CSR (Certificate Signing Request)

CSR (Certificate Signing Request)

Ein CSR (Certificate Signing Request), zu Deutsch Anforderung auf Ausstellung eines Zertifikats, ist eine speziell formatierte und verschlüsselte Nachricht. Die wird von einem Antragsteller für ein digitales SSL-Zertifikat (Secure Sockets Layer) an eine CA (Certificate Authority / Zertifizierungsstelle) gesendet. Der CSR bestätigt die Informationen, die eine CA benötigt, um das Zertifikat ausstellen zu können.

Ein PKI-System (Public Key Infrastructure) ermöglicht den sicheren Austausch von Daten über das Internet zwischen verifizierten Parteien. In so einem System muss vor der Bestellung und dem Kauf eines SSL-Zertifikats ein CSR erschaffen werden. Der Antragssteller muss zunächst ein Schlüsselpaar generieren. Der Private Key (privater Schlüssel) dient zu Entschlüsselung der verschlüsselten Daten und der Generierung von digitalen Signaturen. Den Public Key (öffentlichen Schlüssel) benutzt man, um die Daten zu verschlüsseln und die Signaturen zu verifizieren. Sie müssen sowohl das Schlüsselpaar als auch den CSR auf dem Server erstellen, auf dem Sie das SSL-Zertifikat benutzen wollen. Das ist zwingend erforderlich, um die Integrität des Schlüsselpaars und der PKI im Allgemeinen zu garantieren.

Sobald das Schlüssel-Paar präpariert ist, kann der CSR generiert werden. Die CA wird all die notwendigen Daten des CSRs (siehe Tabelle) verwenden, um das Zertifikat

auszustellen. Wie ein CSR generiert wird, hängt von der eingesetzten Webserver-Software ab. Sobald der CSR erstellt ist, kann man ihn bei der CA einreichen. Ist ein Antrag erfolgreich und für gültig erklärt, wird die CA das SSL-Zertifikat ausstellen und unterzeichnen.

Information	Beschreibung	Beispiel
Common Name	Der FQDN (Fully Qualified Domain Name) des entsprechenden Servers.	www.meinefirma.de mail.meinefirma.de *
Business Name / Organization	Der offizielle Name Ihres Unternehmens	Meine Firma, Mein Unternehmen
Department / Organization Name	Die Abteilung Ihres Unternehmens, die für das Zertifikat verantwortlich ist.	IT, Finanz-Abteilung
City / Town	Die Stadt, in der Ihre Firma den Sitz hat.	München, Hamburg
State & County / Region	Das Bundesland oder die Region, in der sich Ihre Firma befindet. Verwenden Sie hier keine Abkürzungen.	Bayern, Hessen
Country	Der zweistellige ISO-Code für das Land, in dem sich Ihr Unternehmen befindet.	DE, US

Email Address	Eine E-Mail-Adresse, um die Firma kontaktieren zu können.	admin@meinefirma.de zertifikate@meinefirma.de

** Generiert man einen CSR für ein so genanntes Wildcard-Zertifikat, sollte der Common Name mit einem * beginnen. Ein Beispiel wäre *.meinefirma.de*

Was ist ein SSL-Proxy?

Was ist ein SSL-Proxy?

Ein SSL-Proxy ist ein Gerät, normalerweise ein Router oder Computer, der den Datenverkehr von einem Client zu anderen Servern mithilfe des SSL-Protokolls (Secure Sockets Layer) weiterleitet. SSL ist ein verschlüsseltes Protokoll, das eine sichere Verbindung von einem Client zu einem anderen Client oder Server herstellt. SSL wird häufig in Verbindung mit dem Hypertext Transfer Protocol verwendet, um beim Surfen im Internet eine sicherere Verbindung herzustellen. Das resultierende Protokoll oder die Sprache in einfacheren Ausdrücken wird als HTTPS bezeichnet.

Die Funktion eines Proxyservers besteht darin, den Datenverkehr für ein Netzwerk oder einen Client weiterzuleiten und zu filtern. In einem typischen Szenario gibt der Client, normalerweise ein Computer, eine Anforderung aus, in der Regel das World Wide Web zu besuchen, und der Proxy-Server empfängt diese Anforderung, filtert sie und leitet sie entsprechend weiter. Der Vorteil eines Proxyservers besteht darin, dass er den Netzwerkverkehr zentralisieren und gleichzeitig Sicherheit

bieten kann.

Der Proxy kann Anfragen nach fast allen gewünschten Kriterien filtern. Wenn ein Unternehmen beispielsweise nur zu einer bestimmten Tageszeit zulassen möchte, dass der Datenverkehr aus dem Hauptnetz in ein anderes Netzwerk oder das World Wide Web geleitet wird, kann es den Proxyserver so einstellen, dass der gesamte Datenverkehr außerhalb des Netzwerks für den Rest des Netzwerks blockiert wird die Zeit. Da der Datenverkehr einen Server durchlief, konnte er auch für Nutzungsstatistiken überwacht werden. Eine hilfreiche Sache für viele Unternehmen.

Secure Sockets Layer (SSL) ist ein Protokoll, das Daten aus Sicherheitsgründen verschlüsselt. Zusätzlich zur Verschlüsselung wird auch ein System von Zertifikaten verwendet, mit denen andere Computer oder Server ihre Authentizität überprüfen. Das HTTPS-Protokoll, die Kombination aus HTTP und SSL, wird häufig zum Herstellen sicherer Verbindungen im Internet verwendet. Viele Unternehmen, die Kreditkarten online akzeptieren, verwenden beispielsweise das HTTPS-Protokoll, sodass niemand auf den Datenstrom zugreifen und vertrauliche Informationen abrufen kann.

Der Hauptzweck eines SSL-Proxys besteht darin, vertrauliche Daten in großem Umfang zu schützen. Es gibt viele Fälle, in denen dies wünschenswert wäre. Ein typisches Beispiel wäre ein großes Unternehmen, das sensible Daten wie finanzielle oder rechtliche Informationen verarbeitet. Das Netzwerk könnte so eingerichtet werden, dass der gesamte ausgehende Datenverkehr des gesamten Unternehmens oder einer bestimmten Abteilung über einen SSL-Proxy geleitet wird. Dies kann zu einem zusätzlichen Schutz beim Senden von Informationen führen, insbesondere von Daten, die über das Internet übertragen werden müssen.

Eine andere typische Verwendung für einen SSL-Proxyserver wäre für Unternehmen, die Zahlungen in irgendeiner Form entgegennehmen. Oft haben sie einen Reverse-SSL-Proxy. Der Reverse-Proxy nimmt den eingehenden und nicht den ausgehenden

Datenverkehr auf und kann das SSL-Protokoll intakt halten sowie das Innere des Netzwerks vor möglichen Eindringlingen schützen.

Was ist ein SSL-Proxy?

Was ist ein SSL-Proxy?

QR-Codes – Sicherheitsprobleme

Gefahr im Bithaufen

QR-Codes: Sicherheitsproblem oder nicht?

QR-Codes können ähnlich wie Phishing-Mails Träger gefährlicher URLs sein. Wir erklären, welche Tricks sich Kriminelle ausgedacht haben und worauf Sie beim Scan von QR-Codes achten müssen.

Von Wilhelm Drehling

Die quadratischen Codes sind im Alltag nützliche Helfer: Mit einem Scan können Sie eine URL aufrufen, einen Kontakt hinzufügen oder dem Gast zu Hause das Abtippen des WLAN-Passworts ersparen. Weil sie praktisch sind und auch mal leichtfertig gescannt werden, haben auch Angreifer ihre Freude an QR-Codes gefunden. Denn das Aussehen des QR-Codes verrät

nichts über dessen Inhalt, so kann sich in dem Pixelhaufen ein gefährlicher Link zu einer täuschend echten Anmeldeseite einer Fake-Bank oder zu einem Trojaner verbergen. In den vergangenen Jahren haben Kriminelle originelle Methoden erfunden – denen man aber zum Glück nicht schutzlos ausgeliefert ist.

Quishing

Das erste Angriffsszenario gehört in die Kategorie der Phishing-Angriffe: Vermutlich kommen Ihnen dubiose Mails wie „PayPal: Ihr Konto ist vorübergehend eingeschränkt“ bekannt vor. Mit solchen Mails versuchen die Angreifer häufig, an Ihre Anmeldedaten heranzukommen, indem sie Sie auf eine gefälschte Webseite mit gewohntem Anmeldefenster weiterleiten. Enthält die Mail einen QR-Code, der zur Phishing-Seite führt, spricht man von Quishing.

Der große Unterschied zu den üblichen Mail-Betrügereien: Es hat sich bereits herumgesprochen, dass man nicht einfach so auf Links in Mails klicken sollte, die möglicherweise obendrein in schlechtem Deutsch verfasst sind. Bei QR-Codes ist das nicht der Fall. Ergo schenkt man QR-Codes mehr Vertrauen, scannt sie ein und landet dann womöglich auf einer Phishing-Seite oder Ärgerem.

Diese Masche tritt häufig in unterschiedlichen Varianten auf: Die Volksbank warnte im Dezember 2021 vor Mails und sogar Briefen mit QR-Codes, die Kunden dazu aufforderten, eine neue App herunterzuladen und sich dort zu registrieren. Ähnliche Angriffe mit QR-Codes häuften sich in letzter Zeit so sehr, dass die Polizei eine Warnung vor QR-Codes in Mails aussprach (sämtliche Warnungen haben wir Ihnen unter ct.de/yrf5 verlinkt).

Ob diese Warnungen wirklich etwas bringen, lässt sich diskutieren. Der c’t-Security-Experte Jürgen Schmidt geht in seinem Kommentar im Kasten rechts dieser Frage auf den Grund.

QR-Codes sind nicht das Problem

Ein Kommentar von Jürgen Schmidt (Leiter heise Security)

Die Krypto-Börse Coinbase platzierte in der Halbzeitpause des Superbowls einen Werbespot, der die Zuschauenden dazu verleiten sollte, einen über den Fernseher hüpfenden QR-Code mit der Handy-Kamera einzufangen. Auf der dann angezeigten Website erwartete sie nur eine Meldung, dass der Dienst nicht erreichbar ist – vermutlich wegen Überlastung. Aber das ist eine andere Geschichte.

