzustellen und zu dokumentieren. Dann stellen wir weitere Analysen rund um den betreffenden Dienst an und stoßen nicht selten auf weitere Probleme: Alte Versionen von Serversoftware, Lücken in der Server-

konfiguration (etwa aktives Verzeichnis-Listing bei Apache-Servern, über das man eigentlich vertrauliche Ordner findet) oder Probleme mit HTTPS und dem Zertifikat sind typischer Beifang. Meist bestätigt sich die Beobachtung der Leser, manchmal fanden wir noch tiefergehende Probleme, weil wir schon ähnliche Systeme kannten und die Lücken mit Erfahrungen von anderer Software kombinieren konnten. Über all diese Beobachtungen informieren wir die Betreiber im Rahmen von Responsible Disclosure – solange Daten noch ungewollt öffentlich erreichbar sind, schreiben wir nicht über den Fall.

Allzu ähnliche Probleme

Sind die Probleme abgestellt, berichten wir oft ausführlich über die Fälle – vor allem, damit andere Entwickler und Administratoren nicht in ähnliche Fallen tappen. Zuletzt veröffentlichten wir Probleme mit der Online-Funktion für die Aldi-Schnelltests [1]. Seit Anfang 2021 haben wir uns aber immer häufiger dagegen entschieden, jeden Fall, der im Postfach landet, in einem Artikel vorzustellen. Schlagartig hatten bundesweit Arztpraxen und Apotheken, Betreiber von privaten oder kommunalen Testzentren die Aufgabe, Termine für Schnelltests und Impfungen (abseits der Impfzentren) zu vergeben, Ergebnisse zu kommunizieren oder online prüfbare Testzertifikate auszustellen. Und genauso schlagartig hatten Anbieter passende Softwarelösungen bereit, die Ärzte, Apotheken und Testzentren in ihre Homepage integrieren konnten. Die Anbieter treten teilweise nur regional begrenzt in Erscheinung, beliefern etwa mehrere Arztpraxen in einer Stadt mit ihrer Lösung. Obwohl viele kleine Hersteller völlig unabhängig voneinander eigene Software geschrieben haben, sehen sich die Fehler alle extrem ähnlich.

Wir prüfen zwar weiterhin eingehende Hinweise, stellen die Fehler nach und informieren die Betreiber mit einer ausführlichen Beschreibung des Problems, haben uns aber dazu entschieden, die typischen Probleme dieser Softwarelösungen in einem Artikel zu sammeln. Spannender und lehrreicher ist ohnehin die Anatomie typischer Sicherheits- und Datenschutzpannen. Eins lässt sich festhalten: Von der Optik darf man sich nicht täuschen lassen, sie sagt nichts über die Fähigkeiten der Entwickler aus. Offensichtliche Fehler fanden wir sowohl in Plattformen im Retro-Look als auch in schicken modernden Frontends.

1. Falsche Einstellung

Wer eine Terminvergabesoftware baut, die Impftermine oder Schnelltests verwaltet, kommt schnell mit Gesundheitsdaten von Nutzern in Kontakt. Für diese fordert die DSGVO einen besonderen Schutz. Wer an die Aufgabe mit der Einstellung herangeht, „mal eben“ eine Software zusammenzustricken, wird also zwangsläufig scheitern. Ein ausführliches Gespräch mit dem hauseigenen Datenschutzbeauftragten ist Pflicht, eine Beratung bei einem Anwalt für IT-Recht kann nicht schaden, wenn man in das Geschäftsfeld einsteigen will – und zwar bevor man die erste Zeile Code schreibt.

Selbstverständlich ist das nicht: Bei einem Telefonat mit dem Datenschutzbeauftragen eines Test-Anbieters mit akuten Problemen erfuhren wir, dass dieser erst einbezogen wurde, als die Software schon am Netz war und mehrere Tausend Nutzerdatensätze verarbeitet hatte. Bei einem anderen Anbieter mit offenen Hintertüren gelang es uns schlicht nicht, den Betreiber oder dessen Datenschutzbeauftragten überhaupt zu erreichen: Die Mail-Adressen aus Impressum und Datenschutzerklärungen existierten nicht, telefonisch waren weder der Datenschutzbeauftragte noch der Geschäftsführer zu erreichen. Schließlich informierten wir den Arzt, der den Dienst in seine Seite eingebettet hatte. Danach verschwand der Dienst erst vom Netz und erschien dann runderneuert und ohne die offensichtliche Schwachstelle wieder (mit neuem Datenschutzbeauftragtem).

Zu einem verantwortungsvollen Umgang mit Nutzerdaten gehört es auch, auf Überflüssiges zu verzichten: Neben den offensichtlichen Datenlecks fanden wir bei vielen Anbietern Google-Analytics-Cookies, Einbettungen (Grafiken und CSS) von Facebook und PayPal, Schriftarten, die von Google Fonts nachgeladen wurden, und JavaScript von externen CDN-Servern. Sowas passiert leicht, wenn die Entwickler gedankenlos auf ihren Standardbaukasten zurückgreifen.

Die eindringliche Warnung an alle Betreiber: Lassen Sie in diesem sensiblen Bereich die Finger von solchen Spielereien! Eine Test- oder Impfterminseite für deutsche Patienten gehört komplett auf Server in deutschen oder europäischen Rechenzentren. Tracking und externe Einbindungen haben hier nichts verloren – schon die Information, dass sich jemand überhaupt fürs Impfen interessiert, geht Dritte nichts an. Aus gutem Grund möchten sich viele Nutzer nicht tracken lassen, wenn sie Gesundheitsdaten in ein Formular eingeben sollen.

Name	Domain	Typ	Übertragungsgröße	Zeit
translate_24dp.png	www.gstatic.com	png	—	—
googlelogo_color_42x16dp.png	www.gstatic.com	png	—	—
translate_24dp.png	www.gstatic.com	png	—	—
analytics.js	www.google-analytics.com	js	—	—
translateelement.css	translate.googleapis.com	css	—	—
main_de.js	translate.googleapis.com	js	—	—
element_main.js	translate.googleapis.com	js	—	—
element.js	translate.google.com	js	—	—
sharethis.js	platform-api.sharethis.com	js	—	—
font-awesome.min.css	maxcdn.bootstrapcdn.com	css	—	—
1Ptxg8zYS_SKggPN4iEgvnHyvveLxVvaorCIPrcVIT9d0c8.woff	fonts.gstatic.com	woff	—	—
4iCs6KVjbNBYlgoKfw72nU6AFw.woff2	fonts.gstatic.com	woff2	—	—
css	fonts.googleapis.com	css	—	—
css	fonts.googleapis.com	css	—	—
portal-v2.html	c.sharethis.mgr.consensu.org	dokument	—	—
5fbea2d19a50de00123228ef.js	buttons-config.sharethis.com	js	—	—

Elemente von Google und anderen Drittanbietern sind nicht vertrauensfördernd, wenn eine Website sensible Gesundheitsdaten verarbeiten soll. Auf dieser Terminseite fanden wir reichlich solcher Inhalte, nicht alle wurden geschützt per HTTPS nachgeladen.

