Pegasus bei BND und BKA

Pegasus bei BND und BKA

Nach und nach werden weitere Kunden der israelischen NSO Group bekannt. Offenbar haben auch deutsche Polizeibehörden und Nachrichtendienste die Spyware Pegasus gekauft.

Deutsche Behörden nutzen umstrittene Spyware

Nach und nach werden weitere Kunden der israelischen NSO Group bekannt. Offenbar haben auch deutsche Polizeibehörden und Nachrichtendienste die Spyware Pegasus gekauft.

Von Sylvester Tremmel

Das Bundeskriminalamt (BKA) und der Bundesnachrichtendienst (BND) setzen offenbar die Überwachungssoftware Pegasus ein. Das berichten Zeit, Süddeutsche Zeitung, WDR und NDR. Im Fall des BKA soll das Bundesinnenministerium über den Einsatz informiert gewesen sein, nicht aber Innenminister Horst Seehofer selbst. Beim BND war angeblich das Bundeskanzleramt eingeweiht. Das Parlamentarische Kontrollgremium, dem unter anderem die Kontrolle des BND obliegt, soll nicht informiert worden sein.

Pegasus war im Juli dieses Jahres durch Veröffentlichungen des Rechercheverbundes „Pegasus Project“ der breiten Öffentlichkeit bekannt geworden. Den Recherchen zufolge wird Pegasus von einer Vielzahl von Akteuren auf der ganzen Welt eingesetzt; nicht nur zur Bekämpfung schwerwiegender Kriminalität, sondern auch, um Politiker, Oppositionelle, Menschenrechtsaktivisten und Journalisten zu überwachen.

Das steht im krassen Gegensatz zu den Versicherungen des israelischen Herstellers NSO Group: Das Unternehmen schreibt, man lizenziere seine Software nur an „ausgewählte, genehmigte, bestätigte und berechtigte Staaten und staatliche Behörden“. Pegasus dürfe nur zur „nationalen Sicherheit“ und in „größeren Ermittlungen“ von Sicherheitsbehörden zum Einsatz kommen. Andererseits betont die NSO Group auch, nicht zu wissen, wie ihre Kunden Pegasus tatsächlich nutzen.

Laut NSO Group kommt Pegasus nur gegen Terror und Kriminalität zum Einsatz.

Pegasus fürs BKA zu mächtig

Dem BKA wollte die NSO Group ihre Software 2017 verkaufen, berichtet Tagesschau.de. Dazu sei es nicht gekommen, weil das BKA Vorbehalte gehabt habe: Deutsches Recht unterscheidet zwischen Online-Durchsuchungen und der Quellen-Telekommunikationsüberwachung (Q-TKÜ). Im ersten Fall werden auf einem Gerät gespeicherte Daten ausgeleitet. Bei der Q-TKÜ wird dagegen nur die Kommunikation abgegriffen, analog zur abgehörten Telefonleitung. Pegasus habe diese Unterscheidung nicht getroffen und noch weitere Probleme aufgewiesen.

Nach einem Bericht der Wochenzeitung Die Zeit änderte sich dies 2020. Die NSO Group habe dem BKA eine angepasste Version von Pegasus zur Verfügung gestellt, die mit deutschem Recht vereinbar sein soll – zumindest nach Ansicht des BKA. Wie genau der BND Pegasus einsetzt, ist nicht bekannt.

Mit dem Einsatz von Pegasus stellen sich deutsche Behörden in eine Reihe von fragwürdigen Käufern, die erhebliche Zweifel daran aufkommen lässt, dass die NSO Group ihre Kunden ausreichend sorgfältig überprüft. Anfang Oktober befand etwa

ein englisches Gericht, dass Muhammad bin Raschid Al Maktum, Herrscher des Emirats Dubai, die Software eingesetzt habe, um seine Exfrau und ihre Anwälte zu überwachen.

Bedenklich ist auch der Verdacht, die NSO Group könnte Einblick in die mit Pegasus durchgeführten Überwachungsoperationen haben – entgegen ihrer Aussagen. Gegenüber der Zeit erklärten BND und BKA, das technisch ausschließen zu können. Die Zeitung berichtet aber von entgegenstehenden Aussagen ehemaliger Mitarbeiter der NSO Group. Demnach würden die exfiltrierten Daten über Server des Unternehmens fließen.

Hinzu kommt ein moralisches Problem: Um Software wie Pegasus auf Zielgeräte ausspielen zu können, muss die NSO Group schwerwiegende Sicherheitslücken in aktuellen Versionen von iOS und Android kennen und geheim halten. Die daraus erwachsende Gefährdung sämtlicher Smartphone-Besitzer wird in Kauf genommen. Kunden der NSO Group finanzieren dieses Geschäftsmodell, statt die breite Masse ihrer Bürger zu schützen.

Im Fall von Android ist nicht bekannt, über welche Lücken Pegasus auf Geräte gelangt. Unter iOS war ein Einfallstor mutmaßlich eine Lücke in der App iMessage. Darüber konnte Pegasus ausgespielt werden, ohne dass die iPhone-Nutzer irgendetwas tun mussten – eine sogenannte Zero-Click-Lücke. Die hat Apple mittlerweile geschlossen, welche weiteren Lücken die NSO Group noch kennt, weiß nur sie selbst. *(syt@ct.de)*

Recherchen zu Pegasus: ct.de/yfzj

ct.de/yfzj

- **The Pegasus Project** Seite des Pegasus Projekts beim Journalismus-Netzwerk Forbidden Stories.
- **Forensic Methodology Report: How to catch NSO Group's**

Pegasus Forensischer Bericht zu Pegasus des Security Labs von Amnesty International.

c’t-Berichterstattung zum Thema Pegasus

- **Infiziert ohne Klick: Amnesty International deckt Massenüberwachung durch Pegasus auf**
- **Rüffel vom Fachmann: Sicherheitsforscher fordert grundlegende iOS-Überarbeitung**
- **Spyware-Entdecker: Geheimdienst-Spionagetool Pegasus auf dem iPhone enttarnen**

Pegasus an deutschen Behörden

- **BKA bekam maßgeschneiderten Trojaner** Tagesschau.de zum Pegasus-Einsatz beim BKA.
- **Bundesnachrichtendienst setzt umstrittene Cyberwaffe ein** Zeit-Bericht zum Einsatz von Pegasus beim BND.
- **Bundesnachrichtendienst spitzelt mit Pegasus** Tagesschau.de zum Pegasus-Einsatz beim BND.

Zertifikat für Container-Profis

Aktuell | Cloud

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

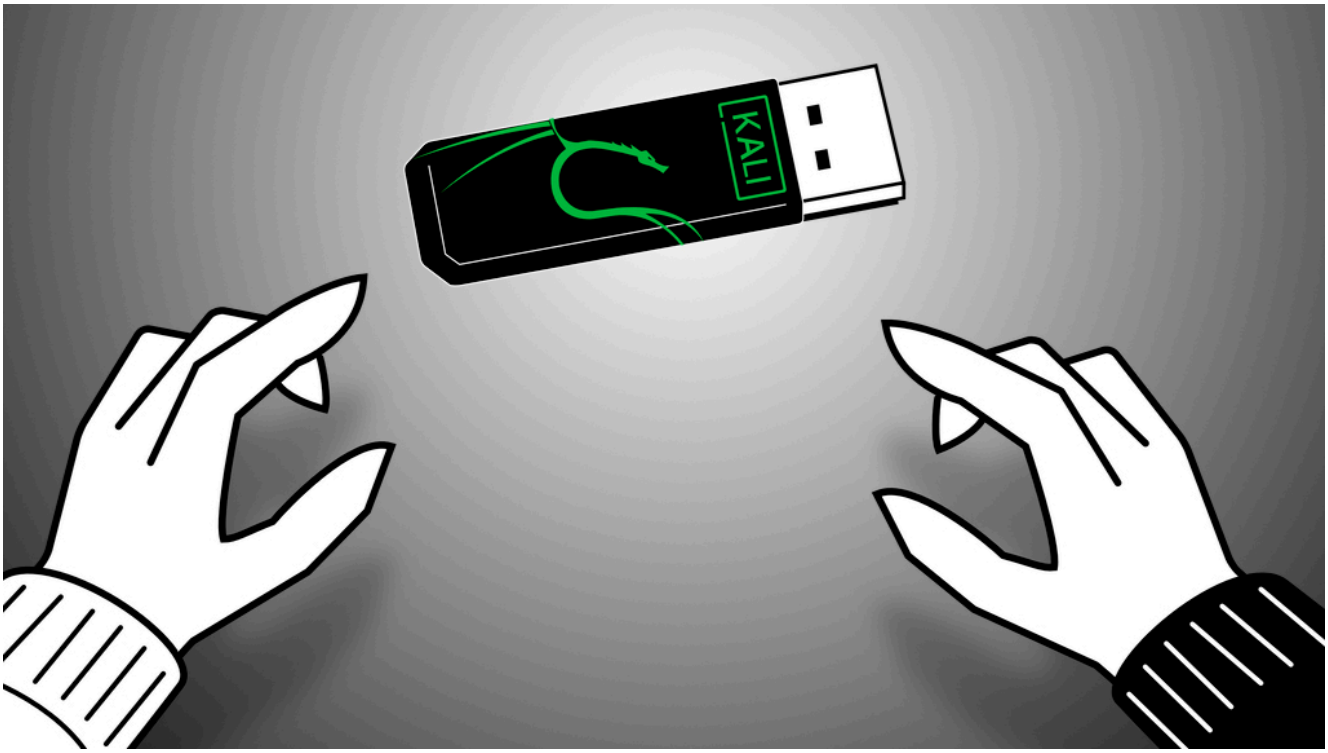
Zertifikat für Container-Profis

Spezialisten, die sich mit dem Container-Orchestrator Kubernetes und Software aus dem Cloud-Umfeld auskennen, sind im IT-Personalmarkt noch einmal besonders gefragt. Wer Arbeitgebern zeigen möchte, dass er Kompetenz in diesem Bereich mitbringt, kann sein Wissen von der Linux Foundation dokumentieren lassen. Die hat jetzt im Rahmen der Kubernetes-Konferenz KubeCon eine neue Zertifizierung vorgestellt: **Kubernetes and Cloud Native Associate (KCNA)** darf sich nennen, wer in einer Onlineprüfung grundlegendes Wissen zu Container-Verwaltung, Cluster-Einrichtung und der Arbeit mit kubectl

nachweist.

Eine Übersicht über die geprüften Inhalte und Informationen zur Prüfungsanmeldung finden Sie über ct.de/ytvq. Auf dem Wissen für die KCNA-Prüfungen bauen die schon bestehenden Zertifikate zum Certified Kubernetes Administrator (CKA), Application Developer (CKAD) und Security Specialist (CKS) auf. Ende des Jahres soll das Onlineexamen zum KCNA freigeschaltet werden. (jam@ct.de)

Kali Linux auf USB-Stick einrichten



Hacking-Stick

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

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

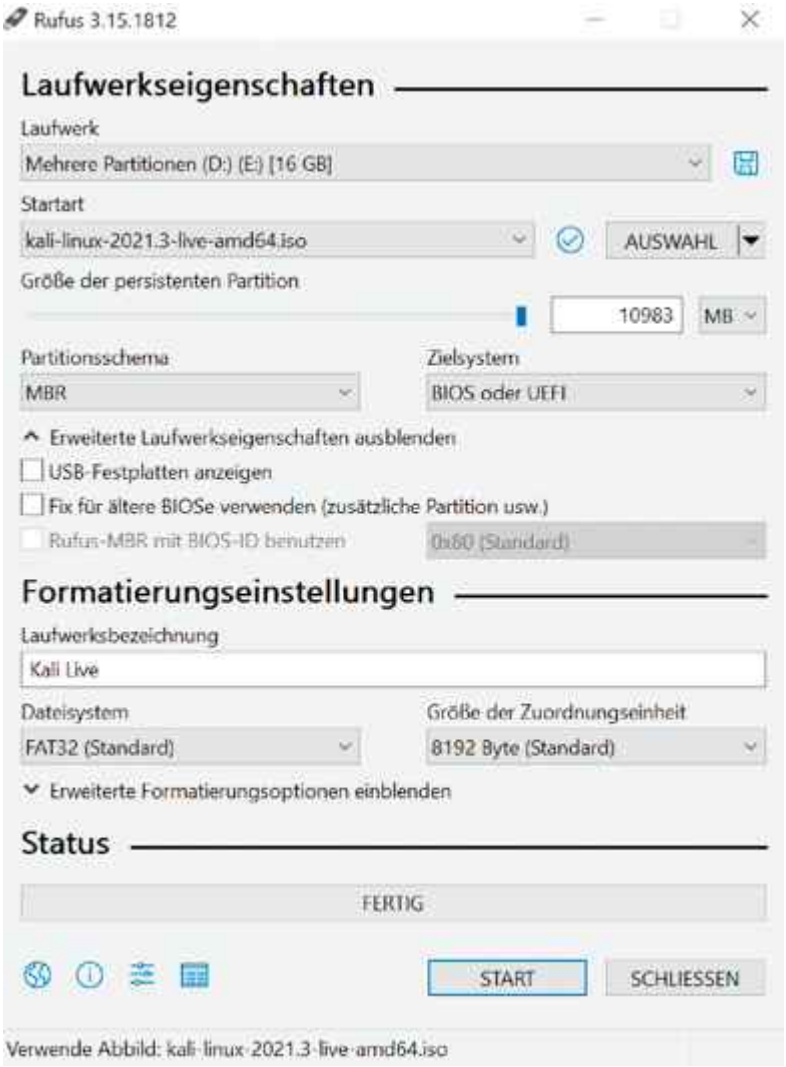
Dieser Artikel zeigt Ihnen das Einrichten eines Kali-Live-Sticks, den Sie universell einsetzen können, sowie die ersten Schritte, damit Sie komfortabel damit arbeiten können. Gegenüber einer virtuellen Maschine hat so ein Live-Stick den Vorteil, dass sein Betriebssystem direkt auf die Hardware des Rechners 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/ypk1) 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.

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.



Klick, Klick, Stick: Rufus erstellt nach ein paar Mausklicks einen bootfähigen Kali-Stick samt Persistence-Partition, in der Sie Daten dauerhaft ablegen können.
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/ypk1) 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 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/ypk1), 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/ypk1). Dort erfahren Sie auch, wie Sie die Partition mit LUKS verschlüsseln, um sie vor unbefugten Zugriffen zu schützen.

Die Kali-Installation enthält etliche Security-Tools, die man ohne Installation ausprobieren kann.

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.

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

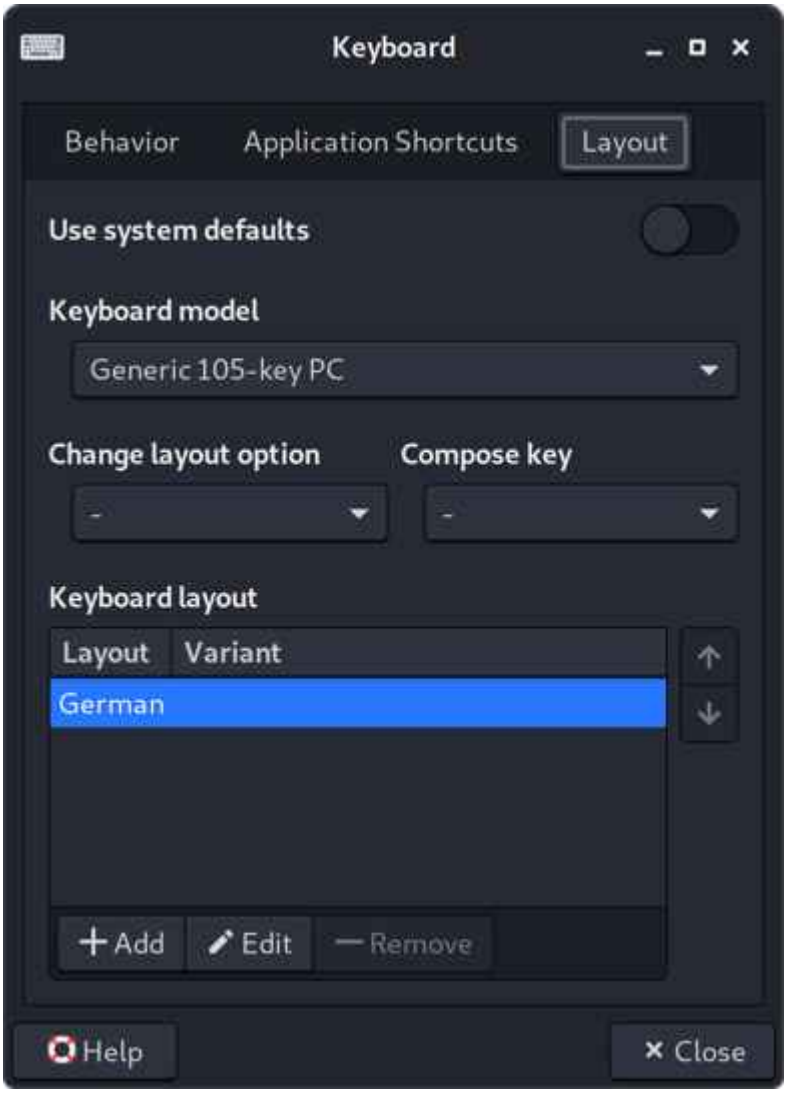
Hat alles geklappt, bootet Kali nach kurzer Zeit automatisch bis zum Desktop durch, die Eingabe eines Passworts ist nicht nötig. Falls sich Kali nach einiger Zeit der Inaktivität sperrt, erlangen Sie mit dem vorgegebenen Nutzernamen kali und dem gleichnamigen Passwort kali wieder Zugriff.