Es folgte ein Aufschrei der um die Sicherheit besorgten Experten, dass man den Anwendern unsichere Verhaltensweisen antrainiere und somit Phishing-Betrügern in die Karten spiele. Schließlich könne sich hinter dem QR-Code doch auch eine bösartige Phishing-Webseite verbergen, die es auf ihre Zugangsdaten abgesehen hat. Ich halte diesen Ansatz für falsch.

Das World Wide Web beruht darauf, dass Anwender Links öffnen. Auch solche, bei denen sie vorher nicht wissen, was genau sich dahinter verbirgt, schließlich will man ja Dinge entdecken. Es ist deshalb unsere (uns hier im Sinne von all denen, die im weitesten Sinne das Web mitgestalten) Aufgabe, den Anwendern Werkzeuge bereitzustellen, mit denen sie das tun können. Sprich: Anwender sollten einen Link ohne unmittelbare Gefahr öffnen können. Wenn allein durch das Öffnen eines Links etwas Böses passiert, dann ist das ein Fehler im Browser, den dessen Hersteller zu verantworten und zu beseitigen hat.

Die Verantwortung des Anwenders beginnt, wenn er mit der Seite

interagiert. Bevor er dort persönliche Daten oder sogar ein Passwort eingibt, sollte er sich die Frage stellen, ob und wie weit er der Seite vertrauen kann. Da spielt primär der Kontext eine wichtige Rolle. Das ist in der analogen Welt nicht anders: Dem Hotel-Angestellten beim Check-in gibt man seine Kreditkarte; einem Unbekannten am Bahnhof eher nicht.

In der digitalen Welt zeigt sich da schon das erste Problem: Browser zeigen immer öfter gar nicht mehr an, wo sich der Anwender gerade befindet und machen es damit schwer, die Vertrauenswürdigkeit einer Passwortabfrage zu beurteilen oder gar zu überprüfen. Immerhin können sich Anwender fragen: Wie bin ich hierher gelangt? Über ein gespeichertes Lesezeichen oder einen QR-Code in einem eher zweifelhaften Zusammenhang? Der Vertrauens-Check ist nicht trivial – aber etwas, was man Anwendern beibringen kann und sollte. „Klicke nicht auf Links“ oder „Verwende keine QR-Codes“ hingegen sind keine sinnvollen Lernziele. Darüber hinaus kann man Anwender zu Multifaktor-Authentifizierung und insbesondere FIDO2 ermuntern, weil sie konzeptionell vor Phishing schützen.

Eine Verteufelung von QR-Codes hingegen führt nur zu noch mehr angeblichen „Best Practices der Security“, die zwar gebetsmühlenartig wiederholt werden, an die sich niemand wirklich hält, weil sie praxisfern sind. Ich scanne den QR-Code im Restaurant, um mir die Speisekarte anzuschauen und ich würde mir wünschen, dass auch meine Bank Girocodes einführt [1], weil ich es satthabe, ständig gefühlt 100-stellige IBANs von Hand einzutippen. Ich werde also auch anderen Menschen, die sich von mir Sicherheitstipps erhoffen, nicht erzählen, dass sie keine QR-Codes benutzen dürfen, sondern lieber zur Zweifaktor-Authentifizierung raten.

Überklebt

Ein deutlich gefährlicherer und unscheinbarer Angriffsvektor geht von öffentlichen QR-Codes aus, die Sie in Broschüren, Werbeplakaten oder Speisekarten finden. Angreifer können die

Codes überkleben und die Opfer somit auf gefälschte Webseiten locken. Die Idee hinter dem Angriff ist nicht neu, schon 2013 warnte das Bundesamt für Sicherheit in der Informationstechnik (BSI) vor überklebten QR-Codes.

Das passiert nicht unbedingt bei Speisekarten; vorsichtig müssen Sie bei QR-Codes sein, die „alternative Bezahlmöglichkeiten“ anpreisen. Das FBI warnt in den USA zum Beispiel davor, keine QR-Codes bei Parkplätzen zu scannen, die zu einem Bezahldienst weiterleiten: Anstatt zum Parkautomat zu laufen, könne man so bequem die Rechnung für die Parkdauer bezahlen. Doof nur, wenn das Geld dann nicht an den Parkplatzbetreiber fließt, sondern direkt in die Taschen der Betrüger.

Überklebte QR-Codes verheißen auch bei Außenwerbung Unheil, die dazu einlädt, eine App herunterzuladen oder Webseiten zu besuchen. In solchen Fällen greifen die Angreifer erneut nach Ihren Daten und im schlimmsten Falle versuchen sie, über eine App einen Trojaner auf Ihr Smartphone herunterzuladen (zugegebenermaßen ist das leichter beim Google Play Store zu bewerkstelligen als über den App Store auf iOS).

Genauso kritisch sind leicht zugängliche QR-Codes in Zügen oder Einkaufszentren, die einen einfachen Zugang zum WLAN anbieten: Ein solcher QR-Code kann von Angreifern überklebt worden sein. Mit einem Klick verbinden Sie sich mit einem von Angreifern eingerichteten gleichnamigen Hotspot.

Gegenmaßnahmen

Hersteller von Smartphones haben schon früh reagiert: Kamera-Apps folgen nicht mehr direkt einer gescannten URL. Ein Großteil aller modernen Kamera-Apps zeigt den Link stattdessen auf dem Bildschirm an. Danach ist es an Ihnen, zu entscheiden, ob Sie darauf klicken oder nicht. Dabei ist der gesunde Menschenverstand gefragt: Sieht die URL merkwürdig aus, dann sollten Sie den QR-Code genauso wie eine Phishing-Mail in den

Papierkorb befördern.

Wenn Sie zusätzlich auf Nummer sicher gehen wollen (oder Familienangehörigen einen Gefallen tun wollen), weichen Sie unter Android auf eine App wie zum Beispiel Trend Micro QR-Scanner aus (siehe ct.de/yrf5), die den Inhalt des QR-Codes prüft und Sie vor potenziell gefährlichen Links warnt. iOS-Nutzer nehmen die App Intercept X von Sophos (siehe ct.de/yrf5). Die sichere Scanfunktion für QR-Codes ist aber nur ein kleiner Teil der Antiviren-App: Mit der App laden Sie leider noch viele weitere Funktionen herunter, deren Sinn mindestens zweifelhaft ist.

Mit der App QR-Scanner von Trend Micro bekommen Sie eine Einschätzung, ob die URL hinter dem QR-Code potenziell gefährlich ist.
Tipp für ganz harte Tüftler: Alternativ können Sie Ihr Smartphone beiseitelegen und den QR-Code per Hand dekodieren [2]. Das ist zwar mühsam, aber Sie fangen sich auf diese Art und Weise definitiv kein Virus ein.

Fazit

Wie bei vielen der vorgestellten Szenarien spielt der Kontext

eine wichtige Rolle: Ein QR-Code mit WLAN-Daten bei Ihnen zu Hause genießt ein höheres Vertrauen als ein QR-Code auf einem Laternenmast, der für ein öffentliches WLAN wirbt. Im Zweifel sollten Sie die Entscheidung, eine fragwürdige URL anzuklicken, dem gesunden Menschenverstand überlassen oder bei noch größeren Zweifeln eine QR-Überprüfungs-App konsultieren. *(wid@ct.de)*

1. Literatur
2. Jan Mahn, Schöner zahlen, Rechnungen schneller überweisen mit QR-Codes, c't 7/2022, S. 138
3. Wilhelm Drehling, Bithaufen, QR-Codes verstehen und ohne technische Hilfsmittel per Hand dekodieren, c't 17/2022, S. 142

Warnungen und Scanner-App: ct.de/yrf5

Windows und Linux zusammen

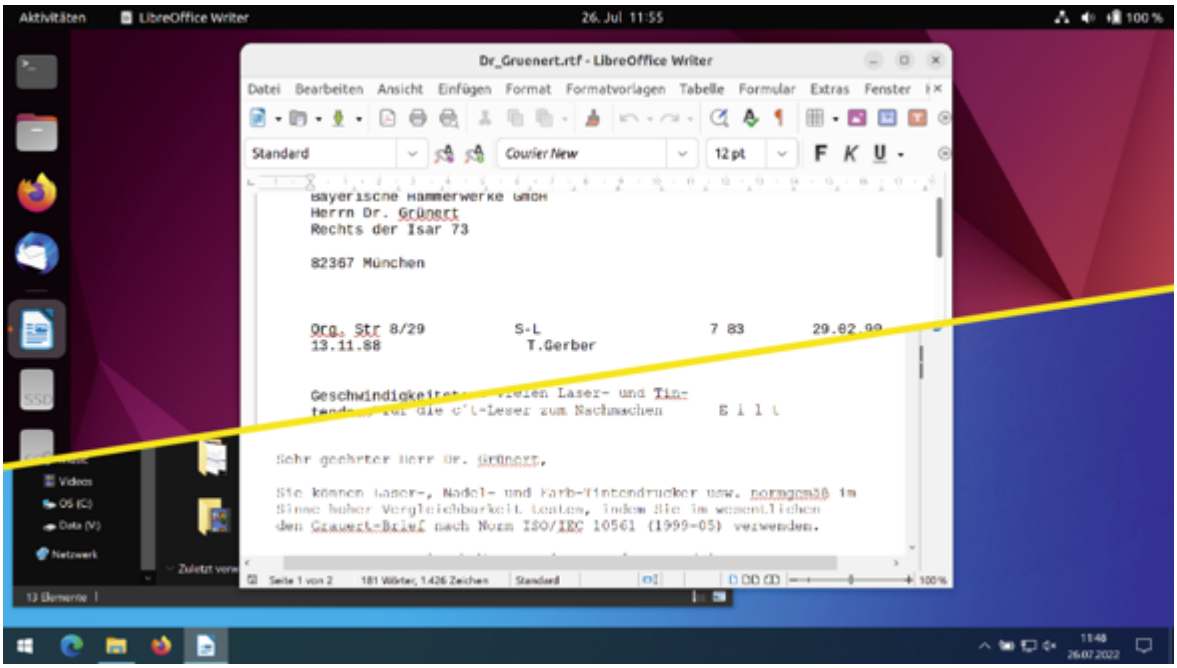
Und los!