2. Berechenbare IDs

Der absolute Klassiker unter den Datenleckursachen ist die einfach zu erratende ID. Mit etwas Ausprobieren findet man so schnell fremde Daten. Diese Fälle sind immer ähnlich: Am Ende eines Terminvergabe- oder Anmeldeprozesses bekommt der Besucher eine PDF-Datei zum Ausdrucken – mit URLs wie

```
https://coronatest.example.org/user/↵
↳1234/print_result.pdf
```

Generiert werden diese Dateien meist dynamisch, ein Blick in die Metadaten verrät, dass häufig die Bibliothek FPDF dahintersteckt, ausgeführt von PHP-Code. Der Server schlägt beim Generieren dieser Datei den Nutzer mit der ID 1234 in seiner Datenbank nach, schreibt Namen, Geburtstag, Impftermin oder Testergebnis in PDF-Daten und liefert diese direkt an den Browser aus.

Wer als Entwickler in der URL mit natürlichen Zahlen arbeitet und keine weitere Sicherung einbaut, gefährdet leichtsinnig die Daten seiner Nutzer. Denn alle bereits vergebenen IDs sind extrem leicht zu erraten. Tippt ein Nutzer 1233 statt 1234 in die Adresszeile, sieht er die Daten seines Vorgängers im System und kann sich durch über 1000 weitere Datensätze hangeln. Manchmal wird diese ID auch als „Geheimnis“ benutzt. An anderer Stelle im System wird genau sie als Passwortersatz zusammen mit dem Namen in einem Formular verlangt, um sich am System anzumelden und dort den Termin zu stornieren oder zu ändern. Variationen des Fehlers fanden wir oft: mal leicht zu sehen, mal etwas versteckt in einem HTTP-Request im Hintergrund, mal in einen QR-Code eingebacken.

Wann immer Sie vor der Aufgabe stehen, ein ähnliches Szenario zu programmieren, nutzen Sie als ID eine ausreichend lange Folge von Zufallszeichen (nicht beschränkt auf Ziffern). Eine 32 Zeichen lange Kette aus zufälligen Buchstaben und Zahlen oder der Hash einer zufälligen Zeichenkette lassen sich in endlicher Zeit nicht erraten. Überlegen Sie als Entwickler auch, was Sie alles auf ein Negativtestzertifikat schreiben oder im QR-Code kodieren wollen. Wenn sich der Friseur, der nur die Gültigkeit prüfen soll, mit den Informationen auf dem ausgedruckten Testzertifikat am System als Nutzer anmelden kann, enthält das ganze System einen offensichtlichen Denkfehler.

3. Datenhalden

Wenn der Grund für die Datenspeicherung entfallen ist, dürfen die Daten auch nicht mehr auf dem Server liegen. Denn was restlos gelöscht wurde, kann bei Datenlecks auch nicht versehentlich ausgespuckt werden. Bei den problematischen Systemen, die wir uns angesehen haben, war diese Erkenntnis nicht immer angekommen. Datensätze, die wir durch andere Fehler fanden, reichten oft Wochen und Monate zurück (bis zum Start des Angebots).

Dabei kann es so einfach sein: Hat man zum Beispiel einen Termin für eine Impfung bei einem Arzt gebucht, ist der Datensatz ziemlich genau bis zu dem Zeitpunkt relevant, an dem die Impfung stattgefunden hat. Auf dem Server kann also ein Cronjob laufen, der alle halbe Stunde die erledigten Datensätze in der Datenbank löscht – und zwar mit einem `DELETE`-Befehl, nicht als Soft-Delete über eine Datenbankspalte wie `isDeleted`, die auf `true` gesetzt wird. Braucht man die Informationen über die Terminvergabe später noch für statistische Auswertungen, kann der Cronjob alle personenbezogenen Daten (etwa Name, Geburtstag, Anschrift) auch mit Zufallsstrings überschreiben oder anonymisierte Datensätze regelmäßig in eine andere Tabelle kopieren und die Originale löschen. Monatelang anlasslos auf dem Server herumliegen dürfen die personenbezogenen Daten keinesfalls. Derlei Sorglosigkeit im Umgang mit Daten ist schon vielen zum Verhängnis geworden.

4. Vermeintlich Geheimes

Ein Fall stieß aus der Masse durch besonders undurchdachtes Design heraus. Auf die Spur kamen wir dem Problem leicht mit einem Blick in die Entwicklerwerkzeuge des Browsers (alle Browser haben einen solchen Werkzeugkasten an Bord). Im Reiter „Netzwerk“ (oder „Network“)kann jeder Besucher einer Seite leicht nachvollziehen, welche Daten der Browser von welchen Servern geladen hat. Wie einfach das geht, war einem Anbieter vermutlich nicht bewusst – sein Server schickte Hunderte Datensätze von Nutzern als JSON-Objekt an den Browser, der dann per JavaScript nur das eigene Ergebnis herauspickte und in der Oberfläche darstellte. Unter allen Möglichkeiten, die Bereitstellung der Daten umzusetzen, ist das die schlechteste! Der Webserver darf zu keinem Zeitpunkt mehr Daten ausliefern, als der Benutzer sehen darf.

Programmierer sind gut beraten, sich selbst immer beim naheliegenden Gedanken „Wer soll da schon drauf kommen?“ auf die Finger zu klopfen. Gehen Sie am Ende der Entwicklungsarbeit alle Schritte der Software noch einmal durch und verfolgen Sie jeden HTTP-Aufruf in den Entwicklerwerkzeugen mit einer Frage im Hinterkopf: „Was könnte man hier Unangenehmes anstellen oder ausprobieren?“ Am besten lassen Sie am Ende einen Kollegen (oder noch besser einen professionellen Penetration-Tester) die Anwendung vor der Veröffentlichung noch einmal gründlich untersuchen.

Denken Sie daran, dass Ihre Anwendung unter besonderer Beobachtung steht. Unter den Impf- und Testwilligen sind sehr sicher auch IT-Experten, die sich Ihre Anwendung genauer ansehen werden. Nicht unbedingt, um sie anzugreifen, sondern im ersten Schritt, um sich ein Skript zu basteln, das automatisch auf freie Termine hinweist. Gerade Impftermine sind aktuell ein knappes Gut und ein Termin-Bot ein nützliches Feierabendprojekt. Bei GitHub sind in letzter Zeit zahlreiche solcher kleiner Projekte aufgetaucht (suchen Sie dort einfach nach „vaccination“).