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 24.

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.



Erste Amtshandlung: Im Live-Modus sollte man zunächst das Tastaturlayout ändern.

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 NetworkManager-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 20) 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. 25). 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 frischmachen

Mit den folgenden Befehlen bringen Sie Kali und die Tools auf den aktuellen Stand:

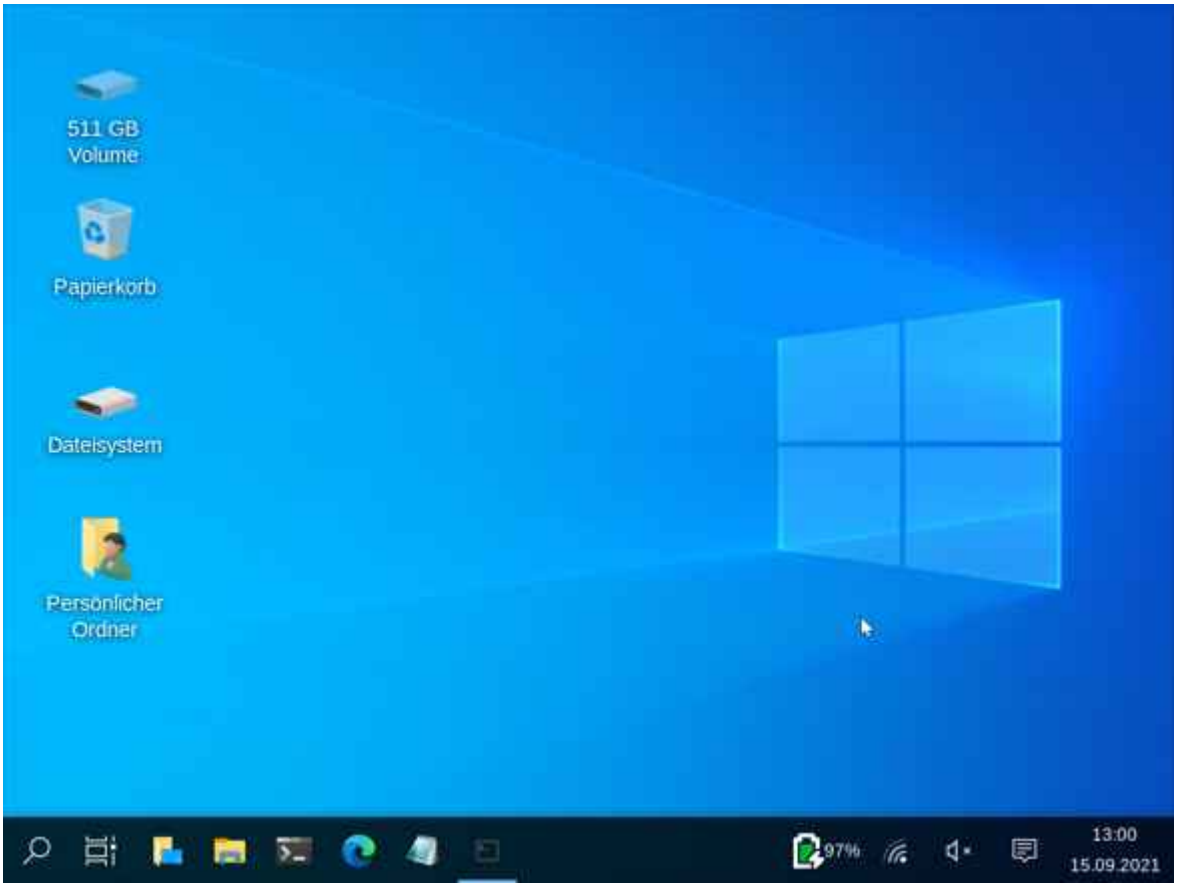
```
sudo apt update
sudo apt full-upgrade
```

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.



Kali tarnt sich auf Wunsch als Windows 10.

Entdecke die Möglichkeiten

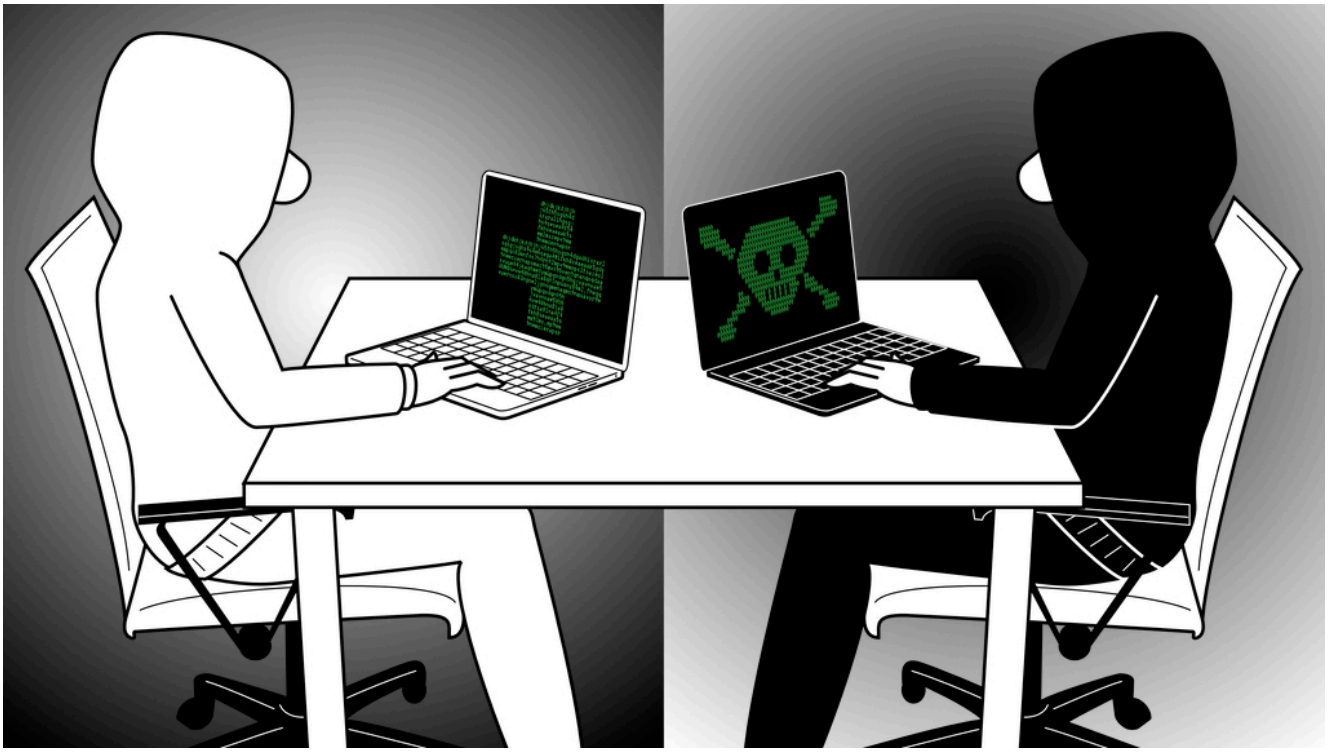
Mit Ihrem Kali-Stick steht Ihnen eine prall gefüllte Werkzeugtasche zur Verfügung, die Ihnen in vielen Situationen gute Dienste leistet. Die meisten Tools lassen sich zwar in die Oberkategorie „IT-Security“ einsortieren, doch Kali kann viel mehr. Wenn die Systemplatte streikt, können Sie mit TestDisk 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 24, der viele wichtige und nützliche Tools detailliert vorstellt. (*rei@ct.de*)

Kali-Download & Tools: ct.de/ypk1

Hacking-Werkzeug für Fortgeschrittene



Gute Tools, böse Tools

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

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 im Artikel „Hack Dich selbst“ auf Seite 18, der nützliche Problemlöser für den Alltag präsentiert.

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 30 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/ygg5. Aber genug der Vorrede – jetzt geht es in die Vollen!

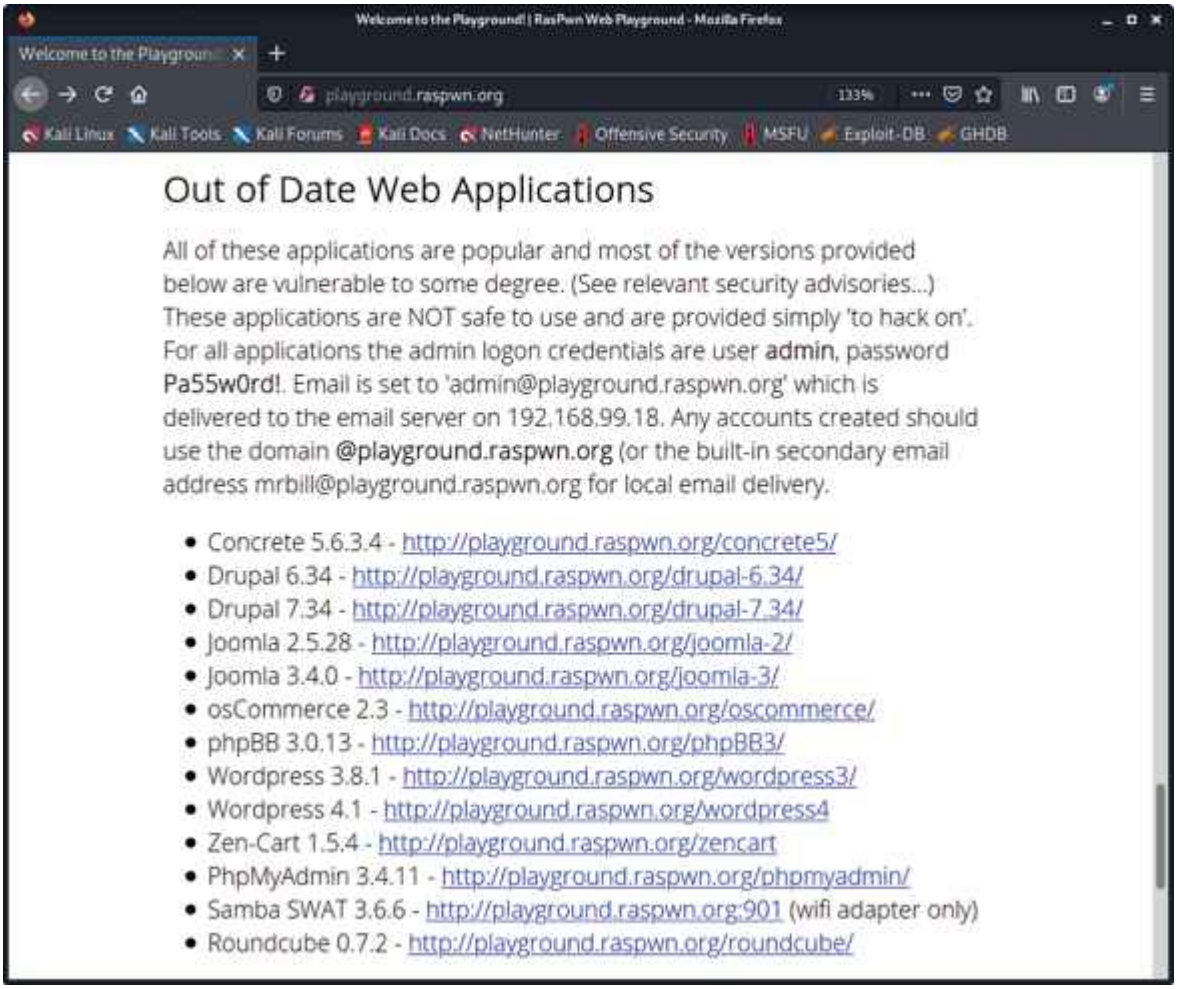
Angreifen erlaubt

Die hier genannten Hacking-Tools sind nicht illegal, aber natürlich dürfen Sie damit nicht gegen geltende Gesetze verstoßen (siehe Seite 170). 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.

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/ygg5).



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

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 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.

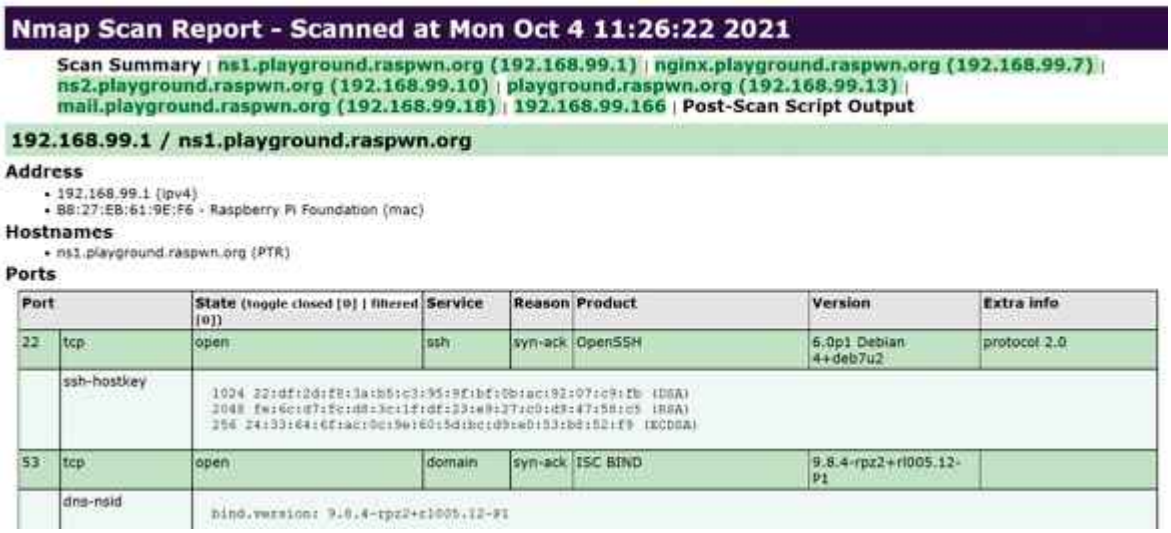
Wirklich komfortabel lesbar ist der Bericht auf der Shell nicht. Sie können jedoch leicht einen formatierten HTML-Report erstellen, indem Sie zunächst Nmap mit -oX ergebnis.xml anweisen, einen XML-Export der Ergebnisse zu schreiben. Anschließend bauen Sie daraus mit dem unter Kali vorinstallierten Tool 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/ygg5). 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.

Hardcore

Eine Übersicht über die mitgelieferten Skripte finden Sie in der Dokumentation von Nmap (siehe ct.de/ygg5). 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.