Die Anleitungen in dieser Ausgabe helfen Ihnen durch die Einrichtung beider Betriebssysteme. Los geht es auf Seite 16, wo wir beschreiben, wie Sie Windows so schrumpfen, dass Linux sich zusätzlich installieren lässt. Der Beitrag ab Seite 22 beschreibt, wie Sie Linux verschlüsselt auf dem gleichen Datenträger installieren.

Abschließend geht es um das Entscheidende: Ihre Daten. Die lagern Sie, sofern das nicht eh schon der Fall ist, künftig getrennt vom Betriebssystem. Würden Sie die Daten auf dem Windows-Laufwerk belassen, müssten Sie später von Linux aus darauf zugreifen. Das ist eine genauso schlechte Idee wie

Windows auf Linux zugreifen zu lassen. Es bestünde in beiden Fällen die Gefahr, dass ein System das andere demoliert, was Folgen bis hin zum Datenverlust haben könnte. Die Trennung vermeidet das. Zudem ist sie die Voraussetzung dafür, dass Ihre Daten ebenfalls verschlüsselt, aber für beide Betriebssysteme erreichbar sind.

Haben Sie erst mal alle Anleitungen durchgespielt, reduziert sich die seit Jahrzehnten andauernde Diskussion um das bessere Betriebssystem für Sie auf die simple Frage, welches Betriebssystem Sie beim Einschalten des Computers starten. Und die völlig undogmatische Antwort lautet: jenes, das in diesem Moment das geeignetere ist. (*axv@ct.de*)

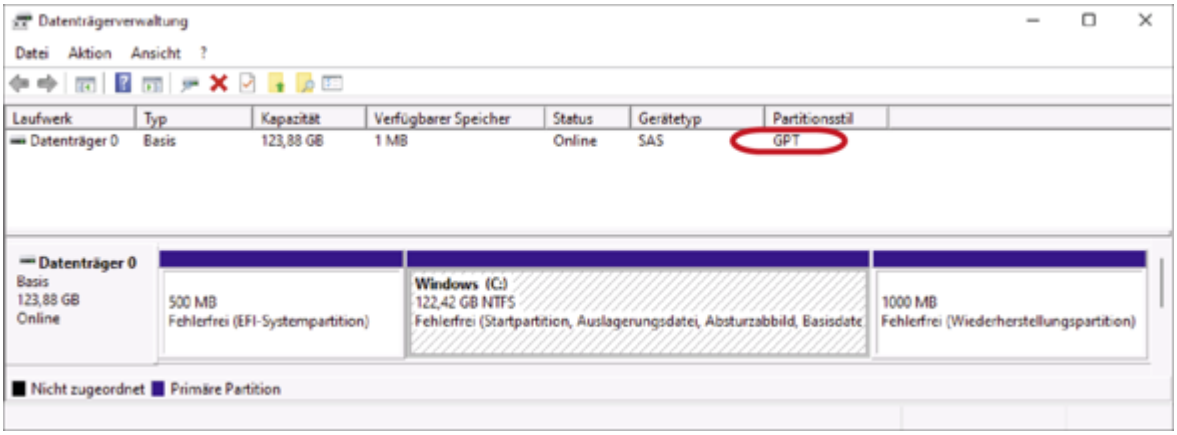


Windows und Linux laufen auf demselben PC und mit beiden Systemen können Sie Ihre verschlüsselten Dateien bearbeiten, ohne erst etwas hin und her zu kopieren.

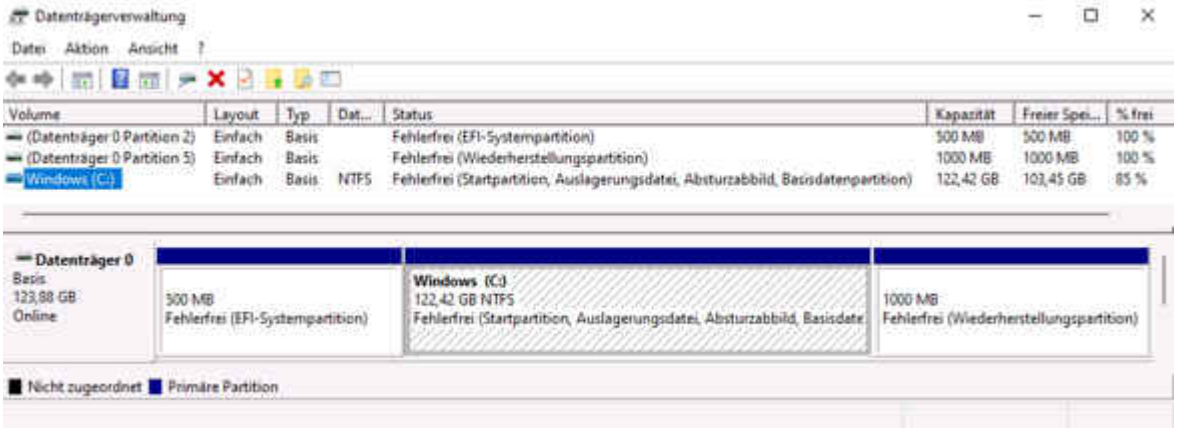
Vorbereiten

Der erste Handgriff ist derselbe wie vor vielen anderen Operationen am offenen Windows: Fertigen Sie ein Backup an. Unser Sicherungsskript c’t-WIMage [1] erstellt auf einem USB-Laufwerk eine Kopie Ihrer kompletten Windows-Installation, die Sie auf quasi jeder Windows-kompatiblen Hardware

wiederherstellen können. Wichtig wie bei jedem anderen Backup auch: Testen Sie nach dem Sichern, ob es wirklich geklappt hat. Alle nötigen Anleitungen und das Skript selbst finden Sie via ct.de/wimage.



Wenn Sie in der Datenträgerverwaltung unter Ansicht die „Anzeige oben“ auf „Datenträgerliste“ umstellen, steht in der Spalte Partitionsstil bei heutigen Computern meist „GPT“. Falls das bei Ihnen anders ist, kommt zusätzliche Arbeit auf Sie zu.



So sieht die Aufteilung eines internen Datenträgers bei einer Windows-Standardinstallation aus: Vorn die EFI-Partition mit dem Bootloader, in der Mitte die eigentliche Windows-Installation und am Ende das Rettungssystem „Windows RE“.
Der zweite Handgriff ist optional: Schaffen Sie Platz auf C:, denn je mehr Platz dort frei ist, umso mehr können Sie von C: abknapsen. Am einfachsten gelingt das mit der Windows-eigenen Datenträgerbereinigung. Die löscht temporäre Dateien, Update-Überreste und vieles mehr. Starten können Sie sie beispielsweise, indem Sie im Eigenschaften-Dialog von C: die Schaltfläche „Bereinigen“ anklicken. Klicken Sie anschließend

auf „Systemdateien bereinigen“. Dann wählen Sie kurzerhand alle Kästchen aus und lassen das Werkzeug seine Arbeit verrichten.

Noch nicht genug Platz frei? Öffnen Sie im Explorer Laufwerk C: und tippen Sie oben rechts in das Suchfeld Größe:>50M ein. Daraufhin sucht Windows alle Dateien auf C:, die größer sind als 50 MByte. Den Wert können Sie nach Belieben anpassen. Achtung: Löschen Sie von den gefundenen Dateien auf gar(!) keinen(!) Fall(!) solche, von denen Sie keine Ahnung haben, wozu sie gut sind. Denn sonst kann es passieren, dass Windows oder einzelne Anwendungen nicht mehr korrekt laufen. Entsorgen Sie also stattdessen ausschließlich, was Ihnen bekannt ist, etwa heruntergeladene Installationspakete, nicht mehr benötigte ISO-Abbilder, bereits gesehene Filme und so weiter.

Falls der Platz immer noch nicht ausreicht: Das Titelthema von c’t 8/2018 bietet gleich fünf Artikel mit vielen weiteren Tipps [2].

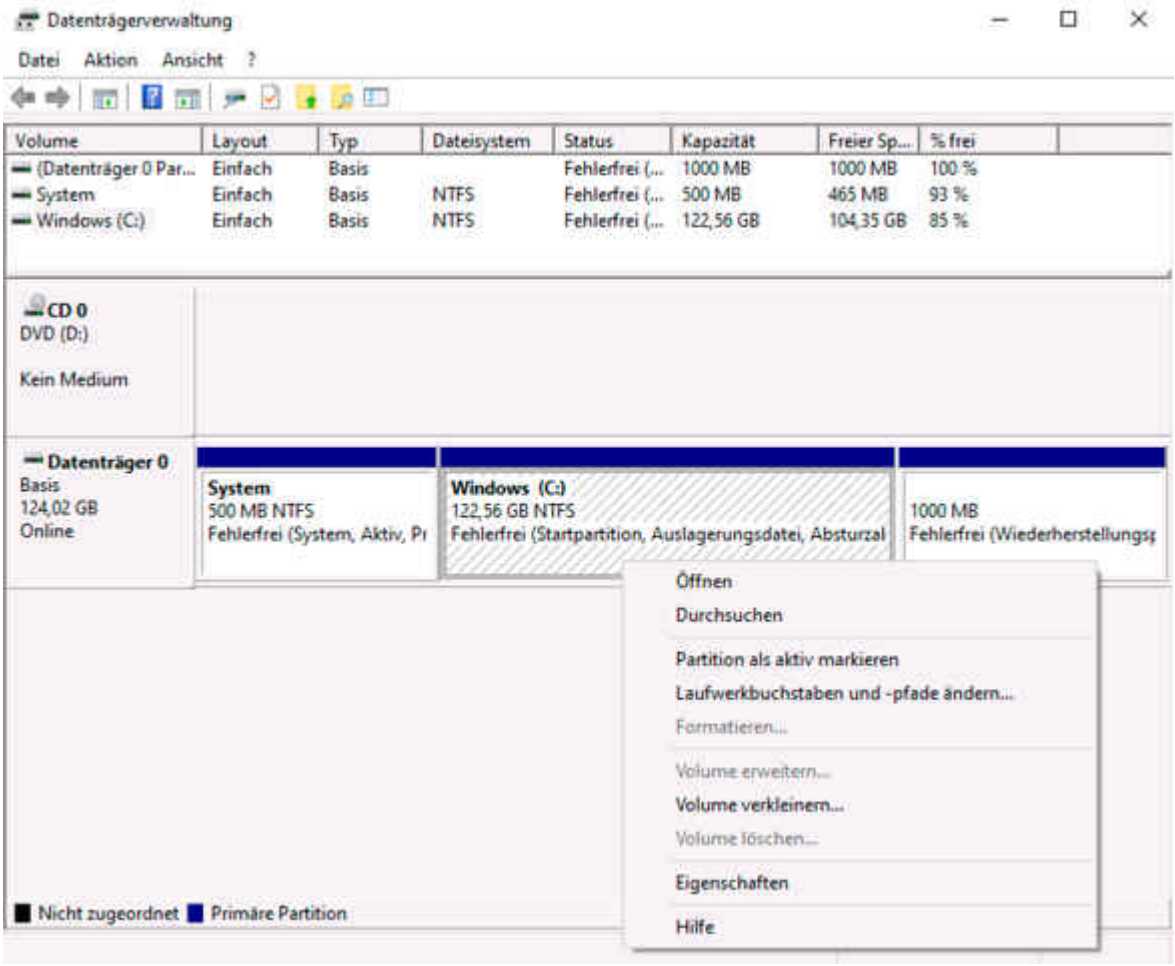
Noch ein letzter Handgriff, bevor es wirklich losgeht: Ziehen Sie alle externen Datenträger wie USB-Platten ab, um nachfolgend die Übersichtlichkeit möglichst hoch zu halten und Verwechslungen zu vermeiden. CDs und DVDs werfen sie aus. Das gilt auch für virtuell eingebundene Festplattendateien im VHD- und VHDX-Format.