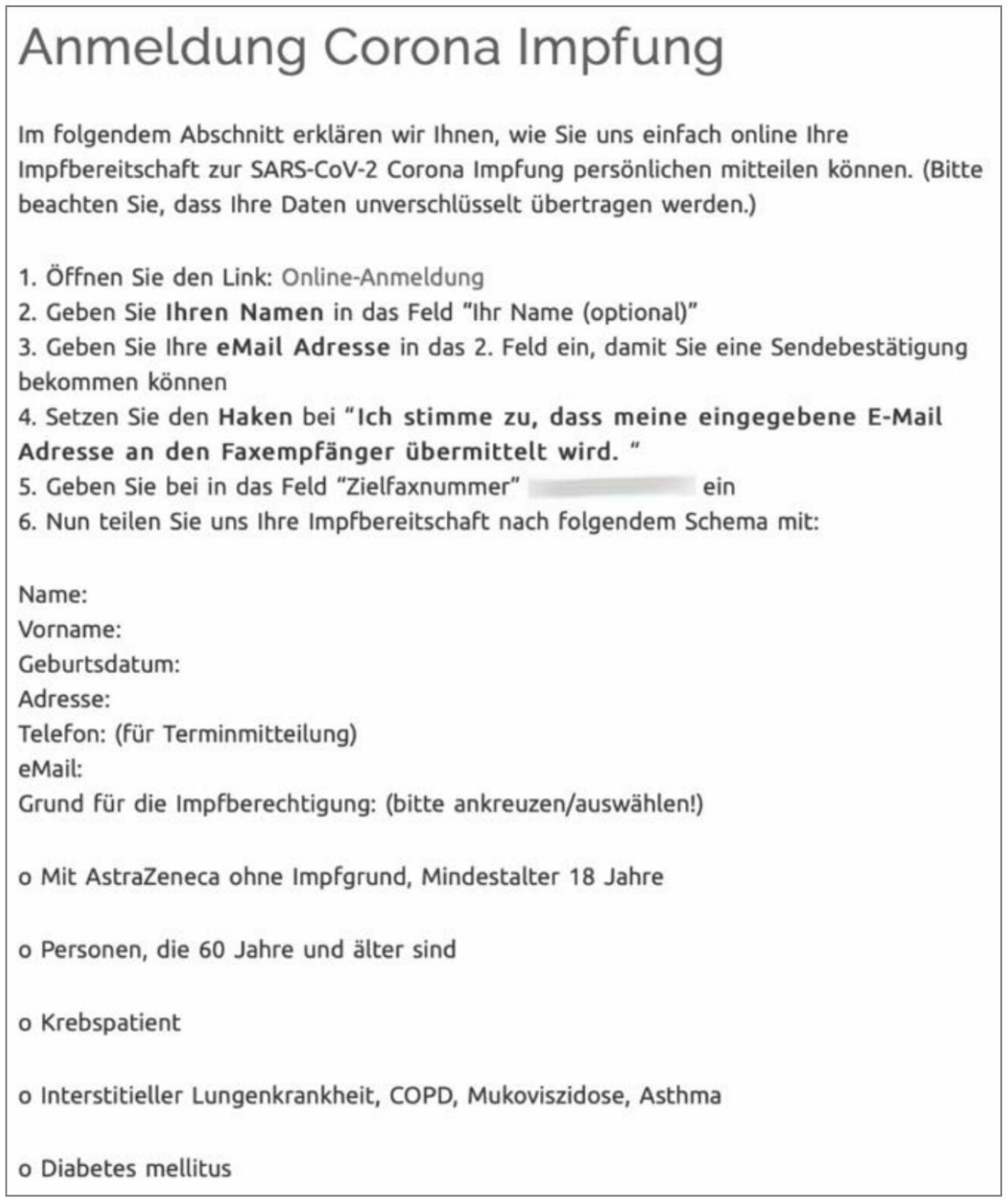
5. Unbedarfte Kreativität

Auf einen sehr kreativen, aber nicht weniger gruseligen Weg wies uns ein Leser aus Hessen hin. Die Praxis seines Hausarztes hatte für Terminvergaben eine Anleitung auf seiner Homepage veröffentlicht: Die Patienten wurden aufgefordert, dem Link zum Angebot eines Online-Faxdienstes zu folgen. Dieser bietet als Demonstration seines Dienstes ein kostenloses Fax über ein Textfeld an – ausdrücklich nur als Demo gekennzeichnet.

Die Patienten sollten dort neben Kontaktdaten auch intime Details zur Krankengeschichte ins Textfeld eintippen und die Terminanfrage als Testfax an die Nummer der Arztpraxis schicken. Versehen war diese einfallsreiche Schritt-für-Schritt-Anleitung mit dem Hinweis „Bitte beachten Sie, dass Ihre Daten unverschlüsselt übertragen werden“. Später heißt es noch, man könne selbstverständlich keine Haftung für die Daten im Internet übernehmen.

Was tun?

Ärzte und Apotheker, die eine Lösung für die Terminvergabe suchen, sollten sich die Software sehr gewissenhaft ansehen (oder einen unabhängigen IT-Experten zurate ziehen) – am besten in einem öffentlichen System in einer anderen Praxis. Probieren Sie (oder ein kompetenter Vertrauter) den ganzen



Anmeldung Corona Impfung

Im folgendem Abschnitt erklären wir Ihnen, wie Sie uns einfach online Ihre Impfbereitschaft zur SARS-CoV-2 Corona Impfung persönlichen mitteilen können. (Bitte beachten Sie, dass Ihre Daten unverschlüsselt übertragen werden.)

1. Öffnen Sie den Link: Online-Anmeldung
2. Geben Sie **Ihren Namen** in das Feld "Ihr Name (optional)"
3. Geben Sie Ihre **eMail Adresse** in das 2. Feld ein, damit Sie eine Sendebestätigung bekommen können
4. Setzen Sie den **Haken** bei "**Ich stimme zu, dass meine eingegebene E-Mail Adresse an den Faxempfänger übermittelt wird.** "
5. Geben Sie bei in das Feld "Zielfaxnummer" [redacted] ein
6. Nun teilen Sie uns Ihre Impfbereitschaft nach folgendem Schema mit:

Name:
Vorname:
Geburtsdatum:
Adresse:
Telefon: (für Terminmitteilung)
eMail:
Grund für die Impfberechtigung: (bitte ankreuzen/auswählen!)

o Mit AstraZeneca ohne Impfgrund, Mindestalter 18 Jahre

o Personen, die 60 Jahre und älter sind

o Krebspatient

o Interstitieller Lungenkrankheit, COPD, Mukoviszidose, Asthma

o Diabetes mellitus

Mit Abstand die kreativste Lösung, aber eine Datenschutzkatastrophe: Ein Arzt beschrieb in seiner Anleitung, die Patienten sollen einen kostenlosen Faxdienst im Internet nutzen und dort ihre Krankengeschichte hinterlassen.

