Editorial

Liebe Leserinnen und Leser,

die schlechte Nachricht zuerst: Die Zahl der Cybercrime-Fälle steigt schnell. Exakt 100.514 Online-Straftaten wie Identitätsdiebstahl und Malware-Angriffe registrierte die deutsche Polizei 2019, rund 15 Prozent mehr als im Vorjahr. Und das sind nur die offiziell erfassten Fälle. Die Dunkelziffer liegt vermutlich um ein Vielfaches höher.

Gleichzeitig werden die Angriffe perfider. Die Banden hinter Malware wie Emotet, Sodinokibi und Co. haben sich darauf spezialisiert, Daten zu verschlüsseln, um Lösegelder zu erpressen. Die Schadenssumme bei betroffenen Firmen geht dann schnell in die Millionen. Werden Krankenhäuser angegriffen, geraten sogar Menschenleben in Gefahr.

Online-Kriminelle zielen aber nicht nur auf große Organisationen. Bei der c't-Redaktion melden sich regelmäßig Personen, deren Bankdaten ausgespäht und missbraucht wurden. Private Mail-Accounts werden für den Versand von Phishingmails zweckentfremdet, Rechner als Bots eingesetzt.

Doch es gibt auch eine gute Nachricht: Alles, was Sie brauchen, um sich vor Hackern und Viren zu schützen, halten Sie bereits in Ihren Händen. Unser Sonderheft c't Security erklärt, wie Sie Ihre Geräte, Anwendungen und Accounts absichern und worauf Sie im Alltag achten müssen. In unseren Checklisten haben wir die nötigen Schritte übersichtlich und verständlich aufbereitet (S. 6).

In den weiteren Schwerpunkten steigen wir tiefer in das Thema IT-Sicherheit ein. Wir schauen Emotet, dem „König der Malware“, über die Schulter (S. 50) und erklären, wie Sie Backups vor ihm schützen (S. 76). Wir helfen, das Passwortchaos zu bändigen (S. 100) und auch unterwegs auf der sicheren Seite zu bleiben (S. 148). Außerdem werfen wir einen Blick in den Hardware-Werkzeugkasten von Hackern - damit Sie wissen, worauf Sie im Extremfall gefasst sein müssen (S. 172).

Christian Wölbert

Inhalt

SICHERHEITS-CHECKLISTEN

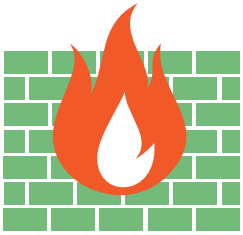
Schutzvorkehrungen gegen Hackerangriffe und Viren erfordern kein Informatikstudium. Die meisten Geräte, Anwendungen und Accounts lassen sich mit ein paar Handgriffen vernünftig absichern. Unsere Sicherheits-Checklisten erklären Schritt für Schritt, wie es geht.

SCHUTZ VOR EMOTET & CO.

Der Begriff Emotet steht beispielhaft für eine hinterhältige Angriffsmethode: Online-Gangster überlisten ihre Opfer mit gefälschten Mails, verschlüsseln Daten und verlangen Lösegeld. Wir erklären, wie Sie sich schützen.

SICHERES BACKUP EINRICHTEN

Backups waren schon immer wichtig, doch in Zeiten von Erpressungstrojanern sind sie wichtiger denn je. Wir erklären, worauf Sie bei Ihrer Datensicherung achten müssen, um wirklich ruhig schlafen zu können.



PASSWORTCHAOS BÄNDIGEN

Gute Passwortmanager schaffen die Quadratur des Kreises: Sie verbinden Sicherheit mit Bequemlichkeit. Wir schauen den Programmen unter die Haube. Außerdem testen wir FIDO2-Sticks, die Passwörter ergänzen oder ersetzen können.

UNTERWEGS SICHER SURFEN

Viele öffentliche WLANs sind gratis nutzbar, bieten Angreifern aber auch die Möglichkeit, sensible Daten abzugreifen. Wir zeigen, worauf Sie im Alltag achten müssen und wie Sie die VPN-Technik Wireguard einsetzen.