Sofern C: mit BitLocker verschlüsselt ist [3], macht das nichts. Alle nachfolgend genannten Handgriffe funktionieren auch dann. Sie brauchen dafür an BitLocker also nicht herumzukonfigurieren.

Wie siehts hier denn aus?

Verschaffen Sie sich zuerst einen Überblick über die Partitionierung. Das gelingt am schnellsten mit der Windows-eigenen Datenträgerverwaltung, die unter Windows 10 und 11 gleichermaßen funktioniert (eine ausführliche Einführung haben

wir in [4] veröffentlicht). Zum Starten drücken Sie die Tastenkombination Windows+X und wählen Sie den Eintrag „Datenträgerverwaltung“.



Die Datenträgerverwaltung bringt einen Assistenten zum Verkleinern der Windows-Partition mit. Der Haken ist die RE-Partition, die hier am Ende des Datenträgers liegt.
Das Programm präsentiert oben eine detaillierte Liste mit den vorhandenen Partitionen inklusive Füllstand, Art des Dateisystems, Status, ob es BitLocker-verschlüsselt ist und so weiter. Klicken Sie in der Menüleiste unter „Ansicht/Anzeige oben“ auf „Datenträgerliste.“ In der Spalte „Partitionsstil“ steht entweder „GPT“ oder „MBR“. Die Abkürzungen stehen für die zwei Partitionsschemata, mit denen sich die Partitionen auf einem Laufwerk verwalten lassen.

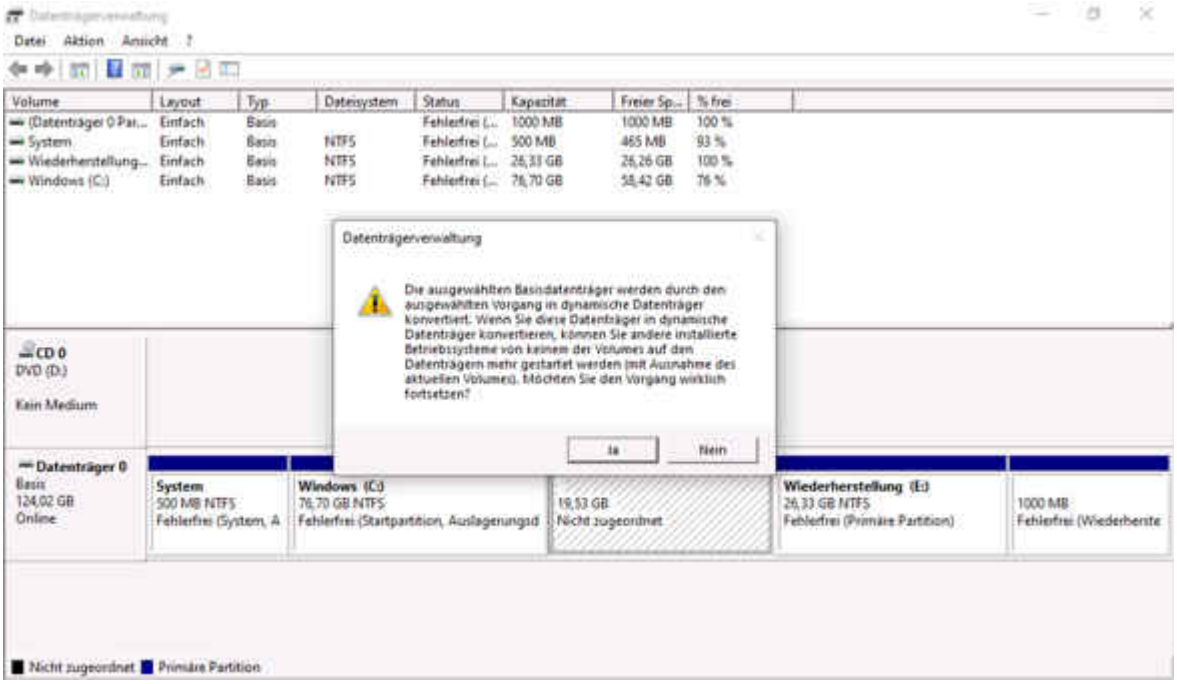
GPT ist das modernere Schema und gilt seit Jahren als Standard. Die Wahrscheinlichkeit ist daher hoch, dass Ihr Datenträger GPT-partitioniert ist, und wenn dem so ist, steht

dem Platzfreischaufeln nichts im Wege. Sie können dann im Abschnitt „Schrumpfkur“ weiterlesen.

Das MBR-Problem

Bei Ihnen steht „MBR“? Das ist unschön, denn MBR (veröffentlicht 1983) leidet an altersbedingten Einschränkungen. Die hier wichtigste: Es verzeichnet die Partitionen in einer Partitionstabelle, die für maximal vier Einträge Platz bietet (die „Primärpartitionen“). Weitere primäre Partitionen können Sie mit MBR nicht anlegen. Um Ihnen eigene zeitraubende Versuche zu ersparen, zuerst zu dem, was hier nicht hilft.

Das MBR-Partitionsschema kennt als Krücke die „erweiterte Partition“. Mit deren Hilfe lassen sich weitere Partitionstabellen mit der ersten verketten, die jeweils Platz für maximal vier weitere logische Partitionen bieten. Das ist aber nicht empfehlenswert, allein schon, weil die erweiterte Partition einen der vier Plätze in der Tabelle benötigt. Sind derzeit alle belegt, müssten Sie also zuerst eine der vorhandenen Partitionen löschen und dazu vorab die Daten von dieser Partition wegsichern. Zudem können Sie nicht frei wählen, welche primäre Partition Sie durch eine erweiterte ersetzen wollen. Denn beispielsweise der Bootloader muss zwingend in einer primären liegen. Kurzum: Lassen Sie das. (Für die Hartgesottenen unter Ihnen, die dennoch wissen wollen, wie sie eine erweitere Partition anlegen: Das geht unter Windows nur mit Diskpart per Create Partition Extended.)



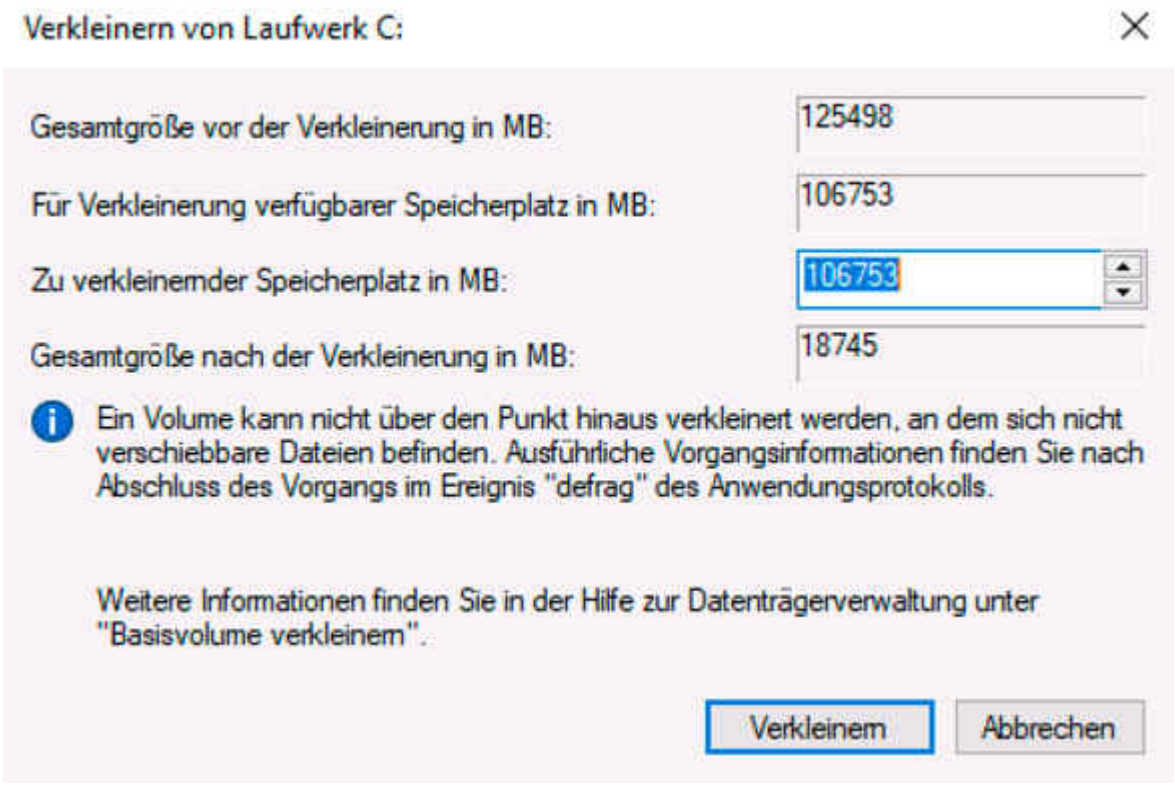
Wenn auf dem Datenträger das alte Partitionsschema MBR verwendet wird, kann das Erstellen einer weiteren Partition scheitern. Die Datenträgerverwaltung hilft dann nicht weiter.
Die Datenträgerverwaltung möchte Ihnen eine andere Krücke andrehen. Wenn Sie probieren, auf einem MBR-Datenträger eine fünfte primäre Partition zu erstellen, will sie den Datenträger in einen „dynamischen“ umwandeln. Dahinter steckt im Wesentlichen eine Microsoft-eigene RAID-Lösung. Hilft nur nichts: Selbst wenn Sie auf „Ja“ klicken, wird der Datenträger trotzdem nicht umgewandelt. Stattdessen beschwert sich Windows mit einer Fehlermeldung über Platzmangel. Es fehlt ja unverändert Platz für einen weiteren Eintrag in der Partitionstabelle.