Prozess einmal durch und achten Sie mindestens auf den häufigsten und einfachsten Fehler. Sobald eine verdächtige Zahl in einer URL auftaucht, lohnt ein kurzer Test mit benachbarten Zahlen. Wie ernst es ein Anbieter mit Datenschutz nimmt, sehen Fortgeschrittene mit einem Blick in die Entwicklerwerkzeuge ihres Browsers: Wer ganze Arbeit geleistet hat, kommt ohne Google- und Facebook-Tracking aus. Schauen Sie auch, welche Daten genau erfasst werden – je weniger, desto besser. Für eine Impfterminvergabe ist es zum Beispiel nicht erforderlich, den genauen Grund einer Priorisierung (schlimmstenfalls die ganze Krankengeschichte) im System einzutragen.

Nachdem Sie die Seite von außen gründlich untersucht haben, bleibt Ihnen als Patient nur Vertrauen. Wie sicher die Daten hinter den Kulissen aufbewahrt werden, finden Sie nicht so schnell heraus. Wenn ein Bestätigungslink oder ein QR-Code auch Wochen nach dem Test oder Termin funktionieren, ist das aber ein schlechtes Zeichen und es lohnt sich, den Anbieter zur Löschung der Daten aufzufordern. Hierfür können Sie sich auf die DSGVO berufen und unseren kostenlosen Musterbrief nutzen (siehe ct.de/w5ah). Sollten Sie offensichtliche Fehler finden, scheuen Sie sich nicht, den Datenschutzbeauftragten des Betreibers in der Datenschutzerklärung ausfindig zu machen und zu informieren. (jam) c't

Literatur

[1] Jan Mahn, **Bedenkliche Zertifikate**, Corona-Selbsttests von Aldi: Online-Zertifikate wertlos, c't 8/2021, S. 30

DSGVO-Musterbrief

ct.de/w5ah

secIT by Heise

Der Treffpunkt für Security-Anwender und -Anbieter

29. – 31.03.2022,
Hannover

SAVE THE DATE

Seien Sie dabei und profitieren Sie als Besucher von neuesten Trends, Produkten und Software-Lösungen in der IT-Security.

Das erwartet Sie:

- Große Ausstellung in zwei Hallen
- Spannende Fachvorträge auf drei Bühnen
- Praxisnahe Workshops mit Security-Experten
- Informative Expert-Talks der wichtigsten Security-Anbieter
- Austausch mit der Community vor Ort

Am **13. und 14. September 2022**
findet zusätzlich eine **digitale secIT** statt.

Veranstalter Heise Medien

Mehr zu den Highlights finden Sie hier:

sec-it.heise.de

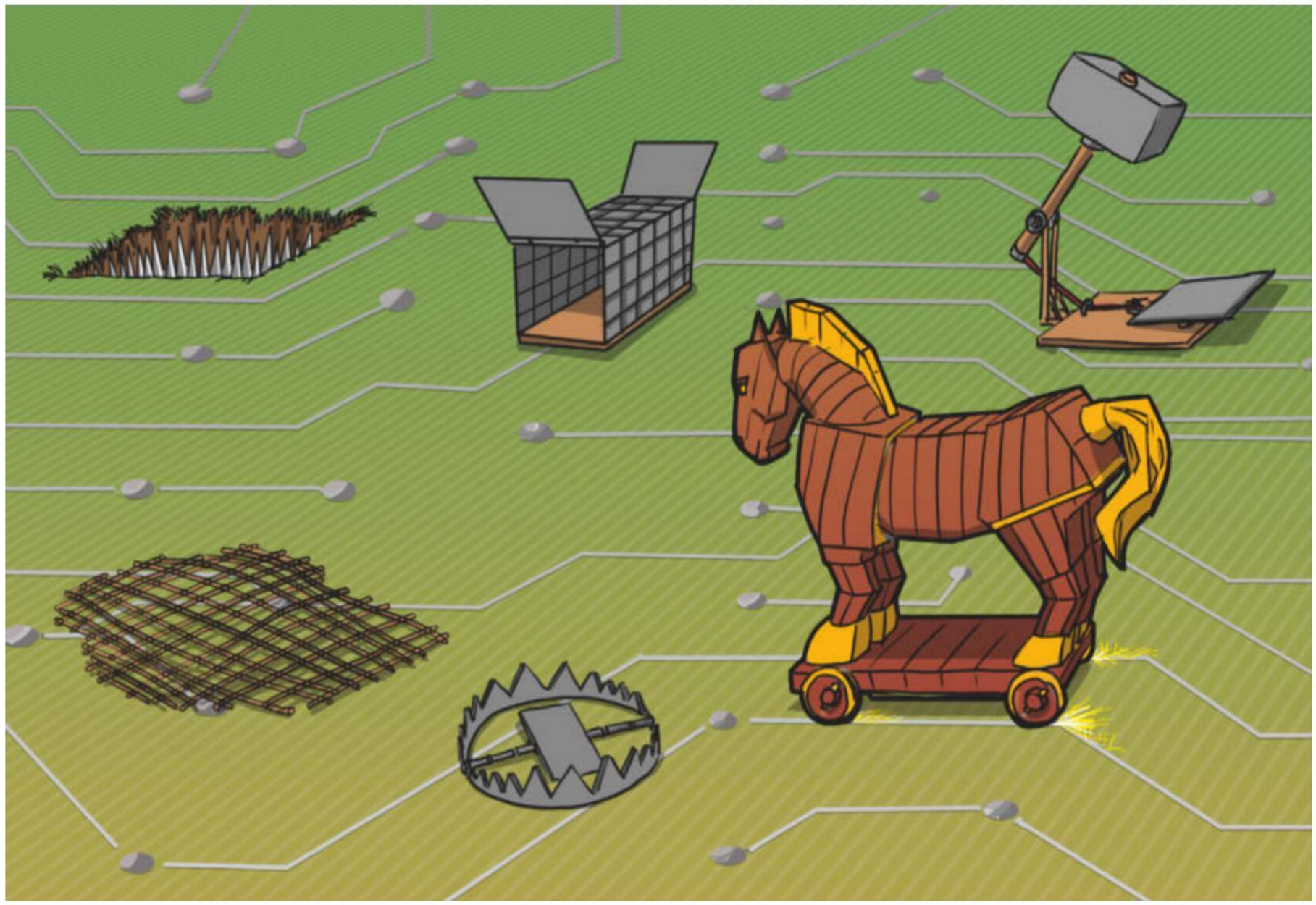


Bild: Thorsten Hübner

Ransomware-Attacke gezielt vereiteln

Erpressungstrojaner sind nach wie vor die Goldesel der Malware-Szene. Online-Kriminelle erpressen Millionensummen und erhöhen den Druck auf Opfer. Doch wenn man weiß, wie eine Attacke abläuft, kann man an den richtigen Stellen entgegenwirken.