HACKING-GADGETS VERSTEHEN

Online kann jeder spezielle Hardware für Hackerangriffe und Spionage kaufen. Wir haben die Hacking-Gadgets ausprobiert, damit Sie wissen, was im Extremfall auf Sie zukommt.

ZUM HEFT

Security-Fachchinesisch erklärt

Beim Buzzword-Bingo der Security-Experten geraten oft sogar gestandene ITler ins Schleudern. Dabei verbergen sich hinter Begriffen wie ReCoBS und Red Teaming so interessante Konzepte, dass es sich lohnt, sie zu kennen.

Von **Stefan Strobel**

Kommen Sie manchmal auch nicht mehr mit, wenn Security-Experten und solche, die sich als welche ausgeben, so richtig loslegen? Keine Sorge – auch wenn es manchmal so klingt, handelt es sich nicht um Raketentechnik. Mit etwas Hintergrundwissen versteht man schnell, um was es geht und ob das Gegenüber wirklich Ahnung hat oder nur angeben will. Dieser erste Teil unseres Security-Ratgebers erklärt nicht nur die wichtigsten Begriffe und deren Anwendungsbereiche, er ordnet

auch den Nutzen ein und ermöglicht Ihnen damit eine bessere Entscheidung, welche Ansätze wirklich zu mehr Sicherheit führen.

Next Gen Malware Protection

Bereits seit einigen Jahren spricht man in der IT-Sicherheit viel über gezielte Angriffe von professionellen Hackern: **Advanced Persistent Threat (APT)**. Gemeint sind damit sowohl Angreifer als auch ihre Werkzeuge und Aktivitäten, die sich ihr Opfer bewusst auswählen und bei Bedarf auch über einen längeren Zeitraum versuchen, Schutzmaßnahmen zu umgehen, um ihr Ziel zu erreichen. In der Regel wird dabei individuell und mit hohem Aufwand entwickelte Malware verwendet. Hinter APTs stehen oft nationalstaatlich organisierte Hacker oder kriminelle Organisationen, denen viel Geld und Zeit für ihre Angriffe zur Verfügung stehen.

Klassische Schutzmaßnahmen wie signaturbasierter Virenschutz sind gegen APTs nahezu wirkungslos und daher haben in den letzten Jahren zahlreiche Hersteller neue Ansätze und Produkte entwickelt. Oft fallen dabei die Buzzwords **Next Generation Malware Protection** oder **Next Generation Antivirus (NG AV)**. Die Mechanismen, die sich hinter diesen Schlagwörtern verbergen, sind je nach Hersteller und Produkt unterschiedlich und führen wiederum zu neuen Buzzwords. Doch hinter den marktschreierischen Bezeichnungen stehen oftmals durchaus vielversprechende Sicherheitskonzepte zum Schutz vor APT-Gruppen.

Abgeschottet im Sandkasten

Sandbox-Analyse und **Sandboxing** sind eigentlich zwei verschiedene Dinge. Eine Sandbox ist zunächst ein Bereich innerhalb des Betriebssystems, der Programme oder Prozesse isoliert und vom restlichen System abschottet, um zu verhindern, dass Schadcode das System manipuliert. Bei der Sandbox-Analyse eventuell aus der Mailbox entfernen, bevor der Schaden eintritt. Doch bei gezielten professionellen Angriffen verzögern Täter inzwischen die Ausführung von Schadfunktionen oder sie versuchen zu erkennen, ob ihre Malware in einer Sandbox läuft. In diesem Fall bleiben die Schadfunktionen inaktiv, damit eine Sicherheitslösung den Angriff nicht erkennt.

Die Sandbox-Analyse ist somit eine Technik, die vor allem in der Erkennung von breit gestreuten Angriffen Vorteile gegenüber klassischem Virenschutz verspricht. Sie richtet sich an Unternehmen, die ihre allgemeine Netzwerksicherheit steigern wollen. Der Ansatz ist aber kein Allheilmittel, da sich Schadcode vor einer Sandbox-Analyse verstecken kann. Die Isolation von potenziell gefährlichen Aktionen, so wie es Sandboxen im klassischen Sinne auf Endgeräten tun, ist dagegen eine präventiv sehr wirksame Idee, die auch hinter **ReCoBS** steckt.