Zum Glück gibt es eine Lösung, die wirklich funktioniert: Ersetzen Sie das MBR-Partitionsschema durch GPT, denn damit sind mindestens 128 Partitionen verwaltbar. Der Haken: Mit dem Umstellen von MBR auf GPT allein ist es nicht getan. Der PC muss anschließend auch UEFI- statt Legacy-BIOS-Mechanismen zum Hochfahren nutzen, sonst bootet Windows nicht mehr. Zwei Methoden zum Umstellen haben wir in c’t bereits vorgestellt, was aber jeweils einen ganzen Artikel füllte. Die erste: Windows hat das Kommandozeilenwerkzeug „MBR2GPT.exe“ an Bord, mit dem das Vorhaben gelingt – jedenfalls dann, wenn diverse

Voraussetzungen erfüllt sind und Sie einige Bugs umschiffen [5]. Die zweite: Verwenden Sie unser bereits erwähntes Sicherungsskript c't-WIMage. Dann springt im Rahmen der Umstellung auch gleich noch eine Sicherungskopie Ihrer Windows-Installation für Sie heraus. Wie die Umstellung mit c't-WIMage gelingt, steht ausführlich in [6].

Schrumpfkur

Nun zum Verkleinern der Windows-Partition. Das erledigen Sie in der Datenträgerverwaltung. Wählen Sie in der unteren Fensterhälfte „Volume Verkleinern …" aus dem Kontextmenü der Windows-Partition. Falls Sie sich wundern, warum Windows scheinbar identische Bereiche des physischen Datenträgers mal als „Partition" und mal als „Volume" bezeichnet: Eine Partition belegt einen ganzen oder nur einen Teil eines physischen Datenträgers, kann sich aber nicht über mehrere erstrecken. Eine Partition enthält wiederum ein Volume, wobei es sich um das eigentliche logische Laufwerk handelt. In den meisten Fällen füllt ein Volume eine komplette Partition. Doch es kann sich auch über mehrere Partitionen erstrecken, die sogar wie bei einem RAID oder Storage Space auf unterschiedlichen Datenträgern liegen dürfen.



Der Assistent zum Verkleinern will nicht die Zielgröße wissen, sondern um wie viele MBytes die Partition verkleinert werden soll.
Nach dem Anklicken von „Volume verkleinern“ startet ein Assistent, der mehrere Werte anzeigt, von denen Sie einen verändern können: „Zu verkleinernder Speicherplatz in MB“. Sie wählen also nicht die Zielgröße des Laufwerks, sondern die Anzahl an MByte, die am hinteren Ende abgeschnitten werden. Der Assistent bietet den Maximalwert an, der vom Füllstand abhängt (die zu Windows-7-Zeiten geltende Beschränkung auf maximal die Hälfte spielt heute keine Rolle mehr).

Wie weit Sie das Windows-Volume verkleinern, hängt von zweierlei ab: Erstens muss Windows hinterher noch drauf passen. Wie viel Platz die Installation belegt, können Sie im Explorer in den Eigenschaften von C: ablesen. Doch dieser Platz allein reicht nicht: Windows braucht zusätzlich im laufenden Betrieb freien Platz beispielsweise für temporäre Dateien und Updates, und das gilt auch für viele Anwendungen. Als Minimum dafür gelten 20 GByte, ziehen Sie also im Assistenten vom vorgegebenen Maximalwert mindestens 20.000 MByte ab. Wenn möglich ist, reduzieren Sie den Wert weiter.

Mehr als 100 GByte freier Platz auf der Windows-Partition ist aber unnötig. Grübeln Sie über den Wert lieber eine Minute länger als zu kurz, denn nachträgliche Änderungen sind zwar machbar, aber nur mit viel Aufwand.

Sie haben einen zufriedenstellenden Wert eingetragen? Ein Klick auf „Verkleinern“ lässt den Assistenten die Schrumpfkur erledigen. In der Datenträgerverwaltung erscheint nun hinter der verkleinerten Windows-Partition ein Bereich „Nicht zugeordnet“ mit einem schwarzen Balken darüber .

Das RE-Problem

An sich können Sie den gerade freigeschaufelten Platz seiner neuen Bestimmung zuführen. Doch lesen Sie stattdessen besser erst noch diesen Abschnitt. Denn außer der Windows-Partition gibt es noch eine weitere, die Ihrer Aufmerksamkeit bedarf. Sie enthält die Wiederherstellungsumgebung „Windows RE“ (Recovery Environment, [7]), von der Sie üblicherweise nur dann etwas bemerken, wenn Windows Probleme beim Booten hat. Bei RE handelt es sich um ein eigenständiges kleines Betriebssystem, welches der Bootloader bei Problemen automatisch startet. Es liegt in einer separaten Partition, die hier nachfolgend RE-Partition heißt.

Wie Windows selbst entwickelt Microsoft auch Windows RE immer weiter, und wie Windows wird auch RE immer größer. Als Folge wächst auch die separate RE-Partition – wenn nicht jetzt, dann irgendwann in der Zukunft, und zwar jeweils im Rahmen eines Versions-Upgrades. Die finden derzeit ungefähr jährlich statt. Wenn es so weit ist, passt Windows die Partitionierung im laufenden Betrieb an. Was dabei herauskommt, hängt von diversen Faktoren ab, die zu erläutern hier zu weit führt (Details in [8]). Scheitert Windows beim Anpassen, startet RE schlimmstenfalls nach einem Versionssprung gar nicht mehr oder nur dann, wenn C: nicht mit BitLocker verschlüsselt ist. Auch Defekte des Bootmenüs des Bootloaders sind denkbar, vor allem bei der Installation eines weiteren Betriebssystems, dessen

Entwickler RE und seine Besonderheiten nicht berücksichtigen. Es können zudem zusätzliche Partitionen entstehen, die Platz verschwenden.

Damit Windows beim Vergrößern der RE-Partition nicht scheitert, muss die RE-Partition direkt hinter der Windows-Partition liegen. Dann kann Windows bei Bedarf die RE-Partition löschen, die Windows-Partition etwas verkleinern und in dem so entstandenen freien Platz hinter der Windows-Partition eine neue, nun eben etwas größere RE-Partition anlegen. Die liegt dann wieder direkt hinter der Windows-Partition.

RE verschieben

Zuerst in Kurzform, was zu tun ist, um Probleme mit der RE-Partition zu vermeiden: Deaktivieren Sie RE, woraufhin das komplette Mini-Betriebssystem vorübergehend von der RE- auf die Windows-Partition verschoben wird (es besteht ohnehin nur aus einer einzigen Datei, die beim Start von RE vorübergehend ins RAM entpackt wird). Erstellen Sie hinter der bereits geschrumpften Windows- eine neue RE-Partition und löschen Sie die alte. Zum Abschluss reaktivieren Sie RE, woraufhin es funktionstüchtig an seinem neuen Speicherplatz landet.

Nun zur Langform. Das Prozedere erfordert nicht nur Mausklicks, sondern auch einzutippende Kommandozeilenbefehle. Über ct.de/yxb1 finden Sie eine kleine Textdatei, aus der Sie alle Befehle herauskopieren können. Das Nachfolgende geht davon aus, dass Sie die Windows-Partition bereits wie oben beschrieben geschrumpft haben. Falls nicht, holen Sie das zuerst nach.

Los geht es in der Datenträgerverwaltung: Sehen Sie nach, auf welchem Datenträger die Windows-Partition liegt. Das erkennen Sie ganz links an der Bezeichnung „Datenträger X“, wobei X für eine Zahl steht, beginnend bei 0. Merken Sie sich die Zahl, die hinter „Datenträger“ steht.

Drücken Sie Windows+X. Wählen Sie aus dem Systemmenü je nachdem, was da ist: „Eingabeaufforderung (Administrator)“, „PowerShell (Administrator)“ oder „Terminal (Administrator)“. Tippen Sie darin den Befehl ein:

```
Reagentc /disable
```

Der Befehl deaktiviert RE. Sollte es dabei zu Fehlermeldungen kommen, liegt das üblicherweise nicht an der RE-Partition, sondern an Windows RE selbst. Hilfe und viele Tipps zum Beheben solcher Probleme finden Sie dann in [9].

Starten Sie den Kommandozeilenpartitionierer Diskpart (Einführung in [10]):

```
Diskpart
```

Wählen Sie den Datenträger mit der Windows-Partition, die Zahl ersetzen Sie durch die, die Sie in der Datenträgerverwaltung abgelesen haben:

```
Select Disk 0
```

Die nächsten beiden Befehle erzeugen eine rund 1 GByte große Partition mit dem Dateisystem NTFS und der eindeutigen Bezeichnung „ctRecovery“:

```
Create Partition Primary Size=1000
Format Quick FS=NTFS Label="ctRecovery"
```

Die Bezeichnung können Sie frei wählen, wichtig ist nur, dass sie eindeutig ist. Das hilft später beim Identifizieren und Löschen der alten RE-Partition.

Damit Windows die neue Partition als RE-Partition erkennt, passen die folgenden zwei Befehle den Partitionstyp an (hier für GPT):

```
Set ID=de94bba4-06d1-4d40-a16a-bfd50179d6ac
GPT Attributes=0x8000000000000001
```

Sollte der Datenträger entgegen unserer Empfehlung noch MBR-

partitioniert sein, reicht stattdessen ein einzelner Befehl: Set ID=27.