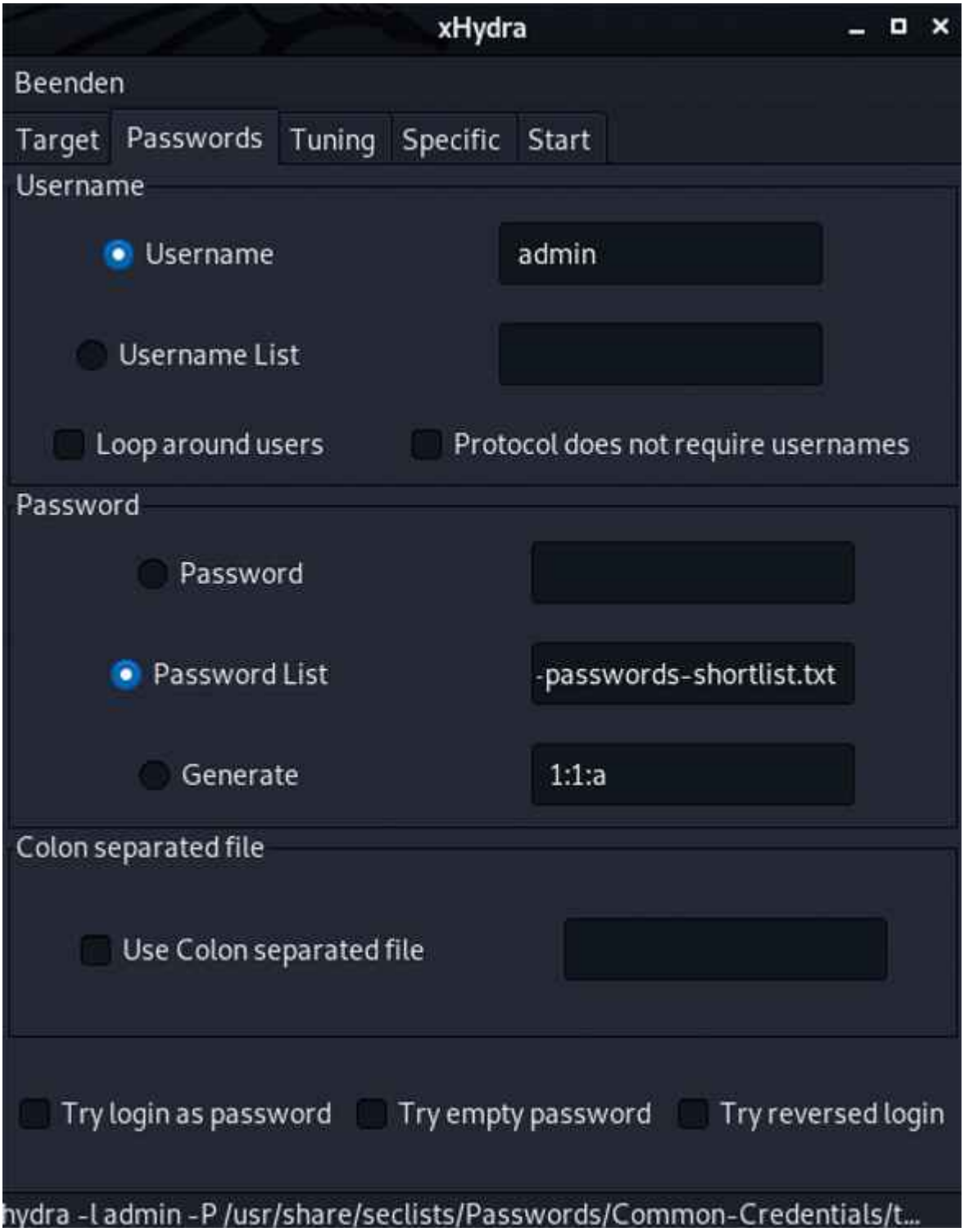


Was ist los im Netz? Der Netzwerkscanner Nmap liefert einen HTML-Bericht über alle Geräte und Dienste.

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 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.



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

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 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.

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

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.
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 170). Beachten Sie, dass die Werkzeuge sehr viele Anfragen und damit potenziell auch eine hohe Last erzeugen, was die Erreichbarkeit des Servers beeinträchtigen kann.

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 (siehe S. 60 ff.) 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/ygg5). 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 Verbindung danach, ehe Sie schließlich 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/ygg5).

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.

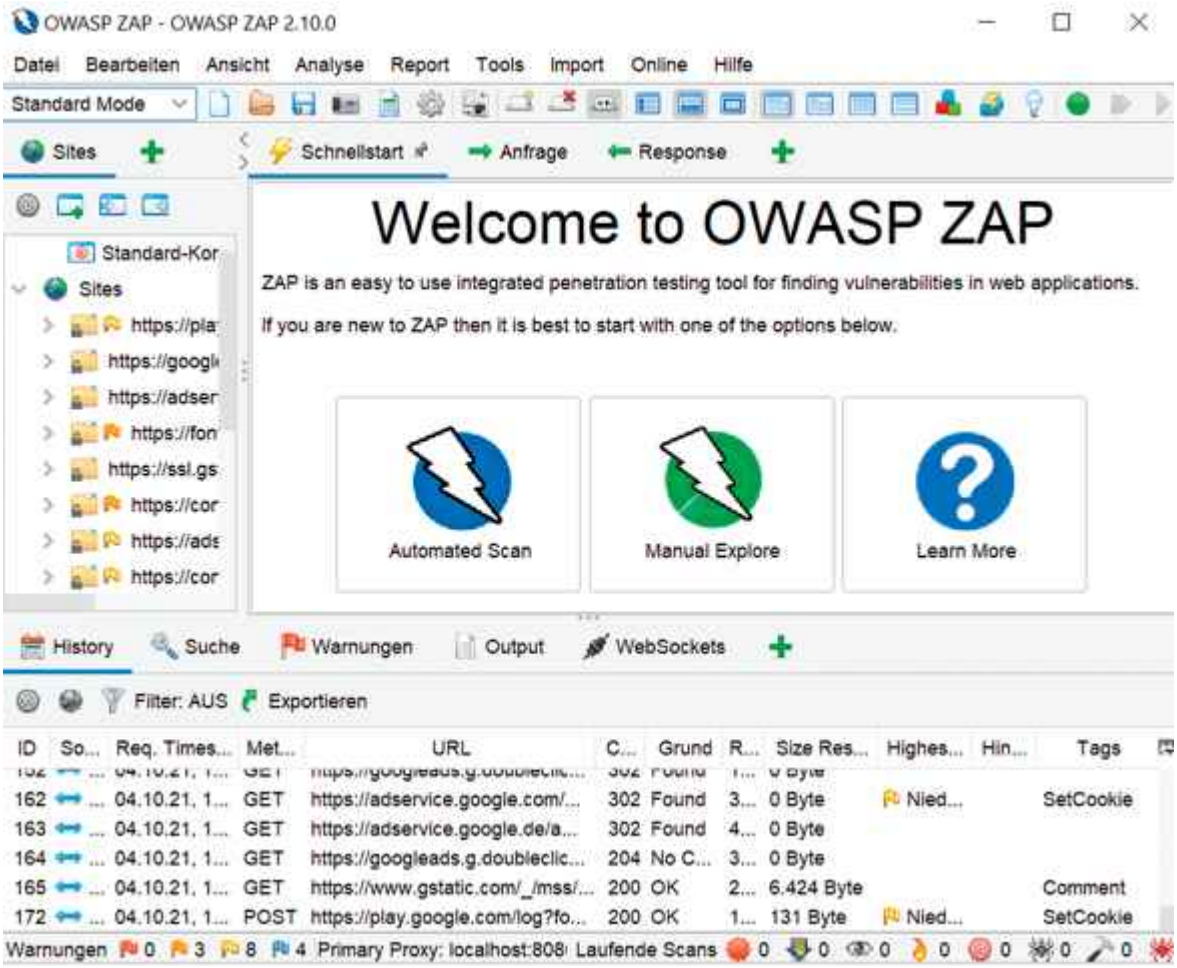
Für einen ersten Funktionstest können Sie die absichtlich anfällige „Wacko Picko“-Website von RasPwn mit SQLmap scannen.