Sicherer surfen

ReCoBS steht für **Remote Controlled Browsing System**. Manche Hersteller nennen diese Technik auch **Threat Isolation**. Dabei surfen Mitarbeiter im Unternehmen nicht mehr mit einem lokalen Browser im Internet, sondern sie nutzen eine Fernsteuerungstechnik, um Browser, die auf einem speziell abgesicherten und isolierten System installiert sind, zu steuern. Das kann im primitivsten Fall eine RDP- oder VNC-Verbindung zu einem dedizierten abgesicherten Server sein oder eine spezielle Software-Lösung, die wiederum Sandboxing auf einem speziellen Gateway nutzt, um dort Browser anzubieten.

Moderne Interpretationen von ReCoBS stellen sich für den Anwender wie Web-Proxies dar, die jedoch genau genommen keine einfachen Proxies sind, sondern jede angeforderte Website selbst über eine Engine wie Chromium rendern und das Ergebnisbild der Seite dem Anwender als Bild in HTML5 verpackt zustellen. Als Anwender bemerkt man den Unterschied in der Praxis so gut wie nicht, da man

Pragmatischer Schutz vor Emotet & Co.

Hightech-Trojaner wie Emotet können jeden treffen, folglich sollte sich auch jeder davor schützen. Die gute Nachricht ist, dass Sie mit einigen pragmatischen Schutzmaßnahmen das Infektionsrisiko erheblich reduzieren können – ganz gleich, ob es um Ihren Rechner zu Hause oder ein ganzes Unternehmensnetz geht.

Von **Ronald Eikenberg, Peter Siering und Axel Vahldiek**

Ein solider Grundschutz bildet das Fundament für den Schutzwall, der Schädlinge von Ihrem System fernhält und im Falle einer Infektion die Schäden klein hält. Der Grundschutz besteht aus Updates, Backups und last, but not least, Virenschutz. Das alles ist nicht teuer und mit wenigen Handgriffen erledigt. Diese haben wir im Kasten „Kleines Schutz-Einmaleins“ auf Seite 66 für Sie zusammengefasst. Um aktuelle Super-Trojaner à la Emotet effektiv abzuwehren, sollten Sie Ihren Schutzwall noch etwas ausbauen. Und zwar mit gezielten Maßnahmen, die sich gegen die Angriffsmaschen der Schädlinge richten.

Schutz hoch zehn

Emotet hat es ausschließlich auf Windows-Nutzer abgesehen und hat eine Vorliebe für Windows 7. Der

kürzeste Weg, sich einer Infektion zu entziehen, ist ein Wechsel auf ein anderes Betriebssystem wie Linux oder macOS. Doch das ist in einer Windows-Welt oftmals keine Option. Wer auf Windows angewiesen ist oder schlicht dabei bleiben möchte, sollte sicherstellen, dass die aktuelle Version 10 installiert ist, da sie die modernsten Schutzmechanismen mitbringt. Windows 7 und älter gehören hingegen verbannt, da diese Versionen keine kostenlosen Sicherheits-Updates von Microsoft mehr erhalten.

Emotet steht nicht nur auf Windows, sondern auch auf Microsoft Office. Die initiale Infektion erfolgt meist über Office-Dokumente, die mit schädlichen Makros gespickt sind. Auch wenn der Makro-Code variiert, seine Funktion ist stets gleich: Er übernimmt die erste Stufe der Infektion, nämlich das Nachladen einer Exe-Datei in den Temp-Ordner und das anschließende Ausführen. Auch hier gibt es wieder einen kurzen Weg, die Infektion zu verhindern. Öffnen Sie eingehende Office-Dokumente nicht mit Microsoft Office, sondern mit LibreOffice (siehe ct.de/w7ta). Das kostenlose Office-Paket beherrscht zwar auch Makros, ist dabei aber nicht vollständig zu dem Microsoft-Pendant kompatibel, weshalb die derzeit bekannten Emotet-Makros nicht zünden. Bislang sind keine erfolgreichen Infektionen via LibreOffice bekannt.