Alte RE-Partition löschen

Nun können Sie die alte RE-Partition löschen. Dazu benötigen Sie ebenfalls Diskpart. Verschaffen Sie sich zuerst einen Überblick über die vorhandenen Partitionen:

```
List Partition
```

Suchen Sie in der Liste nach Partitionen mit Namen wie „Wiederherstellung“ oder „Recovery“. Bei einer solchen kann es sich um die alte RE-Partition handeln, muss aber nicht. Auf PCs mit vom Hersteller vorkonfigurierten Windows sind oft weitere Partitionen mit ähnlichen oder gar identischen Namen vorhanden. Die enthalten beispielsweise herstellereigene Wiederherstellungswerkzeuge, die vom Windows-eigenen RE unabhängig funktionieren, oder Installationspakete der mitgelieferten Anwendungen und Treiber für den Fall, dass der Kunde selbst Windows neu installieren will. Images zum Wiederherstellen des Auslieferungszustands legten PC-Hersteller früher ebenfalls gern in separaten Partitionen ab, gesehen haben wir sowas aber schon länger nicht mehr.

Die alte RE-Partition erkennen Sie am Namen, am Dateisystem NTFS und an der Größe von rund 1 bis 2 GByte oder kleiner – Wiederherstellungspartitionen der PC-Hersteller sind um ein Vielfaches größer.

Der Befehl List Partition listet für jede Partition eine Nummer auf (ab 1 hochzählend). Suchen Sie die für die alte RE-Partition. Folgende Befehle wählen sie aus und zeigen deren Details an (X an die Partitionsnummer anpassen):

```
Select Partition X
Detail Partition
```

Steht nach dem Abschicken des zweiten Befehls in der Ausgabe eine Zeile namens Typ: de94bba4-06d1-4d40-a16a-bfd50179d6ac

und weiter unten eine andere (!) Bezeichnung als die oben von Ihnen vergebene „ctRecovery“, haben Sie die richtige Partition erwischt. Diese kryptische Typ-ID ist auf GPT-Datenträgern RE-Partitionen vorbehalten (bei MBR-Datenträgern steht hier stattdessen Typ: 27).

Sie löschen die alte RE-Partition mit diesem Befehl (X an die Partitionsnummer anpassen):

Delete Partition Override

Lag die alte Partition bislang vor Windows, entsteht dort freier, aber nicht nutzbarer Platz, woran sich mit Windows-Bordmitteln leider nichts ändern lässt. Nun beenden Sie Diskpart durch Eingabe von Exit und reaktivieren Windows RE durch Eingabe von Reagentc /enable. Ob das geklappt hat, offenbart Reagentc /info, bei Problemen sei erneut auf [8] verwiesen.

(Fast) fertig

Das Wesentliche ist geschafft: Die Windows-Partition ist geschrumpft und die RE-Partition liegt trotzdem wieder direkt dahinter. Die nächsten Handgriffe hängen von Ihrem Vorhaben ab.

Soll der freie Platz lediglich zur Aufnahme einer separaten Datenpartition dienen, öffnen Sie ein weiteres Mal die Datenträgerverwaltung. In der unteren Fensterhälfte finden Sie im Kontextmenü des leeren, mit einem schwarzen Balken markierten Rechtecks den Eintrag „Neues einfaches Volume …“. Ein Klick darauf startet einen weiteren Assistenten, in dem Sie nacheinander die Größe, den künftigen Laufwerksbuchstaben und die „Volumebezeichnung“ festlegen können. Alles andere wie das Dateisystem (NTFS) ist sinnvoll vorbelegt, für Änderungen sollten Sie einen guten Grund kennen (Neugier ist keiner). Wenn der Assistent fertig ist, ist das neue logische Laufwerk bereit.

Anders sieht es aus, wenn Sie zusätzlich Linux installieren und Ihre Daten zudem verschlüsseln wollen. Dann geht es nun weiter für Sie mit den nachfolgenden Artikeln. *(axv@ct.de)*

1. Literatur
2. Axel Vahldiek, Ersatzrad, c’t-WIMage erstellt Windows-Backups, c’t 10/2021, S. 18
3. Axel Vahldiek, Windows entschlacken, Titelthema von c’t 8/2018, S. 66
4. Jan Schüßler, FAQ: BitLocker, c’t 17/2018, S. 173, auch kostenlos online lesbar unter ct.de/-4122147
5. Axel Vahldiek, Plattenteiler, Partitionieren mit Windows-Bordmitteln – Teil 1: Datenträgerverwaltung, c’t 2/2018, S. 154
6. Axel Vahldiek, Anders hochfahren, Windows 10 von klassischem Start auf UEFI-Boot umstellen, c’t 14/2019, S. 162
7. Axel Vahldiek, Starker Helfer, PC-Umzug mit c’t-WIMage, c’t 6/2019, S. 22
8. Axel Vahldiek, Aufstehhelfer, Wie Windows Startprobleme selber löst, c’t 5/2018, S. 74
9. Axel Vahldiek, Wo ist sie, und wenn ja, wie oft?, Windows RE und die Recovery-Partition, c’t 18/2021, S. 162
10. Axel Vahldiek, Hilfe für den Helfer, Windows RE prüfen und reparieren, c’t 5/2018, S. 80
11. Axel Vahldiek, Tipp-Schnippler, Partitionieren mit Windows-Bordmitteln – Teil 2: Diskpart, c’t 3/2018, S. 144

Befehle.txt: ct.de/yxb1

Mitbewohner

Debian und Ubuntu verschlüsselt neben Windows installieren

Ein voll verschlüsseltes Dateisystem schützt Ihre sensiblen Daten auf Notebook und Desktop selbst bei einem Diebstahl des Computers. Bei der Linux-Installation gelingt das aber nur, wenn sich Linux auf der ganzen Festplatte breitmachen darf. Wir verraten Ihnen die nötigen Kniffe, mit denen sich Debian und Ubuntu harmonisch neben Windows einfügen und trotzdem ihre Dateisysteme verschlüsseln.

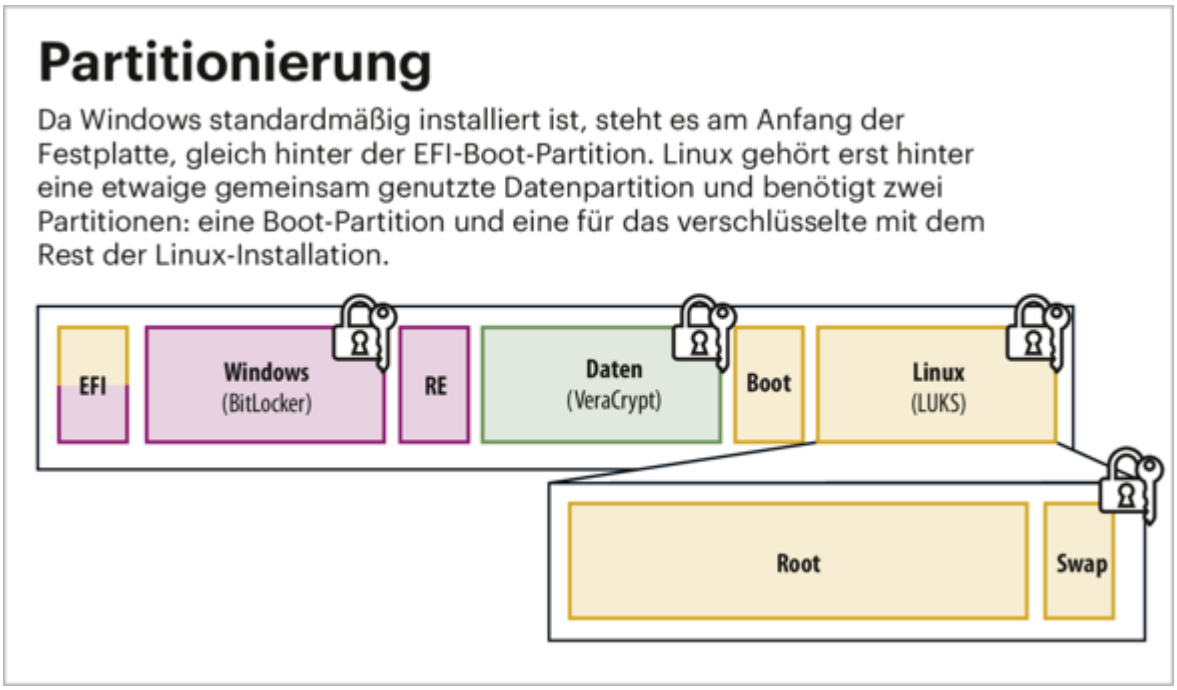
Von Mirko Dölle

Verschlüsselte Betriebssysteminstallationen gehören heute zum guten Ton, so gelangen selbst bei Diebstahl des Computers keine Daten in die falschen Hände. Viele Linux-Distributionen bieten seit Langem voll verschlüsselte Installationen an, jedoch nur dann, wenn sie die gesamte Festplatte für sich beanspruchen dürfen – so auch bei den Installationsprogrammen von Debian 11 und Ubuntu 22.04. Haben Sie Windows parallel installiert, müssen Sie entweder auf die Verschlüsselung verzichten oder sich der nachfolgend beschriebenen Tricks bedienen.

Während es beim eher spartanischen Debian genügt, sich im Installer ein paar Mal im Kreis zu drehen, müssen Sie sich beim ansonsten komfortableren Ubuntu auf der Kommandozeile abmühen, damit sich Linux geschmeidig neben Windows einfügt und trotzdem die Partitionen als LUKS (Linux Unified Key Setup) verschlüsselt. Da Windows auf praktisch allen Rechnern vorinstalliert ist, beginnen Sie damit, Ihre Windows-Installation zu verkleinern und so Platz für Linux zu schaffen. Dazu sollten Sie unbedingt die auf Seite 16 beschriebene Methode mit Windows-Bordmitteln verwenden und

nicht etwa das Partitionierungsprogramm Gparted unter Linux – denn bei Letzterem würden Sie einen Keil zwischen Windows und das Recovery-System treiben.