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 mit --data anweisen, genau das herauszufinden:

```
sqlmap -u "http://wackopicko.playground.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.



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

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.

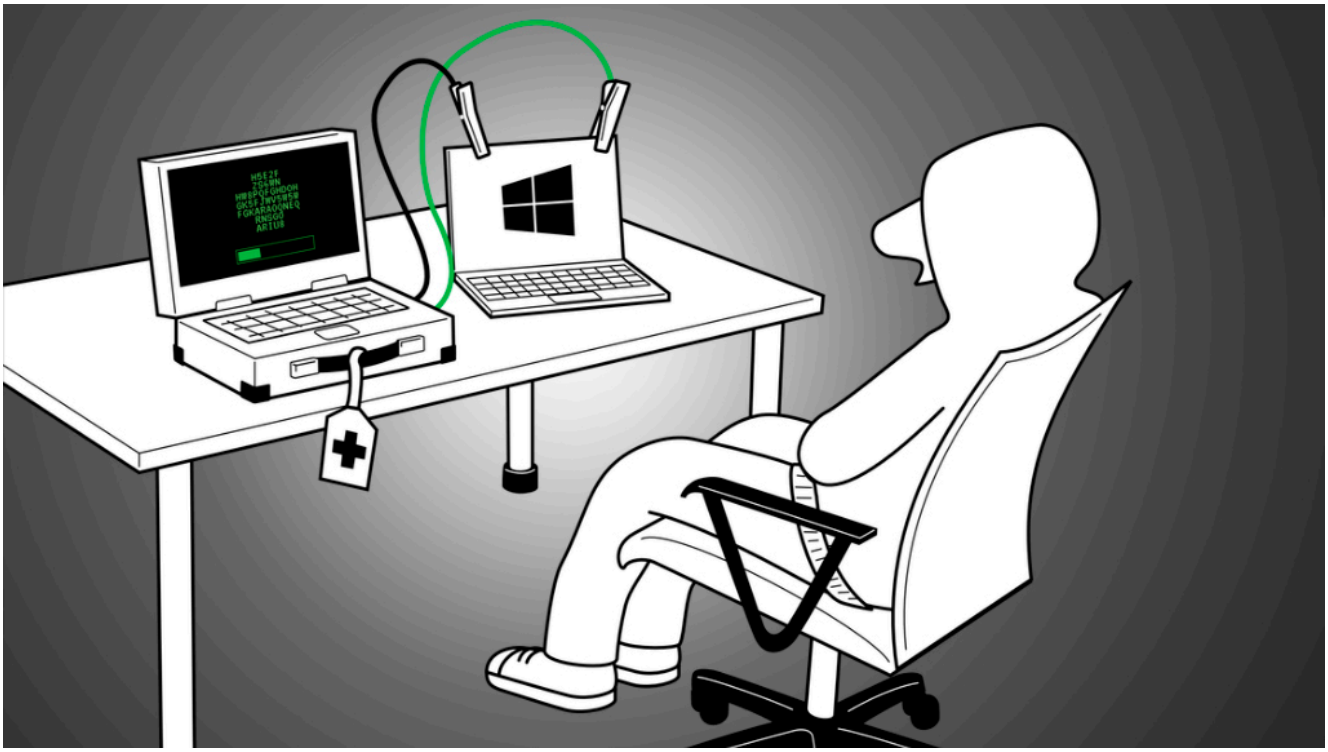
Das von der NSA entwickelte Reverse-Engineering-Toolkit **Ghidra** ist interessant, wenn Sie ausführbaren Code (wie EXE- und DLL-Dateien) bis ins letzte Bit auseinandernehmen und verstehen möchten. Es dekompiliert Binärdateien und kann sie auch wieder zusammenbauen, ähnlich wie der kommerzielle Disassembler IDA Pro. In c't 14/2020 haben wir Ghidra ausführlicher getestet (siehe ct.de/ygg5).

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@ct.de)*

Hacking-Tools & weitere Infos: ct.de/ygg5

Hack Dich selbst – Nützliche Hacking-Tools für den Alltag



Hack Dich selbst

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.
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.

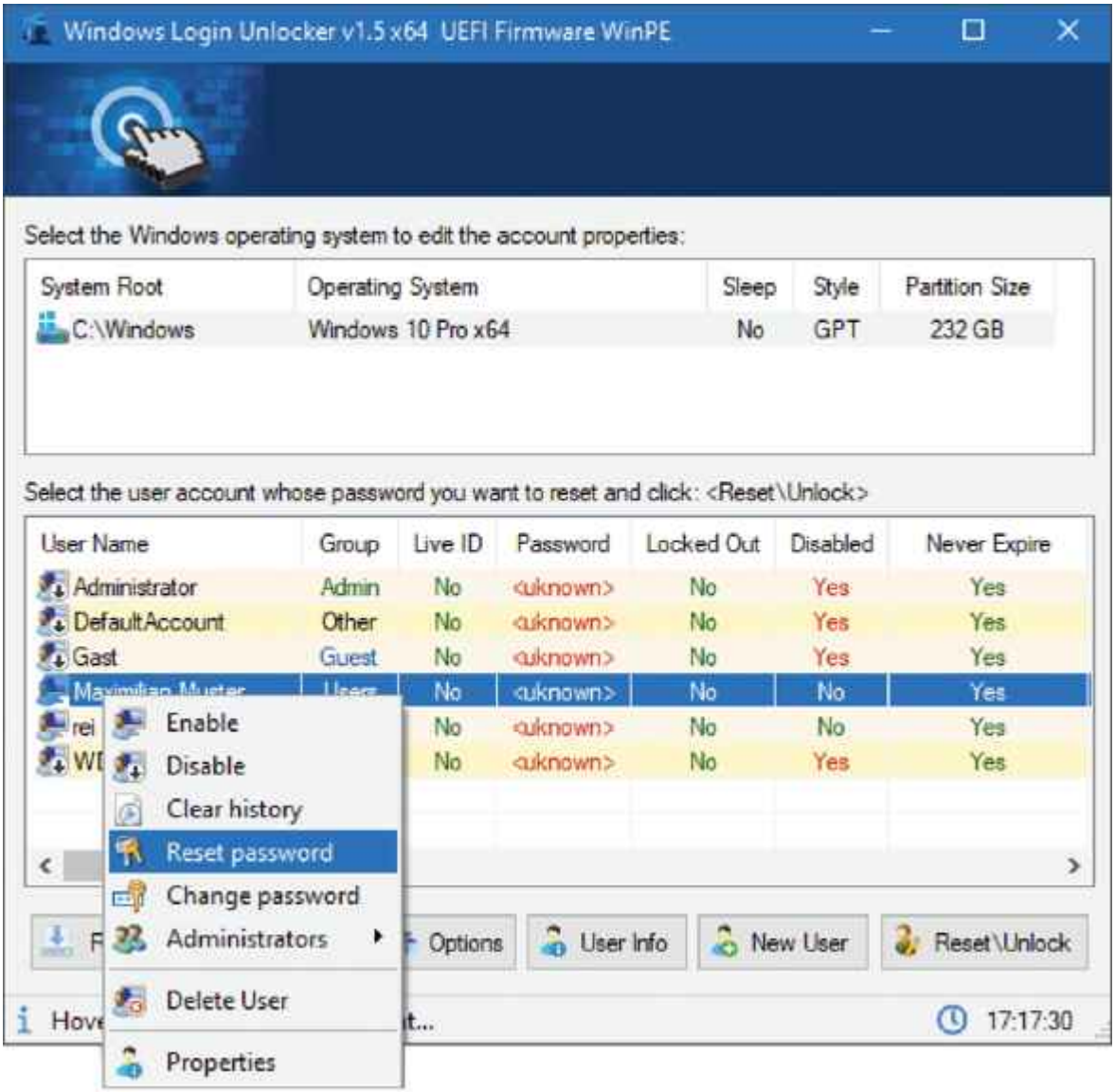
Bei Hackerangriffen ist keine schwarze Magie im Spiel, häufig sind es frei verfügbare Open-Source-Tools, die für sich genommen nicht gefährlich sind. Nach einer Infektion werden sie nachgeladen und automatisiert ausgeführt, um zum Beispiel Dateien oder Passwörter erstmal lokal einzusammeln. Ausgeleitet 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/y41x.

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.



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

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/y41x). 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 30) 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.

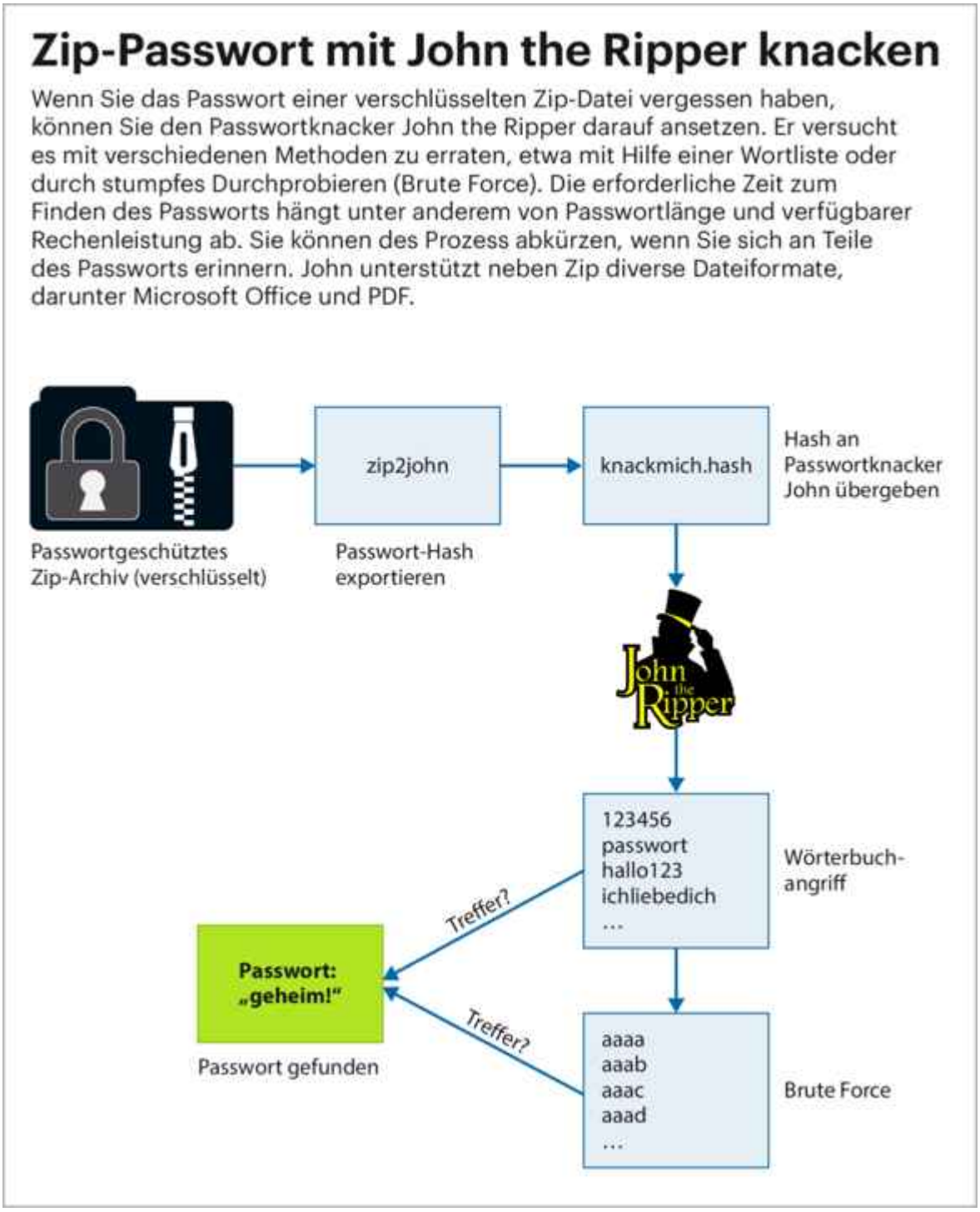
John gibt es für Windows, Linux und macOS, bei Kali Linux (siehe S. 30) ist er bereits an Bord. Er liest die verschlüsselten Dateien nicht selbst ein, er benötigt

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 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 aussichtlos ist. In diesem Fall sollten Sie den Suchradius möglichst weit eingrenzen.



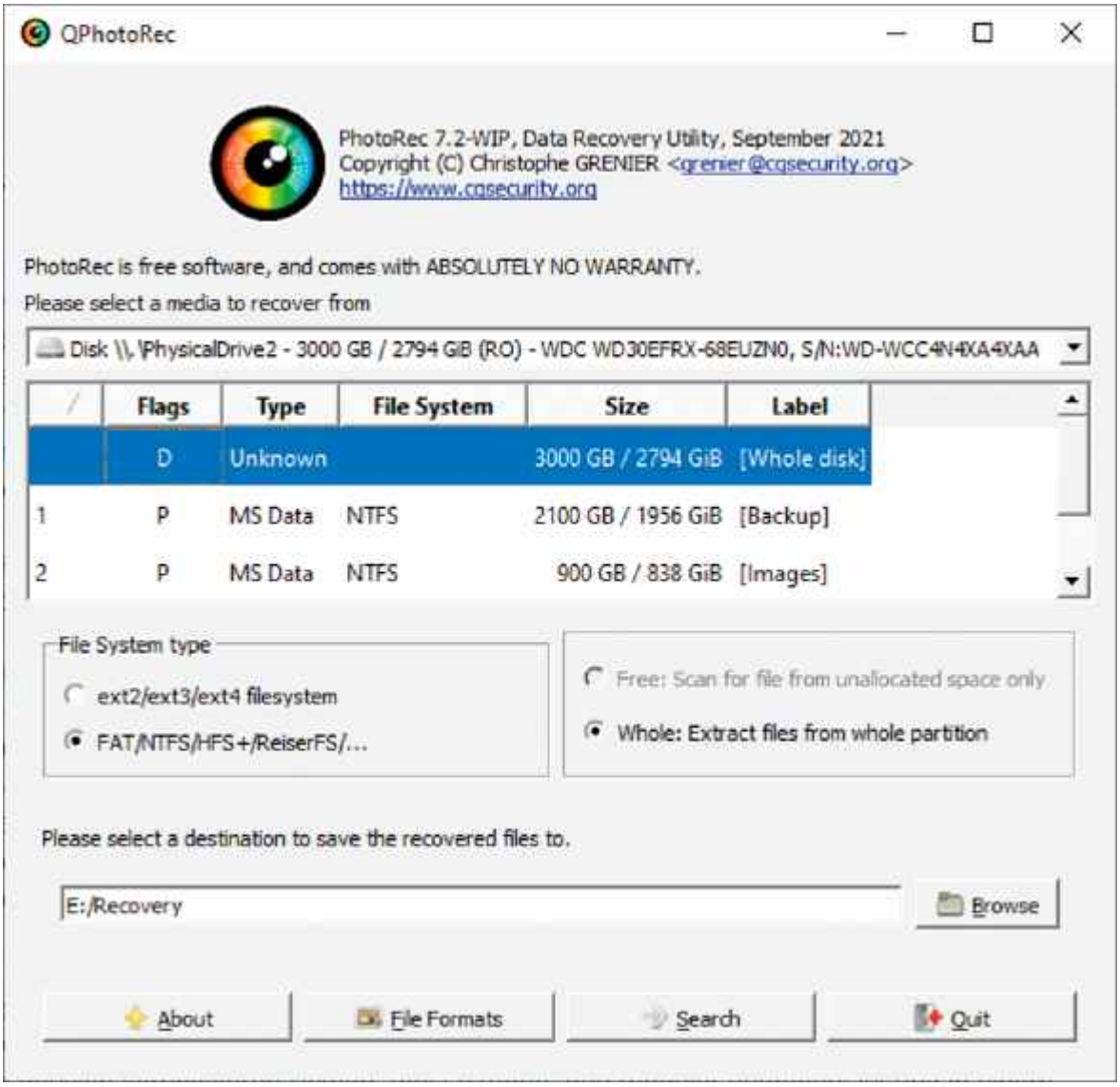
Sie können zum Beispiel eine Mindest- und Maximallänge wie 5 und 6 Zeichen vorgeben, indem Sie -min-length=5 -max-length=6 an den Befehl hängen. Mit -incremental=digits würden Sie den Suchradius auf Ziffern beschränken, um zum Beispiel ein Passwort zu finden, das aus einem Geburtsdatum besteht. Wer einen Teil seines Passworts kennt, sollte John nach einer Passwortmaske suchen lassen. Den Aufbau solcher Masken erklärt die Dokumentation en détail (siehe ct.de/y41x). 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

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 möglichweise 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.



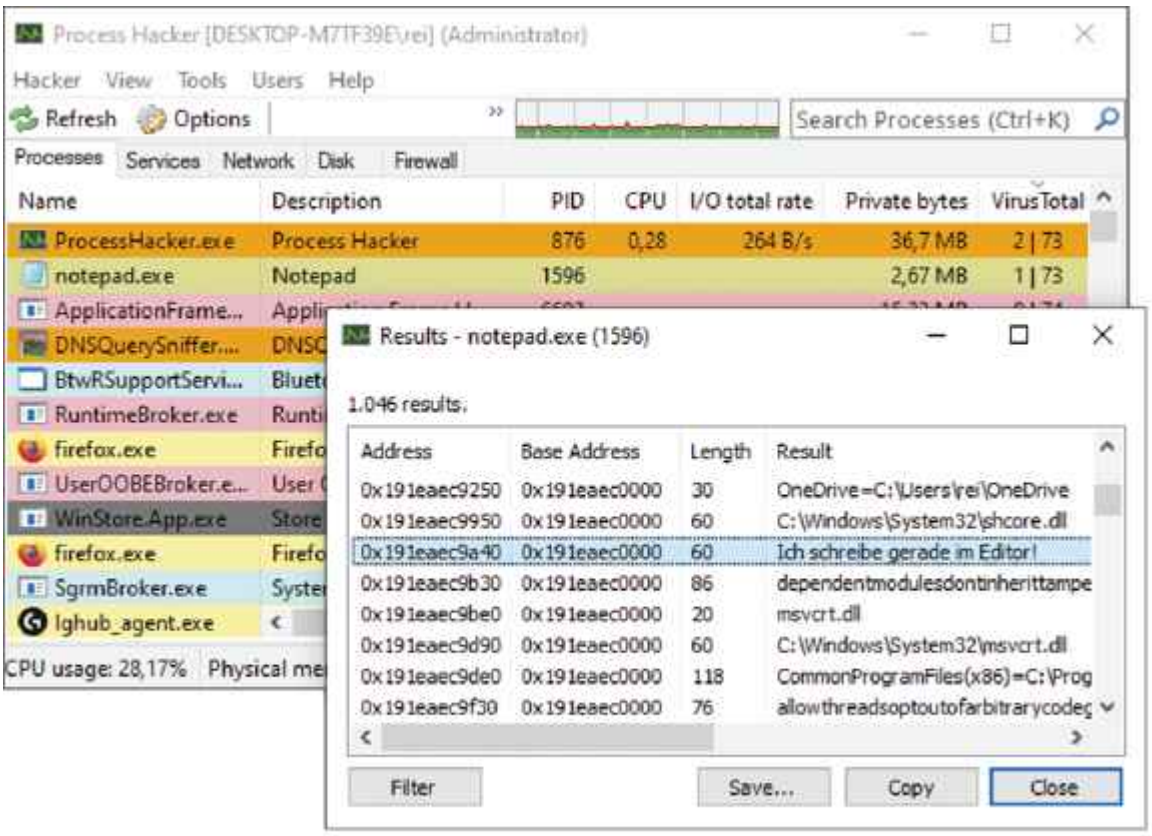
Sind Ihre Dateien noch zu retten? Mit PhotoRec finden Sie es heraus.

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.

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/y41x). 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).



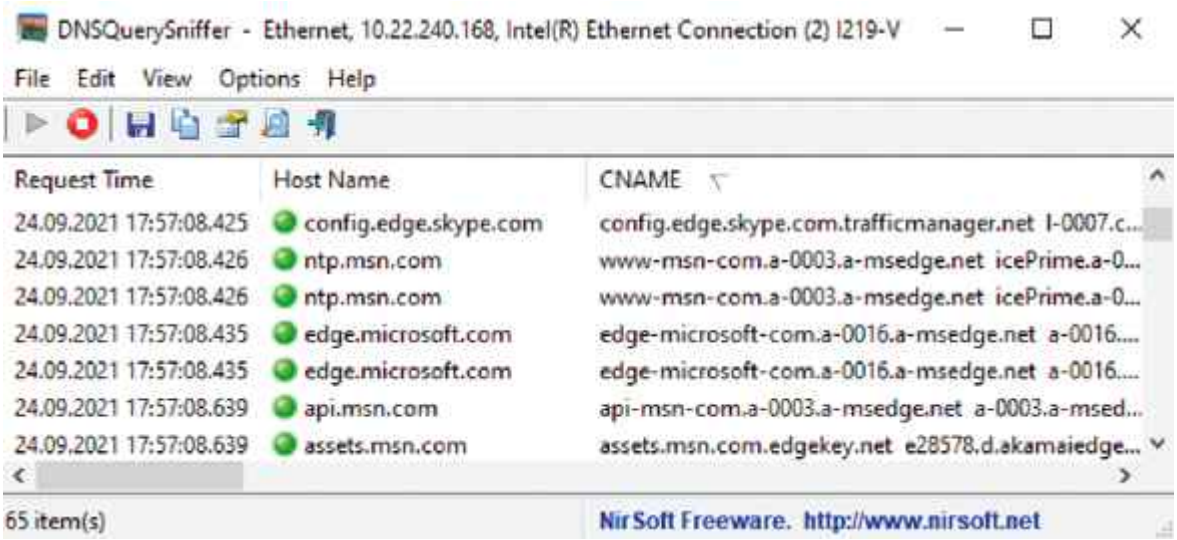
Der Process Hacker macht da weiter, wo andere Taskmanager aufhören: Das Tool erlaubt sogar Eingriffe in den Arbeitsspeicher der Prozesse.
Das Hauptfenster des Process Hacker ist in fünf Tabs unterteilt: „Processes“ zeigt, ähnlich wie der Taskmanager, Informationen über laufende Prozesse an und „Services“ 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) einsehen, 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.



DNS-Anfragen verraten viel über das Kommunikationsverhalten des Systems. DNSQueryView macht sie sichtbar.
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/y41x) 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 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 29). 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/y41x). 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@ct.de*)

Tools, Literaturhinweise: ct.de/y41x

Hacking-Tools

Hacking-Tools

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.

Die Werkzeuge der Hacker 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

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 170.

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 20. Haben Sie sich aus Ihrem Windows ausgesperrt, setzen Sie das Passwort mit dem **Windows Login Unlocker** einfach zurück. Auf Seite 18 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. 19) 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 22 zeigen wir außerdem, wie Sie vermeintlich unrettbar verlorene Dateien wieder ans Tageslicht befördern.

Security-Check

Ab Seite 24 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. 25) 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.

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

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 27.

Last, but not least, zeigen wir Ihnen ab Seite 30, 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 Herbsttage. (*rei@ct.de*)

So optimieren Sie leistungsschwache Inhalte

Lassen Sie nicht zu, dass veraltete oder glanzlose Inhalte Ihre SEO-Leistung beeinträchtigen. Erfahren Sie, wie Sie Content-Underperformer finden und wie Sie sie erneut optimieren können.

Julia McCoy am 5. Dezember 2022 um 8:00 Uhr | Lesezeit: 10 Minuten

Wenn Ihre Inhalte nicht so gut abschneiden, wie Sie es erwartet haben, oder alte Beiträge, die Sie vor einigen Jahren veröffentlicht haben, nicht mehr relevant sind oder an Bedeutung verlieren, ist es Zeit für ein Update.

Insbesondere ist es an der Zeit, Ihre leistungsschwachen Inhalte zu optimieren.

Dies ist der Prozess des Aktualisierens, Optimierens, Bearbeitens und Neuschreibens alter Inhalte, die keinen ROI bringen. Das Ziel ist es, den Inhalt zu verbessern, damit er schließlich beginnt:

- Ranking in der Suche.

- Gelesen werden.
- Engagement wie Shares oder Kommentare gewinnen.
- Conversions verdienen.

Häufig ist die Optimierung Ihrer leistungsschwachen Inhalte eine kostengünstige Methode, um Ihr Content-Marketing insgesamt zu verbessern. Durch die Optimierung müssen Sie nicht in die Erstellung völlig neuer Teile investieren – Sie können das, was Sie bereits haben, einfach umbauen und verbessern.

Es ist eine gute Praxis für jede Marke mit Inhalten (insbesondere als Teil eines Inhaltsaudits), da es sicherstellt, dass jedes Stück weiterhin auf Ihre Ziele hinarbeitet (anstatt sie zu behindern).

Zuerst müssen Sie Ihre leistungsschwachen Inhalte identifizieren – welche Teile ihr Potenzial nicht ausschöpfen – und dann Maßnahmen ergreifen, um sie zu verbessern und zu optimieren.

So erkennen Sie leistungsschwache Inhalte

Woher wissen Sie, welche Inhalte unterdurchschnittlich abschneiden?

Sie müssen sich bestimmte Metriken ansehen, um sie zu finden.

Verwenden Sie Tools wie Google Analytics, Semrush oder Ahrefs, um sich diese Daten anzusehen und Ihre leistungsschwachen Inhalte zu finden.

Messwerte für das Suchranking:

- Organische Keywords
- Durchschnittliche Position

Um Inhalte zu identifizieren, die in den Suchergebnissen unterdurchschnittlich abschneiden, sehen Sie sich Ihre organischen Keyword-Statistiken an, insbesondere die durchschnittliche Position Ihrer Inhalte in Google. Beachten:

- Alles, was auf Platz 5-10 steht: Eine weitere Optimierung könnte möglicherweise zu höheren Rankings führen.
- Alles, was auf Platz 11 und darunter rangiert: Wenn Sie diese weiter optimieren oder neu schreiben, können Sie je nach Keyword möglicherweise Seite 1 erreichen.

Traffic- und Engagement-Metriken:

- Seitenaufrufe
- Sitzungen
- Absprungrate
- Zeit auf Seite
- Soziale Anteile
- Kommentare

Welche Seiten verlieren Traffic?

Welche Seiten erhalten wenig bis gar kein Engagement (d. h. die Leute verbringen nicht genug Zeit auf der Seite, um den Inhalt zu lesen)?

Dies sind großartige Kandidaten für die Optimierung.

7 Fragen zur Optimierung leistungsschwacher Inhalte

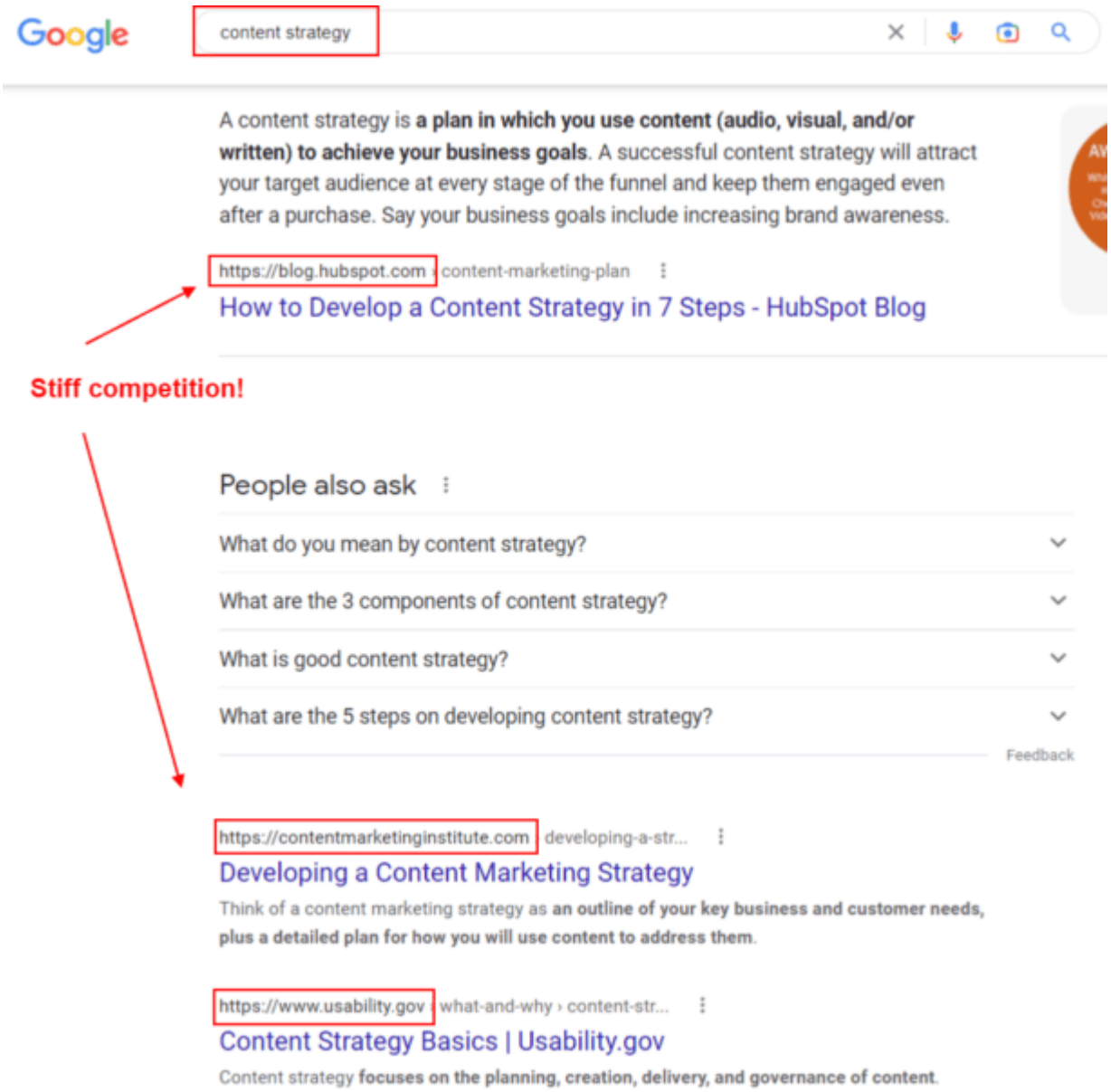
Nachdem Sie Ihre leistungsschwachen Inhalte gefunden haben, die für eine Optimierung am wichtigsten sind, stellen Sie sich die folgenden Fragen, um zu verstehen, wie Sie sie beheben können.

1. Sind die Keywords, auf die Sie abzielen, tatsächlich gewinnbar?

Wenn Ihr Inhalt keine Leistung bringt, überlegen Sie zunächst, ob das Keyword, auf das Sie abzielen, tatsächlich für Ihre Marke gewinnbar ist.

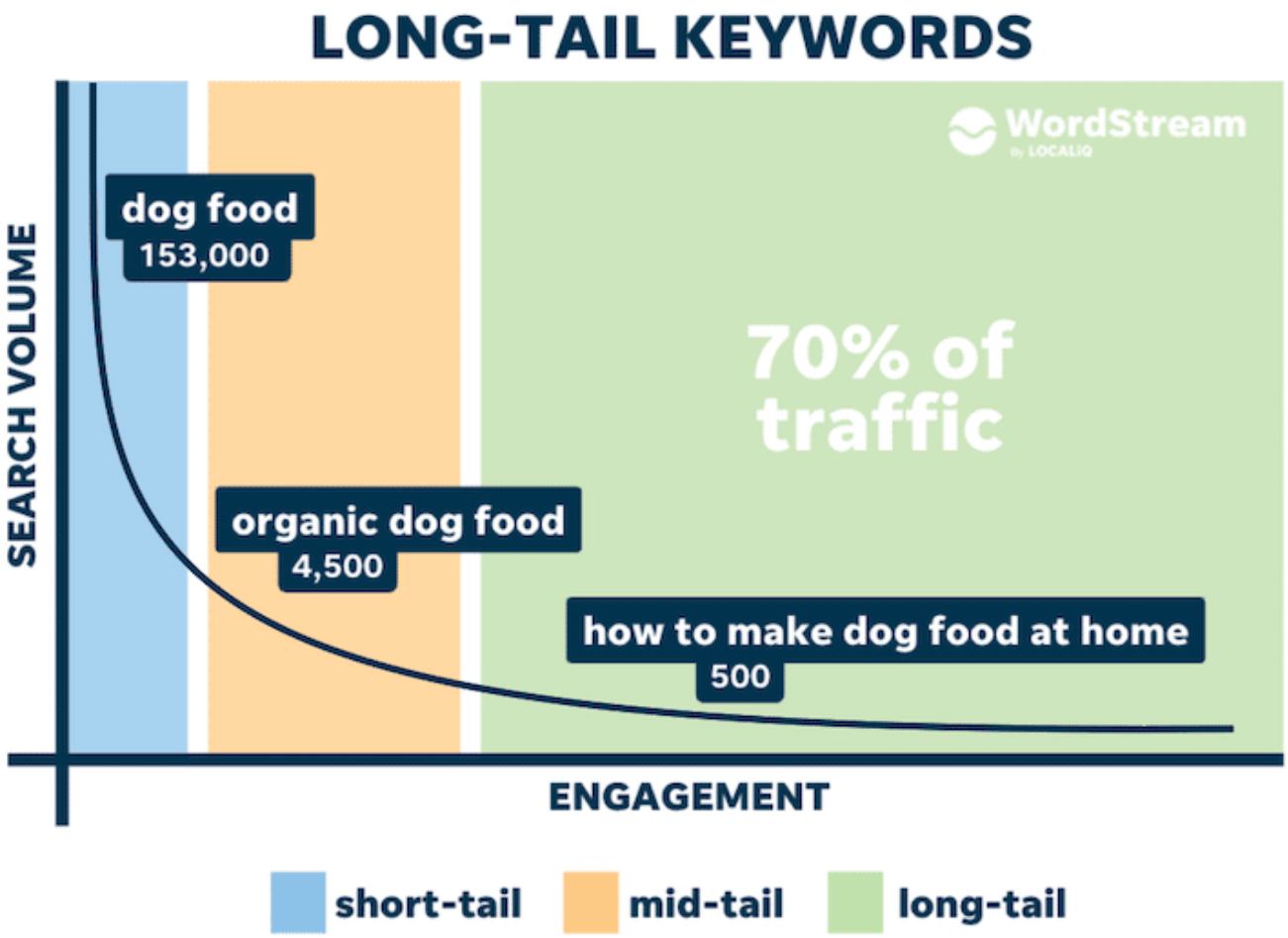
Wenn Sie beispielsweise in einem Artikel auf das Keyword „Content-Strategie“ abgezielt haben und es auf Seite 5 der Suchergebnisse vor sich hin dümpelt, könnte dies auf zwei Faktoren zurückzuführen sein:

- Sie sind eine kleine oder neue Marke, die immer noch Online-Autorität aufbaut.
- Der Wettbewerb um „Content-Strategie“ ist unglaublich hart, mit bekannten, maßgeblichen Namen wie HubSpot, Content Marketing Institute und sogar der US-Regierung, die an der Spitze von Google stehen.



Harter Wettbewerb in den SERPs um die Suchanfrage „Content Strategy“
Es ist zweifelhaft, ob eine neue Website oder Website mit geringer Autorität die Top-10-Ergebnisse für dieses Keyword knacken könnte.

Wenn dies der Fall ist, sollten Sie die Keywords wechseln, um darauf abzuzielen, was Sie tatsächlich gewinnen können. Besonders für neuere oder kleinere Marken sind Long-Tail-Keywords in der Regel einfacher zu ranken. Sie generieren auch [70 % des gesamten Verkehrs](#) .



Anstatt beispielsweise auf „Content-Strategie“ abzuzielen, versuchen Sie es mit „Content-Strategie für Anfänger“ oder „Content-Marketing-Strategie für SEO“.

Long-Tail ist im Allgemeinen eine Win-Win-Situation, da diese Keywords spezifischer sind und Suchende mit spezifischeren Absichten ansprechen.

Diese Suchenden sind möglicherweise auch eher bereit zu konvertieren, weil sie aktiv nach Lösungen suchen – und nicht nur surfen.

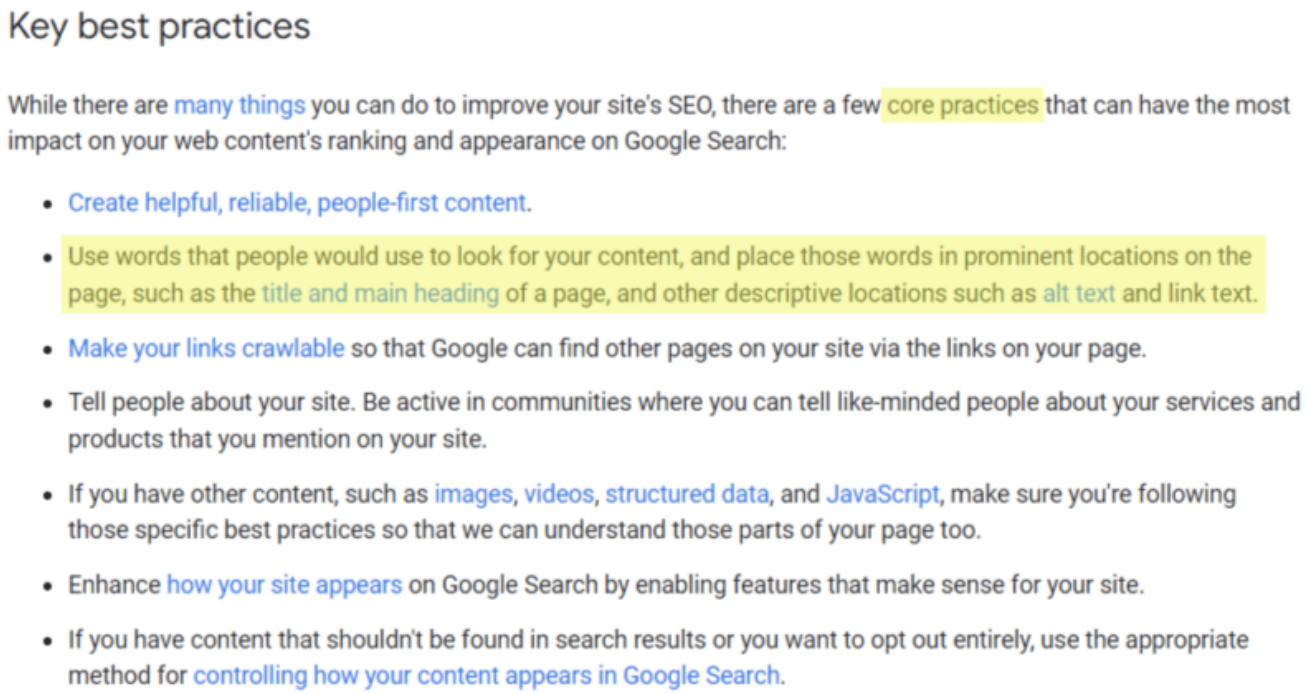
2. Haben Sie den Inhalt mit genügend Keywords an strategischen Stellen optimiert?

Wenn ein Artikel bereits gut geschrieben und für ein gewinnbares Keyword optimiert ist, überlegen Sie, ob er

ausreichend optimiert ist .

Google hat angegeben , dass die wichtigsten Best Practices zur Verbesserung Ihrer SEO Folgendes umfassen:

- Verwenden **Sie die richtigen Wörter** , mit denen die Leute nach Ihren Inhalten suchen würden.
- **Platzieren Sie** die richtigen Wörter **an prominenten Stellen** auf der Seite.



Key best practices

While there are many things you can do to improve your site's SEO, there are a few core practices that can have the most impact on your web content's ranking and appearance on Google Search:

- Create helpful, reliable, people-first content.
- Use words that people would use to look for your content, and place those words in prominent locations on the page, such as the title and main heading of a page, and other descriptive locations such as alt text and link text.
- Make your links crawlable so that Google can find other pages on your site via the links on your page.