Am besten erklären Sie LibreOffice zum Standardprogramm für Office-Dokumente und öffnen fremde Dateien nur dann mit der Microsoft-Software, wenn es unbedingt sein muss und Sie sich davon überzeugt haben, dass sie harmlos sind. In jedem Fall sollten Sie Microsoft Office so konfigurieren, dass es Makros standardmäßig blockiert, sodass Sie gar nicht erst in Versuchung geraten, den Code auszuführen. In Word 2019 etwa klicken Sie hierzu auf „Datei/Optionen/Trust Center/Einstellungen für das Trust Center…“ und wählen dort „Alle Makros mit Benachrichtigung deaktivieren“.

Sie können sich auch vor gefährlichen Makros schützen, indem Sie die Annahme bestimmter Office-Formate verweigern. Makros können zum Beispiel im alten Microsoft-Office-Format (.doc, .xls et cetera) auf Sie lauern. Bei dem aktuellen Format Office Open XML (ab MS Office 2007) dürfen nur bestimmte Dateitypen Makro-Code enthalten. Diese erkennen Sie an der Dateiendung – sind Makros erlaubt, steht hinten ein „m“ wie Makro: .docm, .dotm, .xlsm, .xltm, .xlam, .pptm, .potm, .ppam, .ppsm und .sldm. Von denen sollten Sie sich also besser fernhalten. Endet die Dateinamenerweiterung hingegen auf „x“ (.docx, .xlsx & Co.), dann sind die Dokumente makrofrei.

Erhalten Sie eine potenziell mit Makros bestückte Office-Datei, zum Beispiel ein Word-Dokument mit der Dateiendung .doc oder .docm, dann fordern Sie den Absender auf, das Dokumenten noch mal in einem ungefährlicheren Format wie .docx zu speichern und erneut zuzusenden.

Auch allen anderen Dateitypen sollten Sie skeptisch gegenüberstehen und sie im Zweifel lieber nicht öffnen. Dies gilt insbesondere für .exe-Dateien, aber auch Batch- und Skript-Formate wie .bat, .com, .vbs, ps1, .psm1, und .psd1. Cyber-Ganoven nutzen gern exotische Formate zur Verbreitung von Schadcode. Wenn eine Mail nicht nur ein verschlüsseltes Dateiarchiv, sondern auch gleich das dazugehörige Passwort enthält, dann ist ziemlich sicher etwas faul: Es handelt sich dabei höchstwahrscheinlich um einen Schädling, der auf diesem Weg vor dem Virenscanner versteckt wurde.

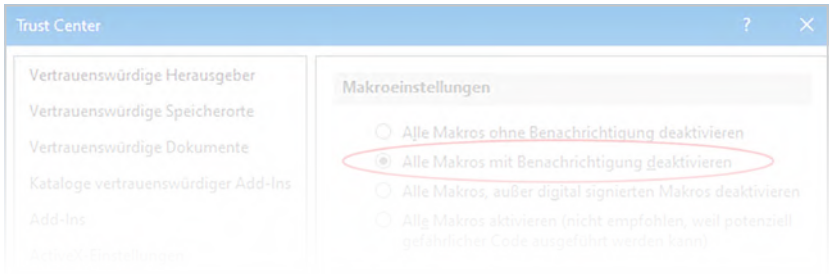


Bild: Andreas Martini

Emotet-sicheres Familien-Backup

Sie würden gern Ihre Dateien und die Ihrer Familie so sichern, dass sie auch nach einem Emotet-Befall noch da sind? Wir haben da einen Vorschlag für Sie.