Damit ergibt sich die rechts oben gezeigte Aufteilung der Festplatte respektive SSD: Am Anfang steht die EFI-Boot-Partition, die Windows und Linux gemeinsam nutzen, dahinter Windows und RE. Wollen Sie später auf Ihre Daten sowohl von Linux und Windows aus zugreifen, wie dies auf Seite 28 beschrieben ist, folgt hinter den beiden Windows-Partitionen die Datenpartition. Dahinter schaffen Sie dann freien, nicht zugeordneten Platz für Linux. Wie viel Platz Sie für Linux benötigen, hängt sehr von der späteren Nutzung ab. Weniger als 50 GByte sollten es nicht sein, auch dann nicht, wenn Sie wie auf Seite 28 beschrieben eine gemeinsame Datenpartition für den Großteil Ihrer Dateien benutzen. Wollen Sie später Spiele installieren, müssen Sie das in jedem Fall einkalkulieren – manche benötigen 100 GByte und mehr für die Installation.



Der Knackpunkt bei der Partitionierung besteht darin, dass Debian und Ubuntu eine verschlüsselte LVM-Gruppe (Logical Volume Management) benutzen, um alle für den Betrieb benötigten (logischen) Laufwerke anzulegen. Dazu gehören mindestens das Root-Dateisystem und Swap, der

Auslagerungsbereich für das RAM. So muss beim Start nur eine Partition entschlüsselt werden, die mit der LVM-Gruppe. Das wiederum erfordert, dass Bootloader Grub, Kernel und die Initial Ramdisk (initrd) auf einer unverschlüsselten Boot-Partition gespeichert sind. Ohne Unterstützung durch die Installationsprogramme müssen Sie die korrekte Partitionierung Schritt für Schritt selbst anlegen. Dies ist absurderweise beim wenig ausgefeilten Debian-Installer einfacher als unter Ubuntu.

Startschuss für Debian

Bei der Debian-Installation folgen Sie einfach dem vorgezeichneten Weg so weit, bis Sie gefragt werden, wo Debian installiert werden soll. Da der Installer die Installation mit einem verschlüsselten LVM nur für den Fall anbietet, wenn Sie die ganze Festplatte für Debian benutzen, wählen Sie hier „Manuell“ aus und finden sich in der Übersicht der Partitionen wieder.

Die nächsten Schritte führen Sie immer wieder zurück zu dieser Übersicht. Manchmal gibt es mehrere Optionen mit scheinbar der gleichen Funktion, folgen Sie dann bitte unserer Anleitung – sonst müssen Sie die Installation schlimmstenfalls wiederholen.

Der erste Schritt ist, eine Boot-Partition im freien Speicherbereich hinter Windows anzulegen. Diese sollte 1 GByte groß sein, damit Platz für mehrere Kernel-Versionen ist. Als Dateisystem verwenden Sie ext4, der Einbindepunkt ist /boot und als Namen sollten Sie den Hostnamen Ihres Rechners gefolgt von „-boot“ verwenden. Also zum Beispiel „debian-boot“, falls Sie den Standard-Hostnamen übernommen haben. Indem Sie möglichst alle Partitionen benennen, behalten Sie leichter den Überblick.

Zurück in der Übersicht der Partitionen wählen Sie den Menüpunkt „Verschlüsselte Datenträger konfigurieren“, um die

Partition für die LVM-Gruppe zu erstellen. Dort wählen Sie den freien Bereich hinter der gerade erstellten Boot-Partition aus, die sie leicht am Dateisystem ext4 in der Liste erkennen. Als Namen empfehlen wir den Hostnamen plus „-crypt“. Erst wenn Sie die Änderungen auf die Festplatte schreiben lassen und „Fertigstellen“ ausgewählt haben, fragt der Installer das Passwort ab und verschlüsselt die Partition. Und wieder landen Sie in der Übersicht der Partitionen, wo die gerade angelegte Partition mit dem Typ „crypto“ aufgeführt ist.

Vor und zurück, vor und zurück: Bis Sie alle für ein verschlüsseltes Debian-System benötigten Partitionen und Laufwerke angelegt haben, landen Sie immer wieder in der Übersicht der Partitionen.

Verschlüsselt, logisch?

Nun können Sie den „Logical Volume Manager konfigurieren“. Auch die „Übersicht der aktuellen LVM-Konfiguration“ werden Sie ebenfalls mehrfach betreten müssen; der erste Schritt besteht darin, eine „Volume-Gruppe“ zu erstellen. Darin

sollten Sie wiederum den Hostnamen Ihres Rechners verwenden – denn das tut auch der Debian-Installer, wenn Sie die ganze Festplatte verschlüsseln lassen. Als physisches Laufwerk für das LVM wählen Sie die gerade erstellte Crypto-Partition aus, die Sie an dem Namenszusatz „-crypt“ erkennen – sie steht normalerweise am Anfang der Liste.

Damit landen Sie erneut in der LVM-Übersicht, wo Sie nun den Eintrag „Logisches Volume erstellen“ vorfinden. Das erste logische Laufwerk, das Sie anlegen, ist für das Root-Dateisystem. Dazu wählen Sie die gerade erstellte Volume Group aus und geben dem logischen Laufwerk den Namen „root“. Bei der Größe sollten Sie mindestens 8192 MByte (8 GByte) für Swap abziehen.

Und wieder landen Sie in der Übersicht der LVM-Konfiguration, wo Sie den noch freien Platz in ein weiteres logisches Laufwerk stecken, diesmal mit dem Namen „swap_1“. Das Laufwerk könnte auch anders heißen, „swap_1“ ist jedoch der Name, den der Debian-Installer standardmäßig für den ersten Auslagerungsbereich bei einer verschlüsselten Installation verwendet.

Die Einrichtung des verschlüsselten LVM ist damit komplett, weshalb Sie sie über „Fertigstellen“ verlassen und schon wieder zur Übersicht der Partitionen zurückkehren. Allerdings weiß der Debian-Installer noch nicht, was er mit den logischen Laufwerken anfangen soll. Deshalb wählen Sie zunächst aus der Liste das logische Laufwerk für Swap aus, klicken auf „Weiter“ und stellen bei „Benutzen als“ „Auslagerungsspeicher (Swap)“ ein.

Jetzt fehlt nur noch das Root-Dateisystem: Zurück in der Übersicht wählen Sie das logische Laufwerk „root“ und klicken wiederum auf „Weiter“, um es als „Ext4“ zu verwenden. Als „Einbindungspunkt“ suchen Sie „/“ aus der Liste heraus und geben der neuen Partition den Hostnamen gefolgt von „-root“, analog zur Boot-Partition.

Damit ist der schwierige Teil der Installation abgeschlossen. Klicken Sie auf „Partitionierung beenden und Änderungen übernehmen“ und dann auf „Weiter“, um den Installer den Rest der Arbeit erledigen zu lassen. Den Abschluss der Debian-Installation bildet ein Neustart, woraufhin Sie dann die Wahl zwischen Debian und Windows haben.

Handarbeit bei Ubuntu

Die Ursache für den Mehraufwand bei der Ubuntu-Installation liegt darin, dass der Ubuntu-Installer bei der manuellen Partitionierung kein LVM unterstützt. Diesen Teil der Arbeit müssen Sie deshalb von Hand im Terminal erledigen. Außerdem bekommt der Installer nicht mit, dass Sie ein verschlüsseltes System einrichten, weshalb Sie auch konfigurieren müssen, dass das Root-Dateisystem beim Booten erst entschlüsselt wird.

Doch der Reihe nach: Wenn Sie Ubuntu vom USB-Stick starten, wählen Sie unbedingt „Ubuntu ausprobieren“ – nur so können Sie in den Installationsprozess eingreifen und zu gegebener Zeit das LVM über das Terminal von Hand konfigurieren. Am Desktop angekommen starten Sie die Installation und folgen dem vorgezeichneten Weg, bis Sie auswählen sollen, wo Ubuntu installiert werden soll.

Komfort gibt es nur, wenn Sie Ubuntu unverschlüsselt oder auf der ganzen Festplatte installieren lassen. Deshalb wählen Sie „Etwas Anderes“ und kümmern sich anschließend selbst um die Partitionierung. Die EFI-Boot-Partition hat Windows bereits angelegt, damit müssen Sie sich nicht weiter befassen. Allerdings benötigt Ubuntu eine eigene Boot-Partition, wir empfehlen dafür mindestens 1 GByte. Lassen Sie sie mit dem Dateisystem ext4 formatieren und unter /boot einbinden.

Im nächsten Schritt legen Sie die Partition für das verschlüsselte Linux-System an. Dabei ist entscheidend, dass Sie unter „Benutzen als“ „physikalisches Volume für Verschlüsselung“ auswählen. Daraufhin erweitert sich der

Dialog um die Passphrase-Abfrage. Sobald Sie den Dialog mit „OK“ bestätigen, verschlüsselt der Installer die Partition unmittelbar, bindet sie unterhalb von /dev/mapper ein und schickt Sie zurück zur Übersicht der Partitonen.

Auf Befehl

Es dauert bis zu einer halben Minute, bis die Partitionstabelle aktualisiert ist und das verschlüsselte Dateisystem als erster Eintrag in der Liste auftaucht. Nun ist es an der Zeit, das Terminal-Programm zu öffnen und das LVM einzurichten. Beginnen Sie damit, die Volume Group vgubuntu anzulegen:

```
sudo vgcreate vgubuntu \
  /dev/mapper/*_crypt
```

Wie viel Platz Sie im LVM haben, verrät Ihnen der Befehl pvdisplay --units m in ganzen Megabytes. Ziehen Sie davon mindestens 8192 MByte für Swap ab, den Rest können Sie mit dem Logical Volume für das Root-Dateisystem belegen:

```
sudo lvcreate -n root \
  -L 200000m vgubuntu
```