- Tell people about your site. Be active in communities where you can tell like-minded people about your services and products that you mention on your site.
- If you have other content, such as images, videos, structured data, and JavaScript, make sure you're following those specific best practices so that we can understand those parts of your page too.
- Enhance how your site appears on Google Search by enabling features that make sense for your site.
- If you have content that shouldn't be found in search results or you want to opt out entirely, use the appropriate method for controlling how your content appears in Google Search.

Die Platzierung und Verwendung von Schlüsselwörtern ist entscheidend dafür, wie gut Sie in der Suche ranken.

Wenn Sie Google nicht genügend Signale gegeben haben, die sagen: „Hey! Dieses Stichwort ist Fokus und Thema dieser Seite!“ es wird das Memo nicht bekommen.

Einige Tipps zur Keyword-Nutzung und -Platzierung in Ihren Inhalten:

- Fügen Sie Ihr **Fokus-Keyword** an **all diesen Stellen ein:** für eine ideale Optimierung
    - In der H1-Überschrift (auch bekannt als

Seitentitel).
    - Im Meta-Titel und in der Beschreibung, idealerweise am Anfang von beiden.
    - Im ersten Absatz.
    - In mindestens einer der H2-Überschriften.
    - In mindestens einer der H3-Überschriften.
    - Auf natürliche Weise im gesamten Fließtext eingestreut.
    - Alt-Text im Inneren des Bildes (für Bilder, die auf der Seite erscheinen).

- Fügen **Sie an diesen Stellen Synonyme und Variationen** Ihres Fokus-Keywords ein:
    - In mindestens einem H2 (je nachdem, wie viele im Inhalt vorkommen).
    - In mindestens einem H3 (wie oben).
    - Natürlich im gesamten Inhalt bestreut.
    - Alt-Text im Inneren des Bildes.

- **Nie Keyword-Sachen** . Versuchen Sie immer, Schlüsselwörter hinzuzufügen, die beschreibend und hilfreich für die Leser sind.
- Strukturieren und organisieren Sie Ihre Inhalte immer mit Keyword-optimierten Überschriften. Diese machen es besser scanbar und damit leichter zu lesen. Überschriften geben Suchmaschinen auch entscheidende Hinweise auf Ihre Seite und ob Ihre Inhalte für die Suchanfrage relevant sind.

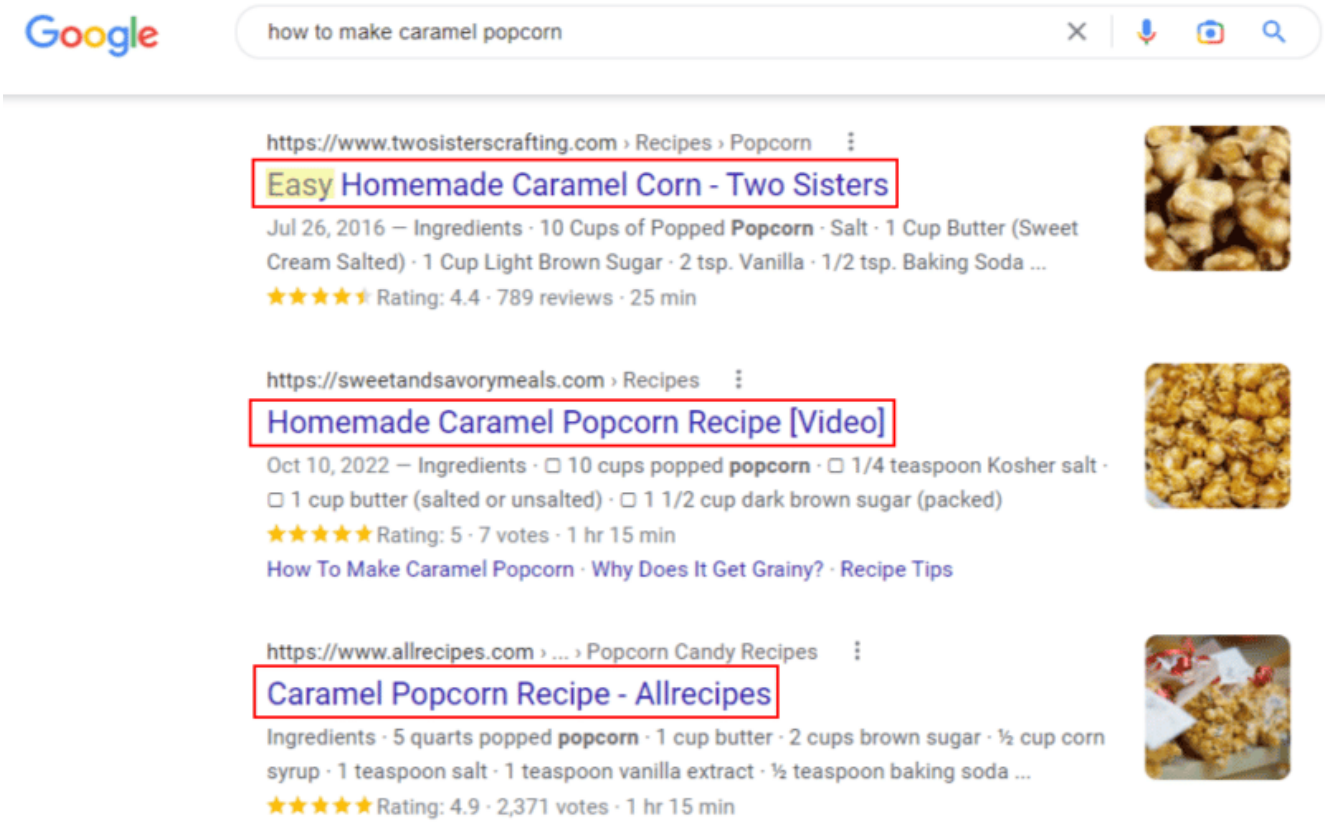
---

3. Sind Ihre Überschriften, Unterüberschriften, Metatitel und Metabeschreibungen stark genug?

Viele Leute übersehen kleine Details (z. B. das Schreiben eines soliden Meta-Titels und einer Beschreibung oder das Erstellen starker, beschreibender Überschriften). Und das ist ein Fehler.

Diese kleinen Stücke leisten viel Arbeit. Der Meta-Titel allein kann Suchende dazu verleiten, Ihren Link unter sehr ähnlichen Ergebnissen anzuklicken – insbesondere, wenn Ihr Link durchdachter oder aussagekräftiger ist als die anderen Optionen.

Wenn ich zum Beispiel in Google nach „wie man Karamell-Popcorn macht“ suche, sind die Ergebnisse fast identisch. Allerdings erwähnt nur einer „einfach“ in seinem Meta-Titel. Das ist genug Unterscheidungsmerkmal, um mich dazu zu bringen, darauf klicken zu wollen.



Nehmen Sie sich vor diesem Hintergrund die Zeit, aussagekräftige Metatitel, Beschreibungen und Überschriften für Ihre leistungsschwachen Inhalte zu erstellen.

Diese Elemente können die Neugier oder das Interesse Ihrer Leser wecken und sie weiter in das Stück hineinziehen, was sich positiv auf seine Leistung auswirken kann.

Einige Tipps:

- **Lengthen your headings.** Longer headings and sub-headings are more descriptive, more creative and engaging, and are prime spots to include keywords.
- **Think of headings and metas as hooks**. Your headings can do much more than just split your content into sections. They can also serve as little hooks that pull your reader down the page. The same goes for your meta description – it can act as a hook that grabs the reader and makes them want to click your link in the search results.
- **Speak to the reader.** So, what makes a good hook? Speak

directly to your reader. Imagine they're sitting across from you; address them. Address their concerns. Make their lives better.

- **Learn to write good headlines**. If you're shaky about crafting any of these pieces, first learn to write a solid headline. That knowledge can be applied to writing metas and headings, too. This article by Brian Clark of Copyblogger is a great place to start.

4. Are your statistics, facts, or links outdated?

This is one of the easiest ways to optimize underperforming content. Make sure it's up-to-date and relevant to modern readers!

For example, are the statistics cited in the content from 2016 or earlier? That's too old, especially since companies usually update studies (or conduct new ones) every few years.

A good rule of thumb: If the statistics in your content are more than five years old, find new ones **unless** the stat is ground-breaking or foundational in your industry.

If a statistic comes from a unique study that hasn't been updated or replicated, then it should be OK to cite it.

Als nächstes, was ist mit den Links? Sind die Links, die auf andere Websites und Ressourcen verweisen, noch relevant? Zeigen sie auf die richtigen Seiten (und sind die Seiten noch da)? Sind die Links hochwertig und verbindlich? Wenn nicht, aktualisieren.

Überprüfen Sie abschließend Ihre Inhalte auf Relevanz. Wenn beispielsweise das Jahr 2020 mehrmals in einem ansonsten immergrünen Blog erwähnt wird, aktualisieren Sie diese Verweise, damit sie aktuell sind.

5. Ist die Inhaltsqualität auf dem neuesten Stand?

Angenommen, der Inhalt, den Sie optimieren, ist relativ kurz und dünn, obwohl Sie erwarten würden, dass er umfangreicher ist.

Vielleicht spricht das Stück das Thema, das es zu behandeln versucht, nicht vollständig an, oder es vertieft sich in Irrelevanzen.

Vielleicht erfordert das Thema unterstützende Statistiken oder Daten, die helfen, dem Stück Gewicht zu verleihen, aber es hat keine.

Oder vielleicht hat es ein paar Rechtschreib- oder Grammatikfehler oder es hat keine Bilder.

Diese Probleme beziehen sich alle auf die **Inhaltsqualität** – wie hilfreich , relevant, genau und informativ/unterhaltsam/stärkend der Inhalt für Ihr spezielles Publikum ist.

Glücklicherweise verbessern in all diesen Szenarien ein paar Updates die Qualität, ohne dass eine vollständige Neufassung erforderlich ist. Zum Beispiel:

- Ergänzen Sie das Stück mit zusätzlichen Informationen, um es umfassender und nützlicher zu machen.
- Kürzen Sie irrelevante Abschnitte und fügen Sie bessere Informationen hinzu, die für die Anliegen Ihres Publikums relevanter sind.
- Finden Sie einige relevante Bilder, die Sie dem Inhalt hinzufügen können, um das Engagement zu erhöhen.

6. Muss der Inhalt komplett neu geschrieben werden?

Manchmal können Sie Inhalte von schlechter Qualität nicht speichern.

Stattdessen müssen einige Teile möglicherweise vollständig überholt werden. Das bedeutet, dass Sie alles löschen und von vorne beginnen.

Woher wissen Sie, wann Ihre Inhalte komplett neu geschrieben werden müssen?

- Es ist schlecht geschrieben, ohne Struktur (sprich: Überschriften) oder logischen Fluss.
- Es verfehlt völlig den Punkt des Themas und was die Leser suchen, wenn sie danach suchen.
- Es konzentriert sich auf die Marke und nicht auf das Publikum der Marke.
- Es konzentriert sich auf ein Ereignis oder Datum, das schon lange vergangen ist.
- Das gezielte Keyword ist für die Marke immer noch gewinnbar und ist die Investition/den Aufwand des Umschreibens wert.

7. Do you have site issues hindering readability or crawling?

Finally, don’t forget to zoom out to look at the bigger picture when you’re optimizing underperforming content.

Your site may be contributing to your content’s poor performance in a few ways.

- Readers are having a hard time viewing your site as a whole.

- Search engines can’t crawl it to index it.

For example, if your site loads extremely slowly, that can affect your rankings and engagement. People won’t wait to read a webpage that doesn’t load quickly.

Or, maybe your site isn’t optimized for mobile browsing, so people trying to access your content on smartphone browsers can’t even read it.

A poor site design can interfere with its readability as well. Make sure there’s enough contrast between the text on your page and the background for comfortable reading.

Avoid long paragraphs, too – those are hard on the eyes when reading from a screen.

Stellen Sie zu guter Letzt sicher, dass Google und andere Suchmaschinen crawlen können, um sie zu indizieren. Ihre Seiten

Manchmal kann ein dummer Fehler unter der Oberfläche lauern, wie z. B. ein „noindex“-Tag, das versehentlich in den Code für einen Ihrer Blogs eingefügt wurde („noindex“ weist Suchmaschinen an, die Seite nicht in die Ergebnisse aufzunehmen).

Optimieren Sie leistungsschwache Inhalte und verbessern Sie Ihren ROI

Die Optimierung Ihrer glanzlosen Inhalte ist eine großartige Möglichkeit, den größtmöglichen ROI daraus zu ziehen.

Jeder Inhalt erfordert eine gewisse Investition (der Aufwand, das Geld und die Zeit, die für die Erstellung aufgewendet werden). Wenn Sie sich die Zeit nehmen, es zu optimieren und

zu aktualisieren, werden Sie diese Investition weiter ausdehnen.

Besser noch, Content, der anfängt zu performen, wird kräftigere positive Renditen bringen.

Das bedeutet, dass Sie mehr Langlebigkeit aus Ihren Content-Assets ziehen, und sie werden auch in Zukunft leistungsfähig sein, um passiven Traffic, Leads und Conversions zu generieren.

Es ist wichtig, den Optimierungsprozess im Rahmen Ihrer Content-Strategie regelmäßig zu wiederholen , um die besten Ergebnisse zu erzielen. Dadurch wird sichergestellt, dass alle Ihre Inhalte weiter funktionieren, um Ihre Ziele zu erreichen .

Reihenfolge von Blog-Beiträgen ändern

WordPress Beiträge sortieren & Reihenfolge im Blog ändern

Du magst die Reihenfolge deiner Blogbeiträge im WordPress nicht? Dann ändere sie doch einfach mit unserem WordPress Tutorial.

Diese Tipps helfen dir deinen Blog

neu zu strukturieren

Wir kennen es selbst, die Reihenfolge der Blogbeiträge macht uns nicht richtig zufrieden: Die Themen passen nicht immer zusammen, der eine Beitrag ist aktueller als der andere oder der optische Eindruck sieht nicht perfekt aus. Bei WordPress werden die Blogbeiträge in umgekehrter chronologischer Reihenfolge angezeigt – der neueste Beitrag erscheint ganz oben, während der älteste Beitrag ganz unten bzw. hinten erscheint. Rückblickend kann das aber nicht für jeden die langfristig beste Lösung sein. Deswegen haben wir uns einmal genauer angeschaut, wie du deinen Blog neu strukturieren kannst.

Inhaltsverzeichnis

1. Die Reihenfolge der Blogbeiträge in WordPress ändern – wann das für dich Sinn macht

Die Reihenfolge der Blogbeiträge zu verändern oder anzupassen kann insbesondere dann sinnvoll sein, wenn du bereits eine Vielzahl an unterschiedlichen Beiträgen veröffentlicht hast. Das betrifft vor allem oft Blogger oder beispielsweise journalistische Webseiten – aber auch uns.