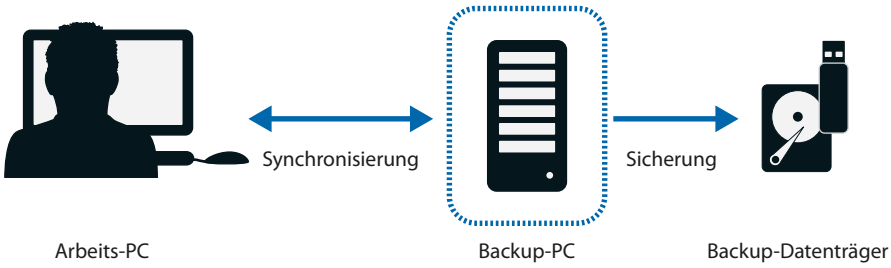
Von **Axel Vahldiek**

Sagen wir doch, wie es ist: Ein Backup anzufertigen ist ebenso notwendig wie nervig. Das gilt erst recht, wenn es nicht nur vor Datenverlust durch Fehlbedienung, Hardwaredefekte, Feuer und Diebstahl schützen soll, sondern auch durch Hightech-Trojaner wie Emotet. Denn dann muss das Backup höchste Anforderungen erfüllen (siehe S. 76), und das ist vor allem im privatem Umfeld letztlich nur durch Handarbeit zu schaffen: Erzeugen Sie Kopien auf externen Datenträgern und lagern Sie diese im feuerfesten Tresor. Der Haken daran ist, dass das regelmäßige Anfertigen solcher Backups nur sehr disziplinierte Menschen durchhalten, zumal es sehr häufig nötig ist, wenn das Backup vor allen Arten von Katastrophen gleichermaßen schützen soll. Es gibt aber einen Ausweg aus dem Dilemma: Betreiben Sie einen separaten PC als Backup-Zentrale, ein alter, eigentlich längst ausgedienter Rechner reicht dafür. Denn dieser Backup-PC hat nichts anderes zu tun, als die zu sichernden Daten von Ihrem produktiv genutzten Rechner einzusammeln und zu sichern. So bekommen Sie vollautomatisch ständig frische Backups für die alltäglichen Notsituationen. Das Sichern auf externe Medien ist so nur noch für den Fall nötig, dass wirklich mal eine Katastrophe wie ein Emotet-Befall eintritt, und kann daher seltener passieren.

Das Betreiben eines Backup-PC hat weitere Vorteile: Sie können damit nicht nur die Daten von einem, sondern von mehreren PCs sichern. Dabei

Basis-Konzept

Die Basisversion des Konzepts: Ein speziell gesicherter Backup-PC sammelt die Daten von einem Arbeits-PC und sichert sie.



kann es sich auch um die von Verwandten und Freunden handeln. Auf diese Weise profitieren alle gemeinsam von täglich frischen und vollautomatischen Backups, und eine einzige Person kann das gelegentliche Sichern auf externe Medien für alle anderen übernehmen.

Noch ein angenehmer Nebeneffekt: Wenn Sie die Sicherung Ihrer Daten durch den Backup-PC wie nachfolgend empfohlen per Synchronisierungssoftware erledigen lassen, sind diese auf Ihrem Desktop-PC und Notebook stets auf dem gleichen Stand. Diesen Service können auch andere Familienmitglieder nutzen. Wenn die Ihnen ihre Daten verschlüsselt übermitteln, dann können Sie als Betreiber des Backup-PCs die Dateien der anderen zwar sichern und wiederherstellen, aber nicht lesen.

Mehrere Arbeits-PCs

Der Backup-PC kann nicht nur die Daten eines einzelnen PCs einsammeln, sondern von mehreren.

FIDO2-Hardware einrichten und ausreizen

Mit den vorgestellten USB-Sicherheitsschlüsseln können Sie schon jetzt viele Dienste absichern – auch solche, die noch kein FIDO2 unterstützen.

Von **Jan Mahn**

Ein zweiter Faktor für Onlinedienste erhöht die Sicherheit ungemein – kommt das Kennwort in falsche Hände, braucht ein Angreifer immer noch einen weiteren Faktor, um sich Zugang zu verschaffen. Mit dem Kauf eines der FIDO2-Sticks, die wir ab Seite 122 vorstellen, und dem Einrichten von FIDO2 als zweiten Faktor bei zwei oder drei Webdiensten hat man noch lange keine zuverlässige und sichere Rundum-sorglos-Lösung für das Anmelden im Internet.