Von **Dennis Schirrmacher**

Online-Kriminelle suchen gezielt das schwächste Glied in der Kette, um erfolgreich zuzuschlagen und in erster Linie Windows-Computer mit einem Verschlüsselungstrojaner zu infizieren. Wer den Ablauf solcher Ransomware-Attacken versteht, kann frühzeitig geeignete Schutzmaßnahmen treffen. Das neuseeländische Computer Emergency Response Team (CERT) zeigt in einem Schaubild (siehe S. 168) konkret, wie Angreifer vorgehen. Außerdem finden Sie in der Darstellung viele Tipps,

welche Schutzmechanismen in den verschiedenen Abschnitten einer Attacke effektiv helfen.

Von solchen Attacken sind zurzeit primär Unternehmen betroffen – hier sind schlicht höhere Lösegeldsummen erpressbar. Aber auch Privatpersonen sind bedroht und sollten die folgenden Angriffsszenarien und Schutzmechanismen ernst nehmen.

Der Weg ins Firmennetz …

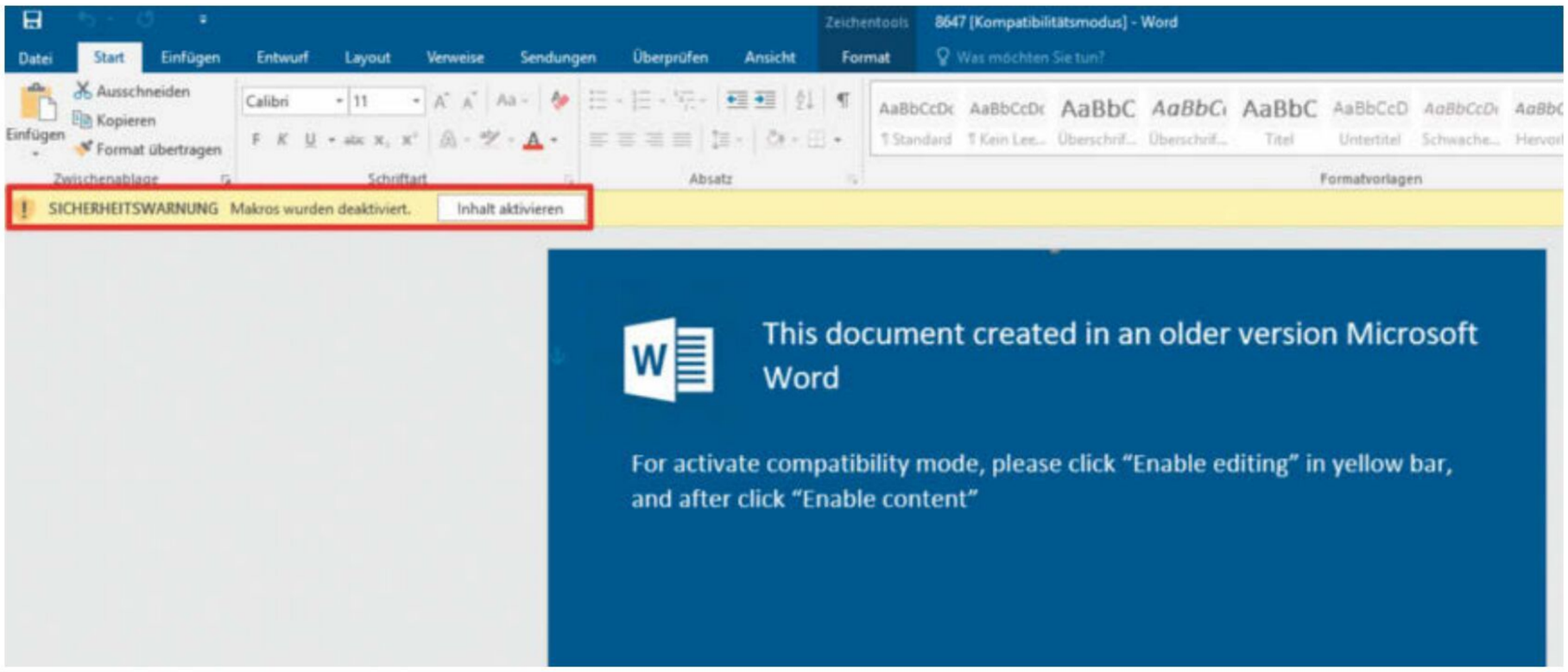
Am Anfang müssen Angreifer Zugriff auf Computer bekommen. Ein weit verbreiteter Weg sind Phishing-Mails, über die Kriminelle versuchen, Log-in-Daten abzugreifen – bevorzugt von Admins. Vorsicht: Die Zeiten von auf den ersten Blick erkennbaren Phishing-Mails mit Schreibfehlern und schrägen Formulierungen sind längst vorbei. Oft müssen sogar erfahrene Admins dreimal hingucken, um so eine Nachricht zu erkennen. Wenn die Angreifer ihre Hausaufgaben gemacht haben, kann so eine Mail etwa unter dem Deckmantel der angegriffenen Firma verschickt werden und zum Reset von internen Zugangsdaten auffordern – dabei muss man natürlich die alten Daten eingeben, die prompt beim Angreifer landen. Damit ausgestattet könnte er sich zum Beispiel bei öffentlich über das Internet erreichbaren Konfigurationsservern anmelden und so einen ersten Fuß ins Firmennetzwerk setzen.

Eine andere Methode ist das Erraten von Passwörtern, um Zugriff auf Server zu bekommen. Durch unzählige Datenleaks zirkulieren Milliarden Passwörter im Internet, die Angreifer in riesige Listen packen, um sie dann automatisiert durchzuprobieren.

Der derzeitige häufigste Verbreitungsweg von Verschlüsselungstrojanern sind Mails mit einem Office-Dokument im Anhang. Das bringt noch nicht den eigentlichen Schädling mit, sondern Makro-Elemente, die nach der Aktivierung Trojaner herunterladen. Dafür muss das Opfer mitspielen. Oft knüpfen solche Mails an bestehende Projekte in Firmen an und fordern Opfer plausibel dazu auf, das Dokument zu öffnen und die Makros zu aktivieren. Häufig steht in einer Word-Datei beispielsweise, dass man den Text erst richtig lesen kann, wenn Makros aktiviert sind. Fällt ein Opfer darauf rein, ist es zu spät und Schadcode gelangt auf einen Computer in der Firma, der oft die Tür ins Netzwerk öffnet. In einigen Fällen nutzen Angreifer auch gezielt Sicherheitslücken aus, etwa in PDF-Anwendungen oder in Windows, um in Netzwerke vorzudringen.