Gerade wenn alte Beiträge durch aktuelle Entwicklungen wieder relevant werden oder wenn du besonders relevante/ qualitativ hochwertige Beiträge prominent für die Besucher deiner

Webseite aufbereiten möchtest, sollten diese Beiträge eher an der Spitze des Blogs stehen. Dadurch bekommen diese mehr Aufmerksamkeit und werden besser zu sog. „Evergreen“ Beiträgen.

TIPP

Natürlich macht es zunächst einmal Sinn, sich ein klares Konzept für die Strukturierung eines Blogs zu überlegen und beispielsweise verschiedene thematische Kategorien in deinem WordPress anzulegen. So kann jeder Artikel einem thematischen Schwerpunkt zugeordnet werden, wodurch die Masse an Beiträgen in den einzelnen Kategorien erst einmal vorsortiert und thematisch übersichtlicher wird. Trotzdem empfiehlt es sich insbesondere für die voreingestellte Kategorie „Allgemein“ deine Reihenfolge noch einmal zu perfektionieren.

Bei speziellen Fragen rund um WordPress Beiträge kann dir eventuell auch die WordPress Community helfen.

2. Das Beitragsdatum in WordPress ändern

Die einfachste und schnellste Methode deine Beiträge neu zu sortieren, ist das Beitragsdatum zu verändern. Der Vorteil dieser Methode ist es, dass du kein Plugin installieren oder über besonders viel technisches Know-How verfügen musst.

Ursächlich für die Platzierung des Beitrags bei WordPress ist nämlich das Beitragsdatum. Wenn du also das Beitragsdatum änderst, ändert sich auch die Position deines Blogbeitrags. Wenn du einen älteren Blogpost – beispielsweise von 2020 – auf den Anfang deines Blogs verschieben möchtest, musst du das Datum des Beitrags einfach auf einen aktuelleren Tag legen,

zum Beispiel auf den 19.10.2022. Gleiches gilt natürlich auch umgekehrt, sofern du einen Beitrag auf deinem Blog weiter nach hinten verschieben möchtest.

Der Nachteil daran ist allerdings, dass das Datum auch für die Aktualität der Inhalte spricht. Das bedeutet, du solltest unbedingt darauf achten, dass die inhaltlichen Themen entweder angepasst werden oder natürlich längerfristig gültig sind. Das könnte sonst bei deinen Lesern zu Verwirrungen sorgen.

‼️Aber Achtung

Achte darauf, dass Datum deiner Beiträge nicht in die Zukunft zu legen. Dadurch werden die Beiträge von WordPress automatisch auf „geplant“ umgestellt und bis zu diesem Termin privatisiert. Das bedeutet, der Beitrag ist bis zu dem neuen Veröffentlichungsdatum nicht öffentlich einsehbar.

Diese Funktion kannst du aber natürlich auch bewusst benutzen.

Um das Beitragsdatum umzustellen klickst du in deinem WordPress Backend zunächst auf den gewünschten Beitrag. Dort findest du in deiner rechten Leiste verschiedene Felder. In dem **Feld „Veröffentlichen“** klickst du anschließend hinter dem Datum auf **„Bearbeiten“.** Hier kannst du jetzt dein gewünschtes Datum neu einstellen.

Möchtest du den Beitrag ganz an den Anfang deines Blogs verschieben, datierst du den Beitrag auf den aktuellen Tag. Du möchtest den Beitrag vielleicht lieber zwischen zwei bestehenden Artikeln einsortieren? Dann wähle ein Datum oder auch eine Uhrzeit zwischen zwei Beiträgen. Somit kannst du die genaue Position im Blog festlegen. Vergiss aber nicht, den Beitrag zu aktualisieren.

3. Das Plugin Post Types Order

Wenn du die Reihenfolge deiner Blogbeiträge bei WordPress

ändern möchtest, ohne das Datum der Beiträge zu verändern, kannst du auf die Hilfe des Plugins „Post Types Order“ zurückgreifen. Dieses kannst du übrigens kostenlos bei WordPress herunterladen. Mit Hilfe des Plugins wird es dir ganz einfach gemacht, die Beiträge hin und her an einen neuen Platz zu ziehen. Das löst wiederum das Problem, dass deine Leser aufgrund des Datums und der inhaltlichen Aktualität nicht verwirrt werden.

Das Plugin „Post Types Order“ installieren und aktivieren

Das Plugin kannst du erst einmal wie gewohnt herunterladen und installieren. Falls du dir nicht sicher bist, wie du vorgehen musst, erklären wir dir in unserem Beitrag „Plugins suchen und installieren“ Schritt für Schritt den Einrichtungsprozess.

Neue Einstellungen auswählen

Nachdem du das Plugin nun installiert hast, klickst du im WordPress Dashboard in der linken Spalte auf **„Einstellungen“** und anschließend auf das Plugin „Post Types Order“. In den Einstellungen des Plugins kannst du jetzt genau auswählen, für welche Arten von WordPress Blogposts das Plugin aktiviert werden soll. Auch hier darfst du nicht vergessen deine Änderungen zu speichern.

TIPP

Beim installieren neuer Plugins empfehlen wir dir vorher ein Backup deiner Webseite zu erstellen. So bist du auf der sicheren Seite, falls es Probleme bei der Installation gibt. Hilfestellungen und Informationen zur Erstellung von Backups findest du in unserem Beitrag „WordPress Backup Plugins im Vergleich“.

Hier kannst du einstellen, wie du deine Blogbeiträge sortieren möchtest und wie die Oberfläche angezeigt wird.

Die Reihenfolge der WordPress Blogbeiträge ändern

Wenn du nun auf deine Beiträge-Seite im Dashboard gehst, kannst du ab sofort ganz einfach die Reihenfolge der Beiträge neu strukturieren und verändern. Das funktioniert über die Drag and Drop Funktion, wie du auch in unserem Gif nachvollziehen kannst. Und mehr braucht es auch gar nicht! Ab sofort hast du also mehrere Möglichkeiten deine Beiträge zu ordnen, zu sortieren und so oft du willst zu verschieben.

4. Fazit

Die Reihenfolge von Blogbeiträgen zu ändern ist an sich gar nicht schwer. Vor allem da es dazu überhaupt keine technischen Vorkenntnisse benötigt und das jeder selbst übernehmen kann. Wir finden die Kombination aus Plugin und Datum einfach super, da die Drag and Drop Funktion bei WordPress selbst leider fehlt. Die Beiträge neu zu sortieren kann vor allem aber auch bei der Überarbeitung von Beiträgen hilfreich sein, um diese im Backend nicht immer suchen zu müssen.

Von uns also einen klaren Daumen hoch für diesen kleinen aber feinen Hack. □□

Gender-Wahnsinn

Der/die Bürger:innenmeister:innenkandidat:innenanwärter:innen?

Gendern ist ein heißes Thema, bei dem oft zwei Welten aufeinander prallen. Die einen möchten künftig mehr auch die weibliche Form betonen, das andere Lager weist darauf hin, dass Sprache mit Sternchen, Doppelpunkten oder Großbuchstaben mitten im Wort schwerer wird. Die Argumente und die Absichten beider Seiten sind durchaus verständlich und nachvollziehbar.

Als Online-Verantwortlicher hat man aber durchaus mehrere Aspekte zu berücksichtigen – unabhängig von der eigenen Einstellung zu Genderschreibweisen.

Ist Text schwerer zu lesen und sinkt damit die Motivation, Content auf Webseiten zu konsumieren? Die Wissenschaft sagt hierzu recht eindeutig Ja. Wer sich mit dem Vorgang des Lesens und dem Zusammenspiel von Auge und Gehirn beschäftigt hat, kann das leicht nachvollziehen. Das Auge fixiert jeweils nur zwei bis drei Buchstaben, dann springt es (Sakkade genannt) fünf bis sechs Buchstaben weiter und nimmt dann erneut wieder nur wenige Buchstaben wahr. In der Sakkade, also beim Sprung mit dem Blickfokus, sind wir „blind“, d. h., die übersprungenen Buchstaben erkennen wir nicht. Vereinfacht erklärt entstehen im Kopf beim schnellen Lesen nur Muster von Wörtern, die mit den bekannten/gelernten Wörtern abgeglichen werden. Stoßen wir auf komplizierte oder unbekannte Wörter, springt das Auge nach einer Sakkade wieder ein paar Buchstaben zurück und macht die Sprünge damit kleiner, häufiger – und das kostet Energie und Zeit. Ein Beispiel:

BEREITS EIN SATZ MIT GROSSBUCHSTABEN ZEIGT, DASS MAN DIESEN NUR SEHR VIEL SCHWIERIGER ERFASSEN KANN, WEIL DIE MUSTER UNGEWOHNT SIND. Und noch mal normal:

Bereits ein Satz mit Großbuchstaben zeigt, dass man diese sehr

viel schwieriger erfassen kann, weil die Muster ungewohnt sind.

Welcher Text ist schneller lesbar, weil er den gelernten Mustern entspricht? Wenn Sie liebe(r) Leser(in) nun bedenken, dass BesucherInnen und potenzielle Kund*innen Ihrer Website häufiger beim Lesen stolpern, länger brauchen und wahrscheinlich deswegen früher abbrechen, weil es anstrengend(er) ist – ist das zielführend für Sie?

Ein weiterer Umstand ist, dass Google bisher noch Probleme hat, die neuen Worte zu verstehen. Der/die Zahnärzt/-innen ist für die Maschine etwas anderes als ein Zahnarzt oder eine Zahnärztin. Demensprechend kann es sein, dass man sich selbst für wichtige Suchbegriffe aus dem Ranking kegelt.

Natürlich gibt es noch einige weitere Dinge zu bedenken. Nehmen es mir z. B. Menschen übel, wenn ich im Text nicht gendere? Und kaufen womöglich nicht? Und was, wenn es dazu gar nicht kommt, weil sie mich nicht (mehr) bei Google finden? Oder: Jeder zehnte Mensch in Deutschland hat eine mehr oder weniger große Leseschwäche oder kann die deutsche Sprache nicht gut. Wie kommt diese Gruppe mit all den Sternchen, Schrägstrichen und Doppelpunkten zurecht?

Alle Gender-Schreibweisen auf einen Blick

Beim Gendern gibt es unterschiedliche Möglichkeiten, weibliche, männliche sowie nicht-binäre Personen anzusprechen:

- **Doppelnennung:** Immobilienmaklerinnen und Immobilienmakler – die Doppelnennung findet sich aktuell häufig in Anreden oder Begrüßungen. Weibliche und männliche Personen werden angesprochen.
- **Binnen-I:** Das Binnen-I soll die Doppelnennung vereinfachen und bezieht weibliche und männliche Personen ein.

Gender-Formen, die sowohl weibliche, männliche als auch nicht-binäre Personen ansprechen:

- **Gender-Sternchen und Gender-Star:** Immobilienmakler*innen
- **Gender_Gap mit Unterstrich:** Immobilienmakler_innen
- **Der Doppelpunkt:** Immobilienmakler:innen
- **Der Schrägstrich:** Immobilienmakler/innen

Eine Alternativ zur Verwendung von Gender-Schreibweisen sind geschlechtsneutrale Sprache sowie neutrale Formulierungen. Bei geschlechtsneutraler Sprache wird häufig ein Plural bekannter Begriffe gebildet, wie z. B. Studierende oder Mitarbeitende. Es findet sich jedoch nicht immer ein passender Plural für jeden Begriff.

Alternativ können auch neutrale Formulieren verwendet werden:

- Alle, niemand, jemand
- Personen, Lehrkraft, Vertretung

Gendern & SEO: Verträgt sich das?

Um in Suchmaschinen prominente Positionen einzunehmen, werden Webseiten häufig auf das generische Maskulinum optimiert. Wie bereits erwähnt, ist dies auf das hohe Suchvolumen dieser Begriffe zurückzuführen. Wer in Texten trotzdem alle Geschlechter ansprechen möchte, hat folgende Möglichkeiten:

- **Doppelnennung:** Aus SEO-Sicht eignet sich diese Gender-Form bei personenbezogenen Keywords. Durch die Verwendung männlicher und weiblicher Begriffe lässt sich das Suchvolumen der Begriffe sozusagen kombinieren, was das Ranking positiv beeinflussen kann. Nachteil: Texte werden hierdurch jedoch deutlich länger.
- **Der Doppelpunkt:** Hier werden weibliche, männliche und nicht-binäre Personen angesprochen. Suchmaschinen können

sowohl die männliche als weibliche Form des Begriffs erkennen. Die Interpretation durch Google ist ähnlich wie bei der Doppelnennung. Nachteil: Diese Variante funktioniert jedoch nicht für jeden Begriff, z.B. Kund:in.