Das Problem beginnt schon damit, dass FIDO2 als sehr neue Technik bisher nur bei wenigen Anbietern konfiguriert werden kann. Die Sticks können dennoch ein wichtiger Baustein in einer privaten Sicherheitsstrategie sein – weil sie oft noch mehr können als nur FIDO2. Die Einrichtung ist aber eher

ein Wochenend- als ein spontanes Feierabendprojekt. Drei Fragen sollte man sich vorab stellen, bevor man den erstbesten Stick bestellt:

- Wie sichere ich Dienste ab, die noch kein FIDO2, dafür aber andere Verfahren als zweiten Faktor unterstützen?
- Wie melde ich mich zukünftig auf meinen mobilen Geräten und von fremden Computern an?
- Was mache ich, wenn ich mein Handy oder einen Hardware-Authenticator verliere?

Am besten beginnt man mit einer Inventur aller Webdienste, die einem so wichtig sind, dass man sie bestmöglich absichern möchte. In einer Tabelle trägt man zusammen, ob der Dienst überhaupt irgendeine Form von zweitem Faktor unterstützt. Dabei hilft ein Blick auf die Website twofactorauth.org. Sie wird von einer großen Community gepflegt, listet zahlreiche Seiten auf und stellt übersichtlich dar, welche Verfahren verfügbar sind. Hinter der Spalte „Hardware-Token" verbergen sich FIDO2 oder der Vorgänger U2F. Mit „Software-Token" in der Tabelle ist meist das Verfahren OATH-TOTP gemeint – wie Sie dieses Verfahren mit einem Hardware-Stick einrichten, erfahren Sie im Abschnitt „Komplizierterer zweiter Faktor". Außerdem gibt es SMS, Anruf und eine Bestätigungsmail als mögliche zweite Faktoren.

Auch ein Blick in die Weboberflächen der Dienste oder die Dokumentation hilft. Den Dialog zum Einrichten des zweiten Faktors findet man in den Einstellungen meist unter einem Menüpunkt wie „Sicherheit" oder „Konto". In der Tabelle sollte man sich außerdem notieren, welche E-Mail-Adresse man hinterlegt hat – an diese wird meist die Mail für Kennwortrücksetzungen geschickt.

Haben Sie eine Tabelle mit allen Accounts zusammengestellt, können Sie mit der systematischen Einrichtung beginnen. Spätestens jetzt ist es an der Zeit, einen Kennwortmanager einzusetzen und diesem die Verwaltung zu überlassen. Eine Übersicht über Passwortmanager (mit und ohne Mobilgeräte-Synchronisierung) haben wir bereits veröffentlicht

Kennwortmanager ablegen – den wahren Namen könnte man mit etwas Aufwand und Recherche in sozialen Netzwerken in Erfahrung bringen. Die meisten Kennwortmanager beherrschen Freitexteinträge.

Einfacher zweiter Faktor

Versteht ein Dienst bereits FIDO2, ist die Einrichtung eines zweiten Faktors schnell erledigt. Die Dialoge in den Einstellungsseiten führen Sie durch den Prozess und ähneln einander: Stick einstecken, Knopf betätigen, fertig. Auf Seite 130 sehen Sie beispielsweise den Dialog in einem Google-Account. Niemals dürfen Sie es bei nur einem zweiten Faktor belassen. Verlassen Sie sich auf nur einen FIDO2-Stick, haben Sie ein mittelschweres Problem, sobald Sie diesen verlieren. Im besten Fall haben Sie einen Stick für den Alltag und einen zweiten, den Sie zu Hause an einem sicheren Ort aufbewahren.

Viele Dienste zeigen Ihnen nach der Einrichtung Rücksetzcodes und empfehlen eindringlich, diese auszudrucken – am besten erledigen Sie das sofort und vertagen diese lästige Pflicht nicht auf später. Bei Google, Facebook & Co. brauchen Sie keine Hoffnung zu haben, über die Hotline oder nette Briefe wieder an Ihren Account zu kommen, sollten Sie Ihren einzigen zweiten Faktor verlegt haben.