… und was man dagegen tun kann

Um Angreifern frühzeitig ein Bein zu stellen, müssen Sie Fake-Mails auf den ersten Blick entlarven und am besten gleich löschen. Im Zweifelsfall sollten Sie sich vor dem Öffnen an den Absender wenden, um sicherzustellen, dass dieser die Nachricht wirklich abgeschickt hat. Mitarbeiter sollten also ihre Sinne schärfen und nicht auf Social-Engineering-Attacken hereinfallen – regelmäßige Schulungen können dabei helfen. Außerdem sollten

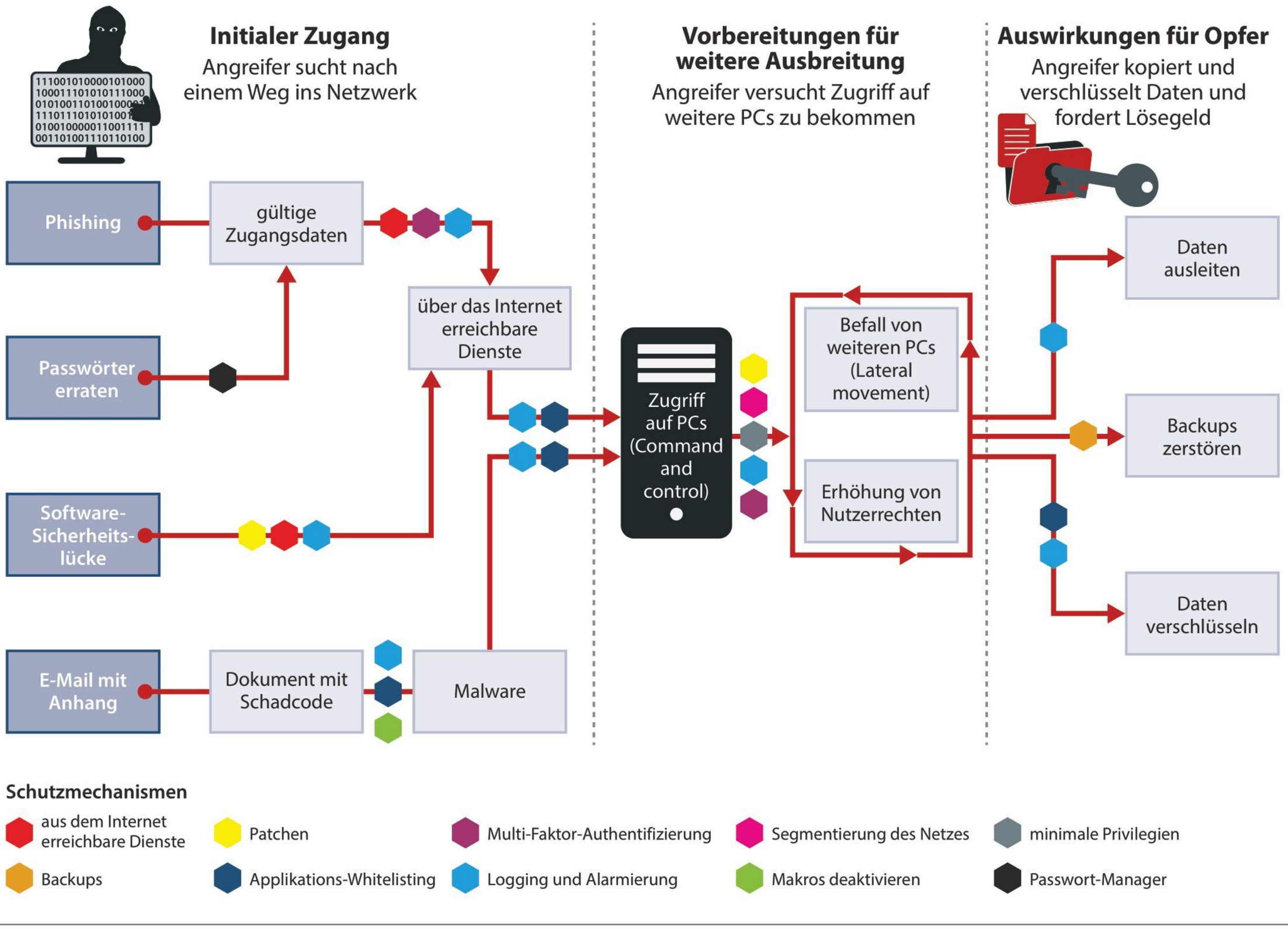


Am häufigsten versuchen Cyber-Erpresser ihre Verschlüsselungstrojaner immer noch über präparierte Word-Dokumente auf PCs zu schieben. Wer auf die Finte reinfällt und die Makros aktiviert, holt sich einen Trojaner auf den Computer, der Daten verschlüsselt.

So verläuft eine Ransomware-Attacke

In dieser Grafik vom CERT aus Neuseeland sieht man, wie Online-Kriminelle bei einer typischen Ransomware-Attacke auf Unternehmen vorgehen und was Sie dagegen tun können. Während der verschiedenen Stadien einer Attacke gibt es jeweils andere Sicherheitskonzepte, um Systeme effektiv zu schützen. Admins sollten das Schaubild genaustens studieren und auf die IT-Infrastruktur ihres Unternehmens anwenden. Im Anschluss sollte klar werden, welche Schwächen das eigene Sicherheitskonzept hat und mit welchen Maßnahmen Sie dagegen steuern können.

Quelle: CERT NZ



Admins sicherstellen, dass sie Office-Makros über Windows-Gruppenrichtlinien global deaktivieren (siehe ct.de/w8d4).

Um weitere Einfallstore zu schließen, sollten Admins Systeme stets auf dem aktuellen Stand halten und Sicherheitsupdates installieren. Extrem wichtig ist auch das lückenlose Protokollieren („Logging“) von Datenverkehr im Netzwerk, damit Admins frühzeitig einen Angriff mitbekommen und untersuchen können.

Außerdem sollten starke Passwörter zum Einsatz kommen, damit Angreifer Kennwörter nicht erraten können. Auf der Website haveibeenpwned.com können Sie prüfen, ob benutzte Passwörter bereits in Datenleaks öffentlich verfügbar und somit verbrannt sind. Ist das der Fall, sollten Sie das Kennwort umgehend ändern. Das regelmäßige Ändern von Passwörtern kann hingegen kontraproduktiv sein, da man in solchen Fällen dazu neigt, Kennwörter nur leicht zu variieren. Das könnten Angreifer leicht durchschauen. Um nicht den Überblick zu verlieren, sollten Sie einen Passwortmanager benutzen.