- **Geschlechtsneutrale Sprache:** Handelt es sich um nicht-personenbezogene Keywords bieten sich geschlechtsneutrale Sprache und neutrale Formulierungen an. Diese Gender-Form gewährleistet, dass sich alle Personen angesprochen fühlen.

Es gibt jedoch auch Gender-Formen, mit denen Suchmaschinen weniger umgehen können. Gendersternchen, Gender_Gap und Binnen-I bereiten der Suchmaschine Google eher Schwierigkeiten und können Rankings negativ beeinflussen.

Gendern oder nicht? Die Checkliste für gendersensible Online-Texte

Gendersensible Sprache beginnt schon vor der Formulierung von Online-Texten. Bereits in Recherche und Planung von Texten wie auch Projekten sollte die Zielgruppe beachtet werden. Mit folgenden Tipps lässt sich die redaktionelle Arbeit geschlechtersensibel gestalten:

Recherche & Konzeption

- Wer gehört zur **Zielgruppe**? Werden Männer, Frauen und/oder nicht-binäre Personen angesprochen?
- Wie liest sich der Text? Verändern sich **Thema und Sichtweise** je nach Geschlecht?
- Wer soll in Interviews Expertenwissen äußern?

Texterstellung & -gestaltung

- Wie soll gegendert werden? Welche Form passt zur

Zielgruppe?
- Gibt es personenbezogene Keywords? Lässt sich das generische Maskulinum vermeiden?
- Werden Rollenklischees in Text und Bild reproduziert? Wie lässt sich das vermeiden?
- Ist der Text trotz gendersensibler Formulierungen verständlich und gut lesbar?

Fazit: Gendern in Online-Texten

Gendergerechte Sprache in Online-Texten spricht alle an! Neben der Vorbildfunktion besitzt Sprache auch eine Wirkung. Wer männliche, weibliche und nicht-binäre Personen in Texten sichtbar macht, vergrößert die eigene Zielgruppe und erreicht dadurch mehr potenzielle Kunden.

In unserer Online Marketing Agentur achten wir auf einen sensiblen Umgang mit Sprache und beraten unsere Kunden hinsichtlich der verschiedenen Möglichkeiten. Dabei stehen Lesbarkeit, Suchmaschinenoptimierung und Verständlichkeit der Texte im Vordergrund. Gemeinsam gehen wir den Weg in eine gleichberechtigte Zukunft.

Bei der Wahl eines komplett inklusiven Schriftbildes für deine Texte empfehlen wir ganz klar das **Gendern mit Doppelpunkt**. Google interpretiert Grafiker:in sowohl als Grafikerin als auch Grafiker. Grafiker_in wird hingegen sehr häufig als die weibliche Form gelesen und die Variante mit Gender-Sternchen führt häufig zur Kategorisierung als männliche Schreibweise.

	Inklusivität			Ranking		
Schreibweise	**m**	**w**	**d**	**m**	**w**	**d**
Grafiker	✓	X	X	✓	X	X
Grafikerin	X	✓	X	X	✓	X
GrafikerIn	✓	✓	X	X	✓	X
Grafiker/in	✓	✓	X	✓	X	✓
Grafiker und Grafikerin	✓	✓	X	✓	✓	X
Grafiker:in	✓	✓	✓	✓	✓	✓
Grafiker_in	✓	✓	✓	X	✓	✓
Grafiker*in	✓	✓	✓	✓	X	✓

Genderschreibweisen und ihre Rankingwahrscheinllichkeit

Der Klickstream Tipp

Um einerseits die Integration aller Geschlechter zu gewährleisten und andererseits keine Rankingnachteile bei Google und anderen Suchmaschinen zu erhalten, empfehlen wir das **Gendern mit Doppelpunkt**. Diese Schreibweise beinhaltet für Google sowohl das feminine als auch maskuline Geschlecht. Zudem werden durch die Inklusivität keine weiteren Geschlechtervarianten ausgeschlossen. Allerdings hat diese Genderschreibweise einen Nachteil, der dann zum tragen kommt, wenn die männlichen Begriffe nicht in ihrer Gänze im Wort vorkommt. Als Beispiel soll hier *Expert:in* dienen. Ungleich unseres Fallbeispiels von Grafiker:in (welches die männliche Variante Grafiker beinhaltet), kann *Expert:in* keine Rankings für *Experte* aufbauen. In einer solchen Konstellation empfehlen wir im Rahmen unserer Online Marketing Beratung immer einen ausgeglichenen Einsatz aller Geschlechterschreibweisen.

Aktuelle Entwicklungen im Gendern für Suchmaschinen

John Müller von Google ging im Zuge des Search Central Webmaster Hangouts vom 10. Juni 2021 kurz auf die Thematik von Genderschreibweisen ein (Quelle). Dabei sagte er, dass Google immer noch abwartend im Hinblick eines eindeutigen Durchsetzens einer bestimmten Schreibvariante reagiere. Synonyme, und so fasst er sowohl die weibliche bzw. männliche Schreibweise zusammen als auch Doppelpunktvariante oder Gendersternchen, *müsste* Google mittlerweile erkennen können. Die Betonung liegt hier allerdings auf dem Konjunktiv. Derzeit scheint das Thema noch nicht ganz so relevant bei Google zu sein und es gäbe noch entsprechendes Tuningpotenzial.

Ebenso äußerte sich John Müller im Dezember 2021 im Podcast Search Off The Record zum Lernprozess inklusiver Sprache. Googles Algorithmus lerne mit sich änderndem Suchverhalten der Nutzenden. Das gelingt Google in einigen Sprachen etwas schneller, während für andere Sprachen noch Zeit benötigt wird, die unterschiedlichen Schreibweisen zuzuordnen. Eine gute Zusammenfassung des Podcasts könnt ihr dazu auch auf SEO Südwest lesen.

Die **Website Boosting** (Quelle Ausgabe #69 , Seite 10) griff die Thematik in ihrer Rubrik *Ask Google* ebenso auf. Google antwortete dort auf die Frage, ob Webseiten Ihre Sprache auf genderneutral umstellen sollen bzw. wie Google damit umgeht. Als Antwort gab Google zu Protokoll, dass Google in der Google Suche nichts Spezielles zum Thema genderspezifische Wortwahl mache. Der Algorithmus lernt automatisch, welche Worte Synonyme sind. Jedoch kann dies bei neuen sprachlichen Entwicklungen etwas Zeit in Anspruch nehmen. Es wird empfohlen, Webseitentexte so natürlich wie möglich zu schreiben. Die Themantik wurde erneut in der Ausgabe #73 aus dem April 2022 auf Seite 10 besprochen. Als Antwort auf die Frage, ob man generell gendern und sich dieser Entwicklung

anpassen sollte, stellte Google klar, dass der Algorithmus verschiedene Schreibweisen problemlos unterstütze und es daher keine Empfehlung gäbe. Vielmehr sollten sich Webseitenbetreibende mit ihren Inhalten an der Erwartungshaltung der Nutzenden orientieren und diese bedienen.

5 Tipps fürs Gendern im SEO

Damit das Gendern auf einer Website oder einem Blog erfolgreich ist und du für deine gesamte Zielgruppe Relevanz aufbauen kannst, kommst du in einigen speziellen Fällen nicht um den Einsatz des generischen Maskulinums herum. Jedoch kannst du diesen Umstand auch kreativ zugunsten gendersensibler Formulierungen und Inhalte nutzen.

Qualitative und vollumfängliche Inhalte für User:innen

SEO und Gendern hin oder her: Ohne qualitative, umfängliche Inhalte und den Grundlagen der Suchmaschinenoptimierung, wirst du nachhaltig keine organischen Suchmaschinenrankings erzielen und gefunden werden. Schreibe deine Inhalte lesbar, verständnisvoll und sorge für die bestmögliche Nutzungserfahrung auf deiner Webseite. Konfiguriere deine Zielseiten so, dass sie technisch einwandfrei crawlbar sind und verlinke intern wie extern auf weiterführende Informationen. Grundsätzlich sollten unter dieser Prämisse alle genderneutralen, femininen und maskulinen Ausdrucksweisen ihren Einzug erhalten.

Themenbereich in den Vordergrund stellen

Stelle das Thema oder die Leistung mehr in den Vordergrund als die handelnden Personen. Bei diesem Ansatz macht es beispielsweise Sinn, eher auf Grafikdesign statt auf Grafikdesignerin oder ähnliche Schreibweisen zu optimieren. Zwar hat Grafikdesign mitunter etwas weniger Suchvolumen als Grafikdesigner, dennoch erreichst du so eine deutlich größere

Anzahl an suchenden Nutzergruppen.

Genderneutrale Ausdrucksweisen wählen

Finde für deine Inhalte genderneutrale Begrifflichkeiten und Synonyme. Statt Chef oder Chefin können auch die Bezeichnungen Führungskreis oder Geschäftsleitung eingesetzt werden. Für Online Marketing Manager oder Sales Managerinnen eignen sich beispielsweise Personal im Online Marketing oder das Sales Management Team.

Symmetrischer Einsatz von Geschlechterbeispielen

Wie du sicher schon bemerkt hast, bemühen wir uns in unseren Artikeln um eine möglichst große Bandbreite an Genderschreibweisen. Wir haben uns neben dem Gendern mit Doppelpunkt bewusst dazu entschieden, maskuline, feminine und gruppenbezogene Beispiele explizit anzusprechen (s. erste Zeile Abschnitt 1.). Nur so kann sichergestellt werden, dass neben der bevorzugten sensiblen Ansprache auch Sichtbarkeit für die weit verbreiteten maskulinen als auch die weniger verbreiteten femininen Suchbegriffe generiert wird. Wir nutzen alle exisiterenden Genderschreibweisen auch an weniger prominenter Stelle, z.B. als Alt Tags bei Bildern.

Übermäßige Zeichensetzung vermeiden

Wir haben uns ebenso bewusst gegen Schreibweisen mit einem Schrägstrich (/) oder Gendersternchen (*) entschieden. Den Grund dafür liefert ein Blick in Googles Quality Guidelines. Google definiert qualitative Inhalte dahingehend, dass sich diese durch fehlerfreie Rechtschreibung und Ausdrucksweise auszeichnen. Übertriebene und falsche Zeichensetzung sind laut Google ein Indikator für eine geringere Seitenqualität. Zugegebenerweise wissen wir nicht genau, ab welcher Zeichenfolge so ein Fall eintritt, wir halten es aber insbesondere bei Schreibweisen mit Artikeln und Adjektiven für deutlich wahrscheinlicher. So könnte „ein/-e gute/-r Manager/-in“ unter Umständen eher als unzureichende Grammatik

eingestuft werden als die Merzahlansprache „gute Manager:innen“ mit Doppelpunkt oder einfach „gutes Management“ oder „gut Managende“.

Wie sieht die Zukunft im gendergerechten SEO aus?

Bis neue Genderschreibweisen mit gleicher Relevanz bisheriger Ausdrucksweisen Einzug in Suchmaschinen halten, wird noch ein Weilchen vergehen. Einserseits steht der Bewusstseinsprozess von Suchenden und Webseitenbetreiber:innen noch am Anfang und andererseits ist Googles Algorhitmus noch nicht so weit, gendergerechte Suchanfragen für indexierte maskuline Varianten ausreichend zu interpretieren. Wir werden den Prozess beobachten und unsere Erkenntnisse den aktuellen Entwicklungen anpassen.

Streitgespräch: Google Analytics vs. Matomo

STREITGESPRÄCH: Google Analytics oder

Matamo? – websiteboosting.com

Eigentlich interessant, dass wir so ein Streitgespräch führen, weil es vor einigen Jahren gar kein Publikum für diese Diskussion gegeben hätte. Dass wir jetzt über Google Analytics und Matomo reden, liegt am Thema Datenschutz. Aber für Digital-Analysten geht es ja auch um Funktionen, Features und… **Eigentlich interessant, dass wir so ein Streitgespräch führen, weil es vor einigen Jahren gar kein Publikum für diese Diskussion gegeben hätte. Dass wir jetzt über Google Analytics und Matomo reden, liegt am Thema Datenschutz. Aber für Digital-Analysten geht es ja auch um Funktionen, Features und Analysemöglichkeiten.**

Google Analytics – Standpunkt von Alexander Holl:

#1 Funktionsumfang von Google Analytics vs. Matomo

Wie gut funktioniert Facebook-Werbung? Um so eine Frage zu beantworten, kann ich mir Konversionsraten ansehen oder auf Basis von Engagement, Konversionen, Attribution und Attributionsmodell-Vergleichen dieser Frage auf den Grund gehen. Hilfreich bei der Analyse ist es, Analysemethoden wie sekundäre Dimensionen, Filter (reguläre Ausdrücke), Kohortenanalysen oder benutzerdefinierte Berichte zu verwenden. Das Ergebnis der Analyse visualisiere ich dann im Tabellenformat, als Kreis-, Balkendiagramm oder als Pivot.