Als FIDO2-Authenticator können nicht nur Hardware-Token dienen, sondern auch Android-Smartphones, -Tablets, Windows-PCs und einige MacBooks. Sie haben einen Chip, der meist als „Trusted Platform Module" bezeichnet wird. Dort liegt dann der private Schlüssel in einer nicht auslesbaren Form und wird zum Lösen der FIDO2-Challenges genutzt. Damit können Sie mehrere der eingangs gestellten Fragen auf einmal beantworten: Sie können unterwegs auf Ihre Accounts zugreifen und haben einen Stick für den PC zu Hause und als Backup-Zugang, wenn das Handy mal verschwindet. Unter Android brauchen Sie ein aktuelles Gerät mit Android 7 oder höher. Das Hinterlegen des Geräts bei einem Dienst funktioniert genau-

Tipps fürs Unterwegs-sein mit WireGuard

Ein Virtual Private Network (VPN) schützt den Datenverkehr von Smartphone oder Computer, indem es Daten in einem Tunnel verschlüsselt überträgt. Damit kann man offene WLAN-Hotspots ohne Abhörgefahr nutzen. Mit der jungen Technik WireGuard geht das besser und einfacher denn je.

Von **Peter Siering**

WireGuard als VPN-Technik ist cool: Verbindungen überleben Roaming, also den Wechsel eines Peers (Clients) zwischen Mobilfunknetz und WLAN, ohne dass Anwender oder Anwendungen das spüren. Das Einrichten eines WireGuard-Zugangs fällt obendrein sehr leicht, weil eine 300 Zeichen große Konfigurationsdatei genügt. Die nötige Software gibt es mittlerweile für alle gängigen Desktop- und Mobilbetriebssysteme. Für wenige Euro pro Monat bieten die einschlägigen VPN-Provider Zugänge an.

Einige VPN-Anbieter stricken für den WireGuard-Zugang eigene Anwendungen. Oft tun sie das, um aus ihrer Sicht Defizite der bisher verfügbaren offiziellen Software auszubügeln. Den Entwicklern hinter WireGuard missfällt das, weil sie inkompatible Entwicklungen scheuen. Deshalb raten sie dazu, solche Software zu meiden. Dieser Artikel folgt der Empfeh-

lung und betrachtet inoffizielle Software oder Erweiterungen nur am Rande, sofern sie das offizielle Angebot ergänzen.

Scan & Surf

Die Eintrittskarte, die ein Peer am WireGuard-VPN-Server vorweisen muss, ist eine wenige Zeilen lange Konfigurationsdatei im klassischen INI-Format. Sie enthält die für den Aufbau und Schutz der Verbindung nötigen Schlüssel und einige wenige weitere Angaben. Wer einen WireGuard-Zugang von einem der Anbieter erhält, muss sich normalerweise um nichts weiter kümmern. Der Anbieter generiert alle Schlüssel und ergänzt nötige Optionen.

Die Daten aus der Konfigurationsdatei passen in einen QR-Code. Mit der WireGuard-App auf einem Mobilclient scannt man den ein und schon ist die Einrichtung erledigt. Einfacher geht es nicht. Darin lauert eine ernste Gefahr: Die QR-Codes sind ein Freifahrtschein. Wer den hat, kann den VPN-Zugang nutzen. Das heißt, dass man diese Codes in der Regel nicht druckt und aus der Hand gibt, sondern besser gleich vom Bildschirm scannt beziehungsweise scannen lässt. Die WireGuard-Software für Desktop-Betriebssysteme verarbeiten die Datei üblicherweise direkt. Ihr Klartext schaut so aus (die Schlüssel haben wir für bessere Lesbarkeit gekürzt):

```
[Interface]
PrivateKey = sBO5dkE+A...gxL/zJuFc=
Address = 192.168.2.1, fdOO:2::1/128
DNS = 1.1.1.1,2606:47OO:47OO::1111
[Peer]
PublicKey = 6VfvK9vRH...xMsgQ1nmQ=
PresharedKey = 9IDsgjmHt...m+bXbnw124=
Endpoint = 192.168.1.1:12345
AllowedIPs = 0.0.0.0/0, ::/0
```