Darüber hinaus empfiehlt es sich, im Unternehmensumfeld Multi-Faktor-Authentifizierung (MFA) einzuführen. Durch einen zweiten Faktor können Angreifer selbst dann nicht eindringen, wenn sie an die Kennwörter gelangen. Außerdem sollten Admins nur Dienste und Server über das Internet erreichbar machen, bei denen das zwingend notwendig ist. Die Verbindung sollte in solchen Fällen über VPN und MFA abgesichert sein.

Was aber, wenn sich trotz aller Sicherheitsmaßnahmen Schadcode im System einnistet? Präventiv sollten Admins für solche Fälle sogenanntes „Application Whitelisting“ einrichten. Dann dürfen auf dem System nur Anwendungen starten, die in einer Liste eingetragen sind. Damit ist jede dem System unbekannte Trojaner-Datei kaltgestellt. Das ist eine schlagkräftige Methode, erfordert aber einiges an Handarbeit und regelmäßige Kontrolle für einen reibungslosen Arbeitsalltag.

Angreifer machen sich breit

Ist ein Angreifer im System und kann eigenen Code ausführen, tut er in der Regel alles dafür, um sich festzusetzen und sich noch weiter auszubreiten. Dafür richtet er eine Verbindung nach außen zu seinen „Command-and-Control-Servern“ (C&C) ein. Von dort steuert der Hacker aus der Ferne die Schadsoftware, spioniert den Rechner aus oder lädt weitere Trojaner-Module und Hintertüren nach.

Bei solch einem Szenario zählt jede Sekunde, weshalb ein effektiv konfiguriertes Protokollsystem Gold wert ist: Wenn ein PC rechtzeitig Alarm schlägt, sobald er sich mit verdächtigen Servern verbindet, kann der Admin häufig gerade noch rechtzeitig eingreifen.

Damit sich Angreifer nicht ungehindert im Netzwerk ausbreiten und weitere Computer infizieren können („Lateral movement“), sollten Dienste mit möglichst niedrigen Rechten arbeiten. Kapert ein Angreifer einen Dienst, kann er dann weniger anstellen als mit Admin-Rechten.

Ist eine Ausbreitung im Netzwerk nicht mehr abwendbar, sollten Admins via Logging das Ausmaß des Befalls einschätzen und das Netz zügig segmentieren. So können sie beispielsweise sicherstellen, dass Produktivsysteme nur in sauberen Netzen laufen und infizierte PCs in anderen Abschnitten isoliert sind.

Das Schadenswerk beginnt

Wenn ein Angreifer freie Bahn hat, beginnt ein Erpressungstrojaner damit, Daten zu verschlüsseln. Gängig ist außerdem inzwischen, dass die Einbrecher interne Daten kopieren und Opfern mit einer Veröffentlichung drohen – als weiteres Druckmittel, um Lösegeld einzufordern. Auch in solch einem Fall kann das Logging des Netzwerkverkehrs vor schlimmeren Schäden bewahren, etwa wenn auffällig viele Dateioperationen im Zuge der Verschlüsselung erfolgen oder Daten nach außen fließen. Admins müssen dann Gegenmaßnahmen ergreifen und etwa Ports schließen und Ransomware-Proesse stoppen.

In der Regel zerstören Verschlüsselungstrojaner auch Backups auf externen Festplatten oder auf im Netz verbundenen Rechnern und somit die letzte Rettung vor dem Super-GAU. Deswegen sollte man sicherstellen, dass Backups auf vom Netzwerk abgetrennten Servern liegen. Im Privatbereich hat es sich bewährt, Sicherungskopien auf externen Datenträgern zu speichern, die nicht dauerhaft am Computer angeschlossen sind.

Fazit

Ein effizienter Schutz vor Ransomware ist immer das Zusammenspiel von mehreren Sicherheitsmechanismen an verschiedenen Stellen. Als zentrale Elemente haben sich Backups, Logging und Application Whitelisting bewährt. Doch auch der Schutz vor Social-Engineering-Attacken spielt eine große Rolle, um Angreifer erst gar nicht ins Netz zu lassen. In einigen Fällen hilft es auch, die von Angreifern verschlüsselten Daten aufzubewahren und auf ein kostenloses Entschlüsselungstool zu hoffen. Es ist schon öfters vorgekommen, dass Sicherheitsforscher auf Fehler in Trojanern gestoßen sind und passende Entschlüsselungs-Software veröffentlicht haben. (des) c't

Weitere Sicherheitstipps, Windows-Gruppenrichtlinien (Makros)

ct.de/w8d4

IMPRESSUM

Redaktion

Postfach 61 04 07, 30604 Hannover
Karl-Wiechert-Allee 10, 30625 Hannover
Telefon: 05 11/53 52-300
Telefax: 05 11/53 52-417
Internet: www.heise.de

Leserbriefe und Fragen zum Heft:
sonderhefte@heise-online.de
Die E-Mail-Adressen der Redakteure haben die Form xx@heise.de oder xxx@heise.de. Setzen Sie statt „xx“ oder „xxx“ bitte das Redakteurskürzel ein. Die Kürzel finden Sie am Ende der Artikel und hier im Impressum.

Chefredakteur: Jobst-H. Kehrhahn (keh)
(verantwortlich für den Textteil)

Konzeption: Christian Wölbert (cwo)

Koordination: Ann-Sophie Eikermann (ase), Angela Meyer (anm)

Redaktion: Ernst Ahlers (ea), Jo Bager (jo), Holger Bleich (hob), Niklas Dierking (ndi), Mirko Dölle (mid), Wilhelm Drehling (wid), Ronald Eikenberg (rei), Alexander Königstein (ako), Jan Mahn (jam), Angela Meyer (anm), Markus Montz (mon), Dennis Schirrmacher (des), Peter Schmitz (psz), Peter Siering (ps), Keywan Tonekaboni (ktn), Sylvester Tremmel (syt), Andrea Trinkwalder (atr), Axel Vahldiek (axv), Christof Windeck (ciw), Christian Wölbert (cwo), Dušan Živadinović (dz)

Mitarbeiter: Verena Ehrl, Tomas Jakobs, Merlin Schumacher, Holger Zuleger

DTP-Produktion: Lara Bögner, Beatrix Dedek, Madlen Grunert, Lisa Hemmerling, Cathrin Capell, Paula Krause, Kirsten Last, Martina Lübke, Steffi Martens, Marei Stade, Matthias Timm, Ricardo Ulbricht

Fotografie: Andreas Wodrich, Melissa Ramson

Produktion: Christine Kreye (Ltg.), Melanie Becker, Kevin Harte, Martin Kreft, Pascal Wissner