Bitte kontaktieren Sie Ihren Matomo-Administrator

Manches geht auch bei Matomo, aber eben nicht out of the box, sondern in der eigen gehosteten Variante als (meist) bezahltes Plug-in. Wir haben Matomo mit 50 Plug-ins im Einsatz. Gerade

steht bei mir im Adminbereich: „Das Plug-in BeeLikedDBIP konnte nicht geladen werden … Bitte kontaktieren Sie Ihren Matomo-Administrator.” Dabei geht es in der Administration nicht um Plug-ins, sondern um Organisation in der Web-Analyse.

Google bietet momentan (Universal Analytics) in der Administration drei Ebenen. Es gibt die Konto-, Property- und Datenansichtsebene. Neben umfangreichen Einstellungsmöglichkeiten auf allen drei Ebenen ist besonders die Flexibilität bei der Nutzerverwaltung extrem wichtig. Ab einer gewissen Mitarbeiterzahl ist die Vergabe von Nutzerrechten Kernanforderung, um die Analyse von Daten zu organisieren. Matomo hat über die Plug-in-Logik eine Überkomplexität in der Integration von Analysemöglichkeiten und eine Unterkomplexität in der wirklichen Administration der Web-Analyse.

#2 Integration von Daten

Du bist ein guter Digital-Analyst, wenn du neben der Analyse von Website-Daten auch SEO, Social Media, Google Ads, Produkt- und Kundendaten aus verschiedenen Tools analysieren kannst. Alles kann auch Analytics nicht, aber gerade die tiefe Integration von Daten aus Google Ads, aus der Search Console, AdSense, der Verknüpfung mit dem Tag-Manager und Optimize ist sicher eine der ganz großen Stärken. Dazu kommt noch der Export von Rohdaten in BigQuery, der in Analytics 4 sogar ohne die 360-Version kostenlos möglich ist. Manches geht in Ansätzen mit Skripten oder Workarounds in Matomo auch. Das ist aber oft sehr aufwendig und im Resultat mit limitierten Daten. Im Vergleich dazu werden über die Verknüpfung von Analytics und Google Ads statt 5 Parametern (Matomo) 14 Parameter wie der CPC oder Kostendaten übergeben.

Externe Integration von Google Analytics

Ein zweiter Aspekt ist auch die externe Integration in SEO-Tools wie Ryte, SISTRIX, Searchmetrics oder den Screaming Frog

und in CRM-Tools wie HubSpot oder Salesforce. Und natürlich für fortgeschrittene Analysen, bessere Visualisierung und Erweiterung der Datenquellen, die einfache Integration in Google Data Studio. Matomo ermöglicht hier nur den Export von Daten in Data Studio über den Umweg eines Google-Sheets.

#3 Community: „Hallo, wie kann ich dir helfen?"

Letztes Jahr habe ich ein großes Unternehmen zu Analytics geschult. Im Anschluss sagte mir ein Mitarbeiter: „Analytics lernen ist wie eine neue Sprache lernen." Und wahrscheinlich stimmt das auch. Aus Daten Wissen zu generieren, ist wie eine neue Sprache zu lernen.

Zum Glück gibt es eine enorme Anzahl an kompetenten „Analytics-Sprachlehrern". Da ist Google selber, die über ihren Blog, den YouTube-Kanal, aber auch über ihre Lösungsgalerie (https://analytics.google.com/analytics/gallery/) Unterstützung anbieten. Allein in dieser Solution Gallery gibt es Hunderte von Dashboards, Berichten oder Segment-Ideen zum Download. Und neben den Google-Ressourcen gibt es eine funktionierende Infrastruktur an (zertifizierten) Agenturen, Beratern, Fachkonferenzen, Blogs und Schulungsangeboten.

Google mit Herausforderungen beim Datenschutz, Matomo bei Funktionen und Administration

Matomo punktet immer beim Thema (behördlicher) Datenschutz. Inzwischen gibt es aber neben den Behörden auch mächtige Player wie Apple oder Firefox, die über Intelligent Tracking Prevention (Apple), IOS 14.5 (Apple) oder Enhanced Tracking Protection (Firefox) den Schutz von Kundendaten priorisieren. Das führt in der Konsequenz zu einer Erosion von Daten. Diese betrifft aber alle Anbieter von Tracking-Tools. Unsere

Herausforderung als Digital-Analysten heißt, mit weniger Daten gute Analysen zu machen. Und leidet die Datenqualität, brauche ich bessere Tools für gute Analysen.

Google muss seine Datenschutzprobleme lösen, Matomo muss Funktionsparität schaffen.

Ich glaube, trotz vieler Herausforderungen ist Google vs. Matomo in einer besseren Situation. Funktionsparität zu Google herzustellen, ist massiv schwer. Google geht ja schon einige der großen Themen in der Web-Analyse an. Zum Beispiel mit Google Analytics 4, das einen deutlich verbesserten Ansatz zum Datenschutz bietet sowie den Export von Rohdaten in die Google-Cloud ermöglicht, und das sogar auf europäische Server. Google Analytics auf eigenen Servern zu betreiben (Server-side Tagging) ist ein weiterer Schritt, um den Schutz von Daten selber zu kontrollieren.

Datenkompetenz ist eine entscheidende Säule der Digitalisierung

Die Digitalisierung der Geschäftsprozesse ist wahrscheinlich der Erfolgsfaktor. Und Datenkompetenz ist einer der Säulen der Digitalisierung. Welche Daten entstehen in meinem Geschäftsmodell und wie kann ich diese möglichst effizient einsetzen? Also wer ausschließlich auf Matomo setzt, nimmt das Risiko in Kauf, Datenkompetenz zu stark auf das Thema Datenschutz zu fokussieren.

Matamo – Standpunkt von Thomas Zeithaml:

Vorteil Datenschutz: Durch die Daten-Sammellust von Plattformen wird der Datenschutz immer wichtiger. Ziel ist es, an dieser Stelle sicherzustellen, dass Daten anonymisiert und

unbefugten Personen Zugang zu ihnen verwehrt wird. Webanalyse und Tracking befinden sich im Wandel, was sich in den juristischen Diskussionen widerspiegelt. Es geht aber vorrangig darum, die Datenhoheit zu behalten und die Privatsphäre der Besucher nicht zu verletzen.

Mit Matomo werden die Daten direkt durch den Seitenbetreiber erhoben. Dadurch hat dieser die vollständige Kontrolle über seine Tracking-Daten. Eine Herausgabe von Daten an Dritte findet an dieser Stelle nicht statt.

Dies kann man bei Google Analytics leider nicht 100%ig sicherstellen. Natürlich gibt es Möglichkeiten, die DSGVO auch mit Analytics umzusetzen. So kann man Einwilligungen zur Nutzung einholen, IP-Adressen anonymisieren und einen Vertrag zur Auftragsverarbeitung abschließen. Etliche Punkte in Bezug auf einen datenschutzkonformen Einsatz von Google Analytics sind noch nicht geklärt und bieten meiner Meinung nach mehr Angriffsfläche als Matomo – aus DSGVO-Sicht ein klarer Vorteil für eine solche selbstgehostete Lösung.

Matomo ermöglicht eine Vielzahl von Einstellungen, um der Datenschutzkonformität nachzukommen. Das ist mitunter Grund genug, weshalb Matomo von vielen Datenschützern favorisiert wird. Immer mehr Webseitenbetreiber wie Kommunen, Vereine oder sogar Regierungen haben diesen Vorteil erkannt und setzen auf Matomo, um ihre Reichweite zu messen. Darüber hinaus verzeichnet Google Analytics einen Marktanteil von ca. 84 % – Matomo nur 1,5 % –, wodurch der Marktriese eher in den Fokus von Datenschützern rückt.

Nicht unbedeutend ist der Serverstandort des Tracking-Tools. In diesem Punkt argumentieren Datenschützer, dass die EU trotz diverser Abkommen über strengere Regeln als andere Länder verfügt. Bei einer Self-Hosting-Lösung hat der Betreiber die Möglichkeit, Server in Deutschland einzusetzen. Die Daten bleiben somit im Inland und erfüllen diese Anforderung.

Wir können davon ausgehen, dass der EuGH in Bezug auf Datenschutz noch Anpassungen vornehmen wird. Ohne eigene Datenhoheit ist es nur schwer möglich, auf zukünftige Entscheidungen zu reagieren.

Vorteil Blockaden: Viele Internetnutzer wehren sich gegen die zunehmenden Werbeformate im Internet und setzen zu diesem Zweck sogenannte Adblocker ein. Inzwischen werden neben klassischen Werbenetzwerken aber auch Trackingskripte ausgeschlossen. Auch Browserhersteller reagierten auf diese Bedürfnisse und setzen verstärkt auf Tracking-Prävention.

Bei der Erkennung von Skripten spielt die Einbindung eine tragende Rolle. Als First-Party-Skripte gelten Skripte, welche auf der Domain selber eingebunden werden. Das Pendant dazu stellen Third-Party-Skripte wie z. B. Google Analytics, AdSense, DoubleClick usw. dar, welche auf externen Domains angestoßen werden. Da Matomo z. B. in einem Unterverzeichnis der eigenen Domain liegt, wird das Trackingskript als First-Party-Script erkannt. Das Entfernen oder Blockieren von First-Party-Skripten kann die Funktionalität der gesamten Webseite beeinflussen. Daher bleiben diese Skripte von Adblockern meist unbeachtet. Ein weiterer Grund könnte sein, dass der Marktanteil von Matomo noch zu gering ist und vielleicht deswegen nicht im Fokus der Adblocker-Betreiber liegt. Zudem kann es auch sein, dass Matomo nicht als Bedrohung in Bezug auf Datenschutz- und Privatsphären-Verletzungen erkannt wird. Durch den Wegfall der Blockade werden mehr Daten erfasst. In einigen Projekten konnten wir beobachten, dass ca. 20 % mehr Daten von Matomo erfasst werden als in der parallel laufenden Google-Analytics-Instanz.

Vorteil Limits: Ein häufig genannter Nachteil von SAAS-Lösungen wie Google Analytics sind diverse Limitierungen. Mithilfe einer Self-Hosting-Lösung wie Matomo lassen sich einige gravierende Beschränkungen elegant umgehen.

So gibt es z. B. keine Einschränkungen in Bezug auf

Nutzeranzahl oder Webseiten innerhalb einer Matomo-Installation. Bei der Datenerfassung existieren keine Begrenzungen. Beschränkungen wie beispielsweise 500 Hits pro Sitzung oder 10 Millionen Nutzer pro Monat entfallen bei Matomo. Die eigene Hardware stellt die einzige Limitierung in puncto Datenerfassung dar.

Eine Besonderheit von Matomo ist es, die Daten live und vollständig auszuwerten. In Matomo findet keine stichprobenartige Darstellung (Sampling) statt. Die Daten stehen in vollem erfasstem Umfang (Rohdaten) zur Verfügung. Außerdem entfällt bei Export-Funktionen oder Schnittstellen ein mögliches API-Credit-System.

Nutzer von Matomo profitieren mitunter von der unbegrenzten Dauer der Datenspeicherung. Gewöhnlich ist der Zugriff bei Google Analytics auf eine Dauer von maximal 26 Monaten beschränkt. Auch wenn man z. B. in Universal-Analytics-Properties andere Einstellungen treffen kann, werden diese Daten in absehbarer Zeit gelöscht. Matomo ermöglicht einen unbeschränkten Datenzugriff, individuelle Aufbewahrung- und Archivierungszeiträume.

Vorteil Transparenz: Matomo besticht durch individuell mögliche Einsatzmöglichkeiten und Transparenz.

Grundsätzlich stehen dem Nutzer erhobene Daten in Form von Rohdaten zur Verfügung. Dadurch können die Daten vollständig ausgewertet und verarbeitet werden. Auch eine Anbindung an Dritt-Systeme wie ein CRM oder CMS sind problemlos möglich.

Matomo ermöglicht als Open-Source-Projekt die Einsicht in die Quelldateien. Nutzern mit Programmierkenntnissen ist es möglich, Berechnungen wie z. B. die Absprungrate oder Verweildauer nachzuvollziehen. Ebenso können alle ankommenden Anfragen eingesehen und analysiert werden.

Matomos modulares System kann um zusätzliche Funktionen erweitert werden. Das bedeutet, benötigte Features lassen sich

als Plug-ins implementieren oder stehen bereits zur Verfügung. Somit ermöglicht Matomo dem Nutzer Flexibilität, Individualität und Transparenz, die GA auf diese Art nicht bietet.