Die Warnung für den Umgang mit dem QR-Code gilt natürlich genauso für die Konfigurationsdatei. Wer

Die Android-App kennt Ausnahmen für Applikationen. Die Daten fließen dann nicht durch den Tunnel.

im WLAN oder im Mobilfunknetz, nur in ausgewählten WLANs (etwa im Freifunk-Netz) oder in ausgewählten WLANs genau nicht (etwa im heimischen). Die von Apple vorgesehenen VPN-Einstellungen muss man nie bemühen – die WireGuard-Verbindungen tauchen dort aber als solche auf.

Die **Android-App** glänzt damit, dass sie für einzelne Apps Ausnahmen definieren kann, die dann den VPN-Tunnel umgehen dürfen. Das gelingt, indem man die Details einer Verbindung bearbeitet. Weitere Wünsche muss man in den Android-Einstellungen anmelden – was dort geht, variiert mit der

Netzwerkschnüffler: Packet Squirrel

Kleine Box, große Wirkung: Das Packet Squirrel zeichnet Netzwerkverkehr auf und kann ihn beliebig manipulieren.

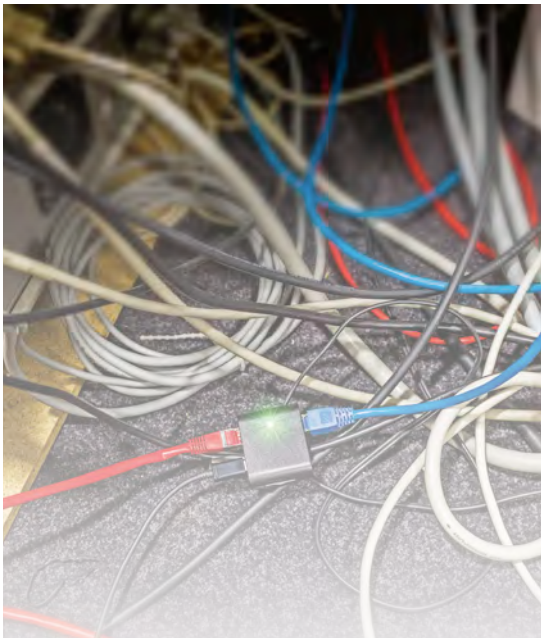
Von **Ronald Eikenberg**

Kaum größer als eine Streichholzschachtel ist das Packet Squirrel. Es handelt sich um einen Kleinstrechner mit Linux, der Netzwerkverkehr aufzeichnen, steuern und manipulieren kann. Die wichtigsten Anschlüsse sind die beiden LAN-Schnittstellen: die eine verbindet man mit einem Netzwerk, die andere mit einem beliebigen Client.

Versorgt man das Squirrel über Micro-USB mit Strom, schleust es den Netzwerkverkehr zwischen den beiden Ports erstmal mit 100 MBit/s durch. Per Schiebeschalter aktiviert man eine von drei Payloads, wodurch das Gerät etwa den durchgeleiteten Netzwerkverkehr mit tcpdump auf einen USB-Stick schreibt.

Anschließend kann man den Traffic mit Wireshark bequem am Rechner auswerten. Eine andere Payload sorgt dafür, dass der Verkehr an ein beliebiges Ziel umgeleitet wird. Dabei fängt das Packet Squirrel DNS-Anfragen des Clients ab und beantwortet sie mit einer einstellbaren IP-Adresse (DNS Spoofing).

Über den Schalter erreicht man auch den Konfigurationsmodus, in dem das Squirrel über SSH konfigurierbar ist. Man stößt auf ein schlankes Linux, das auf OpenWRT basiert. Es ist mit einigen zweckdienlichen Tools ausgerüstet: Neben tcpdump sind



In diesem Kabelsalat lauert ein Packet Squirrel auf Netzwerkpakete.