Illustration: Sven Hauth, Schülp; Thorsten Hübner, Berlin; Andreas Martini, Wettin

Titel: Steffi Martens, www.flaticon.com, www.freepik.com, www.stock.adobe.com

Verlag

Heise Medien GmbH & Co. KG
Postfach 61 04 07, 30604 Hannover
Karl-Wiechert-Allee 10, 30625 Hannover
Telefon: 05 11/53 52-0
Telefax: 05 11/53 52-129
Internet: www.heise.de

Herausgeber: Christian Heise, Ansgar Heise, Christian Persson

Geschäftsführung: Ansgar Heise, Beate Gerold

Mitglieder der Geschäftsleitung: Jörg Mühle, Falko Ossmann

Anzeigenleitung: Michael Hanke (-167)
(verantwortlich für den Anzeigenteil),
www.heise.de/mediadaten/ct

Anzeigenverkauf: Verlagsbüro ID GmbH & Co. KG,
Tel.: 05 11/61 65 95-0, www.verlagsbuero-id.de

Leiter Vertrieb und Marketing: André Lux (-299)

Service Sonderdrucke: Julia Conrades (-156)

Druck: Firmengruppe APPL Druck GmbH & Co. KG,
Senefelder Str. 3–11, 86650 Wemding

Vertrieb Einzelverkauf:
DMV DER MEDIENVERTRIEB GmbH & Co. KG
Meßberg 1
20086 Hamburg
Tel.: 040/3019 1800, Fax: 040/3019 145 1815
E-Mail: info@dermedienvertrieb.de
Internet: dermedienvertrieb.de

Einzelpreis: € 14,90; Schweiz CHF 27.90;
Österreich € 16,40; Luxemburg € 17,10

Erstverkaufstag: 23.11.2021

Eine Haftung für die Richtigkeit der Veröffentlichungen kann trotz sorgfältiger Prüfung durch die Redaktion vom Herausgeber nicht übernommen werden. Kein Teil dieser Publikation darf ohne ausdrückliche schriftliche Genehmigung des Verlags in irgendeiner Form reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfaltigt oder verbreitet werden. Die Nutzung der Programme, Schaltpläne und gedruckten Schaltungen ist nur zum Zweck der Fortbildung und zum persönlichen Gebrauch des Lesers gestattet.

Für unverlangt eingesandte Manuskripte kann keine Haftung übernommen werden. Mit Übergabe der Manuskripte und Bilder an die Redaktion erteilt der Verfasser dem Verlag das Exklusivrecht zur Veröffentlichung. Honorierte Arbeiten gehen in das Verfügungsrecht des Verlages über. Sämtliche Veröffentlichungen erfolgen ohne Berücksichtigung eines eventuellen Patentschutzes.

Warennamen werden ohne Gewährleistung einer freien Verwendung benutzt.

Hergestellt und produziert mit Xpublisher: www.xpublisher.com

Printed in Germany.

Alle Rechte vorbehalten.

© Copyright 2021 by
Heise Medien GmbH & Co. KG

INSERENTENVERZEICHNIS

Cordaware GmbH, Pfaffenhofen 21
DeinData GmbH, Löbnitz 15
FH OÖ Studienbetriebs GmbH, A-Wels 13
netfiles GmbH, Burghausen 172
pCloud AG, CH-Baar 32, 33
PricewaterhouseCoopers GmbH, Düsseldorf 2
retarus GmbH, München 11
secunet Security Networks AG, Essen 9
SySS GmbH, Tübingen 17

WIR MACHEN KEINE WERBUNG. WIR MACHEN EUCH EIN ANGEBOT.

c't

ct.de/angebot

Jetzt gleich bestellen:

ct.de/angebot

+49 541/80 009 120

leserservice@heise.de

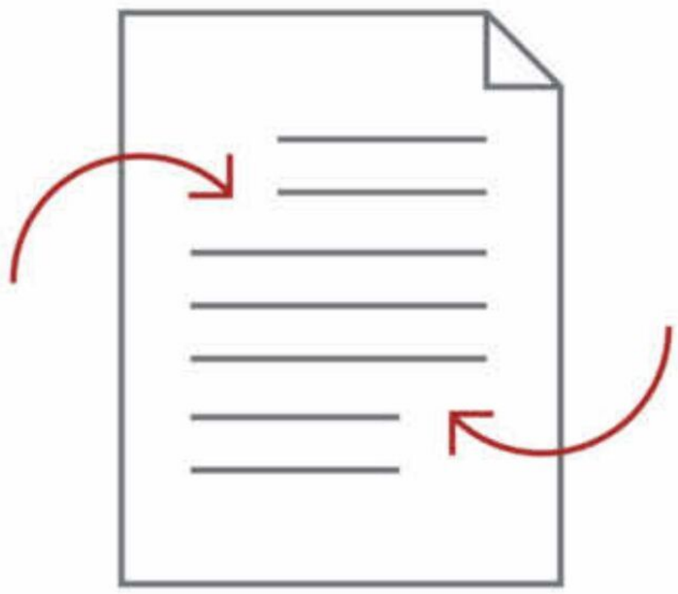
ICH KAUF MIR DIE c't NICHT. ICH ABONNIER SIE.

Ich möchte c't 3 Monate lang mit 35 % Neukunden-Rabatt testen.
Ich lese 6 Ausgaben als Heft oder digital in der App, als PDF oder direkt im Browser.

Als Willkommensgeschenk erhalte ich eine Prämie nach Wahl, z. B. einen RC-Quadrocopter.

Jetzt neu mit
Videokonferenz
Funktion!

NETFILES



netfiles

Sichere Cloud-Lösungen für Datenaustausch und Collaboration

Einfach

Der netfiles Datenraum ist besonders einfach zu bedienen, bietet umfangreiche Funktionalität und steht Ihnen sofort, ohne Installation von Software oder Plugins zur Verfügung. Ein Webbrowser genügt.

Sicher

Im netfiles Datenraum sind Ihre Daten sowohl bei der Speicherung als auch Übertragung durch 256-bit Verschlüsselung sicher und Compliance-gerecht geschützt.

Bewährt

netfiles gibt es seit mehr als 20 Jahren. Profitieren auch Sie von unserer langjährigen Erfahrung und dem zuverlässigen Betrieb. Wir sind ein deutsches Unternehmen und hosten ausschließlich in Deutschland.

www.netfiles.com

Testen Sie jetzt netfiles 14 Tage kostenlos
oder vereinbaren Sie einen Termin für eine Online-Präsentation.

netfiles GmbH · Marktler Str. 2b · 84489 Burghausen · +49 8677 915 96-12 · vertrieb@netfiles.de