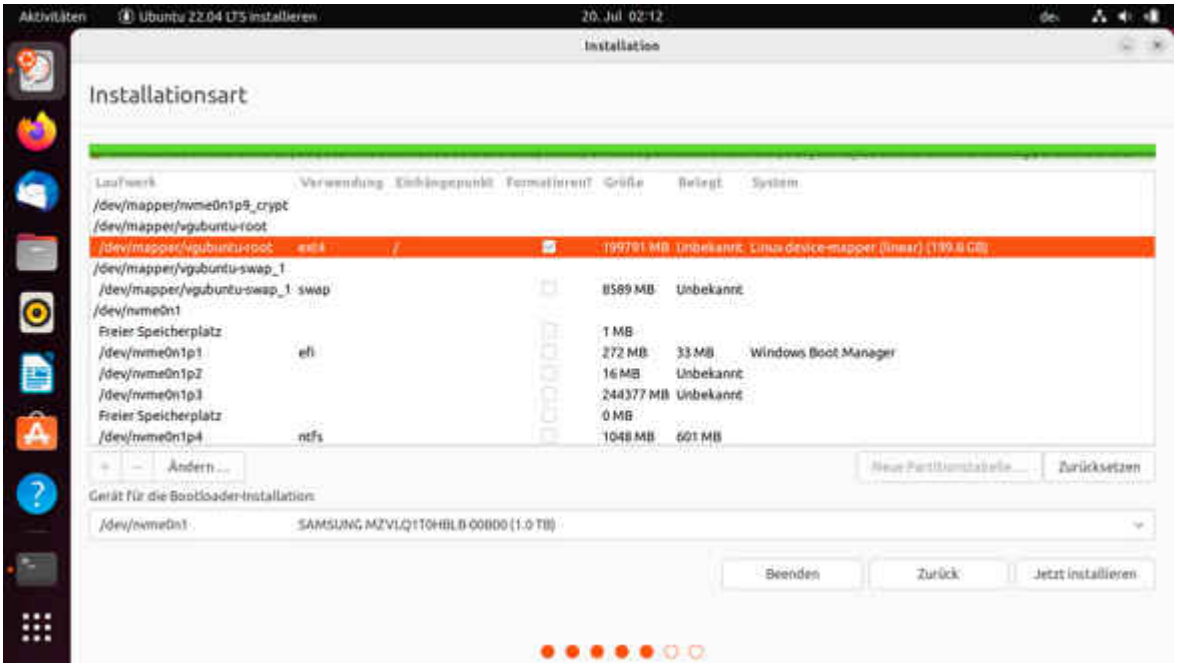
Was noch frei ist, stecken Sie in das Volume „swap_1“:

```
sudo lvcreate -n swap_1 \
  -l 100%free vgubuntu
```

Damit die Einstellungen wirksam werden, übernehmen Sie sie mit dem Befehl sudo vgchange -ay und kehren zum Installer zurück.

In der Partitionsübersicht des Installers klicken Sie nun auf „Zurück“, womit Sie wieder bei der Frage landen, wo Sie Ubuntu installieren wollen. Wählen Sie dort erneut „Etwas Anderes“ und klicken Sie auf „Weiter“ – so erzwingen Sie, dass der Installer die Partitionierung aktualisiert und auch das LVM erkennt. Nun tauchen am Anfang der Liste auch die gerade angelegten logischen Volumes auf. Indem Sie auf den Eintrag

„vgubuntu-root“ respektive „vgubuntu-swap_1“ und dann auf „Ändern“ klicken, lassen Sie das Root-Dateisystem als „Ext4-Journaling-Dateisystem“ formatieren und unter „/“ einbinden; bei Swap müssen Sie lediglich „Auslagerungsspeicher (Swap)“ wählen.



Der Ubuntu-Installer erlaubt es nicht, ein LVM von Hand einzurichten – weshalb Sie diese Schritte im Terminal erledigen müssen. Gibt es ein solches LVM, erkennt es der Installer und erlaubt Ihnen auch, es einzubinden.

Nachgeholfen

Vergessen Sie nicht, die Boot-Partition noch einmal als „Ext4-Journaling-Dateisystem“ zu formatieren und unter „/boot“ einbinden zu lassen: Weil Sie den Partitionierungsdialog verlassen hatten, hat der Installer Ihre früheren Angaben verworfen. Da sich der Installer auch nicht gemerkt hat, dass Sie mit einem verschlüsselten System arbeiten, trägt er die LUKS-Partition auch nicht in der Datei /etc/crypttab auf dem neuen System ein. Als Folge ignoriert das neu installierte System beim Booten die verschlüsselte Partition, findet kein Root-Dateisystem und kann deshalb nicht starten.

Dieses Problem müssen Sie ebenfalls im Terminal lösen, und zwar während der Installer das neu installierte System noch

bearbeitet. Klicken Sie auf „Jetzt installieren“ und bestätigen Sie die Änderungen noch einmal. Während der Installer nun im Hintergrund Dateien kopiert und Pakete installiert, fragt er bereits die Zeitzone ab. Warten Sie einige Minuten, bis die Aktivitäten auf der Festplatte abnehmen. Dann wechseln Sie noch einmal ins Terminal, wo Sie in der crypttab die UUID der verschlüsselten Partition eintragen.

Die UUID besorgen Sie sich zum Beispiel mit dem Befehl

sudo blkid /dev/sda3

falls Sie /dev/sda3 als „physikalisches Volume für Verschlüsselung“ ausgewählt hatten.

Das Root-Dateisystem des neuen Ubuntu ist während der Installation unterhalb des Verzeichnisses /target eingebunden. Mit dem Befehl sudo pico /target/etc/crypttab legt der Editor Pico die Datei neu an und Sie tragen dort folgende Zeile ein:

sda3_crypt UUID=21e8...cf15 none luks,discard

Ist /dev/sda3 nicht Ihre verschlüsselte Partition, müssen Sie den Namen „sda3_crypt“ anpassen – er beginnt stets mit dem Partitionsnamen und endet mit „_crypt“. Die UUID haben wir nur verkürzt abgedruckt, da Ihre ohnehin eine andere ist. Den Rest der Zeile übernehmen Sie 1:1.

Speichern Sie die Datei mit Strg+O, raus aus dem Editor geht es mit Strg+X. Anschließend müssen Sie im Terminal mit folgenden Befehlen die „Initial Ramdisk“ neu bauen lassen:

```
for d in dev sys proc; do
  sudo mount --bind /${d} /target/${d}
done
sudo chroot /target \
  update-initramfs -k all -c
for d in dev sys proc; do
  sudo umount /target/${d}
done
```

Etwaige Meldungen über fehlende Firmware-Dateien können Sie ignorieren. Danach können Sie das Terminal schließen. Zurück im Installer folgen Sie den Dialogen, bis die Installation abgeschlossen ist. Haben Sie den Rechner neu gestartet, empfängt Sie Ihr nun schlüsselfertiges Ubuntu mit der Frage nach dem Passwort Ihres Systems.

Zeitreise

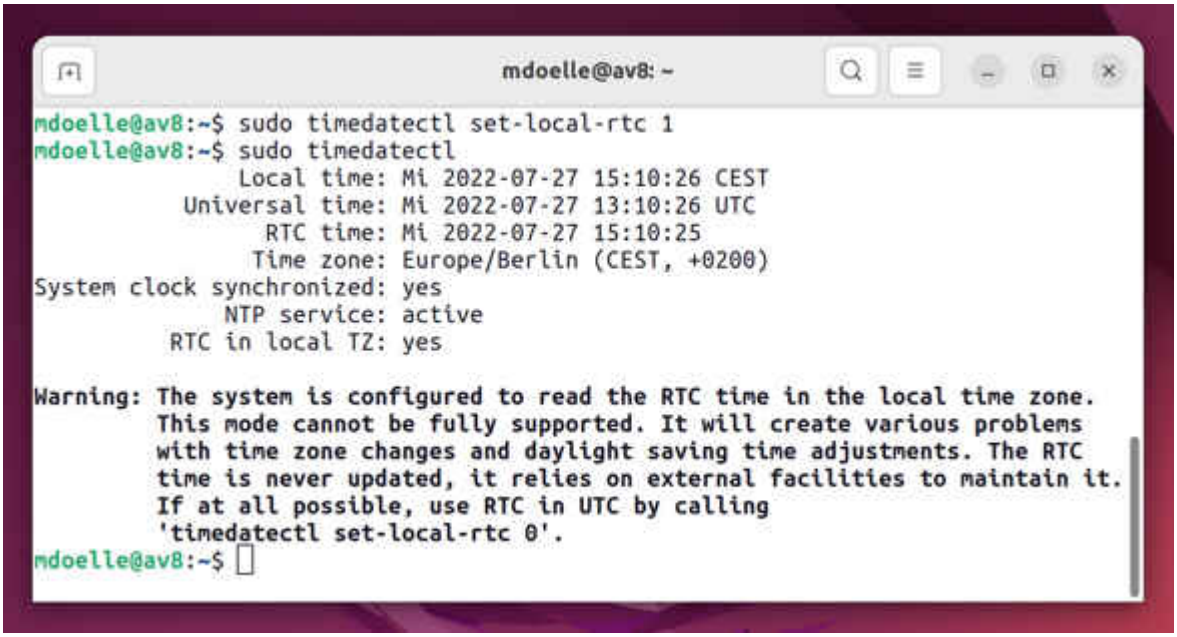
Ein ständiges Ärgernis bei Parallelinstallationen ist, dass Windows und Linux ständig die interne Uhr des Rechners verstellen: Windows speichert standardmäßig die Lokalzeit in der Hardware-Uhr, auch RTC (Real Time Clock) genannt, während Linux standardmäßig die Uhrzeit der Zeitzone UTC speichert. Letzteres lässt sich aber leicht mit dem Programm timedatectl ändern. Dazu öffnen Sie ein Terminal und geben folgenden Befehl ein:

```
sudo timedatectl set-local-rtc 1
```

Anschließend sollten Sie noch die Systemzeit, die in der Standardinstallation mit Zeitservern im Internet abgeglichen wird, in die Hardware-Uhr übertragen:

```
sudo hwclock -w
```

Ob Ihre Hardware-Uhr tatsächlich auf Lokalzeit umgestellt wurde, können Sie anschließend mit dem Befehl sudo timedatectl überprüfen. So vermeiden Sie, dass Windows und Linux ständig mit der falschen Uhrzeit starten und dies erst im laufenden Betrieb korrigieren. Die Warnung, dass es mit der Lokalzeit Probleme etwa bei der Sommer- und Winterzeitumstellung geben könnte, spielt auf Desktop-Rechnern keine Rolle: Das käme allenfalls zum Tragen, wenn Sie während der Zeitumstellung neu booten – und auch dann nur für wenige Minuten, bis die Systemzeit online abgeglichen und damit korrigiert wird.



Während Windows standardmäßig die Lokalzeit im Rechner speichert, benutzt Linux UTC. Dies lässt sich aber leicht ändern, sodass beide Betriebssysteme stets mit der richtigen Uhrzeit booten und nicht ständig an der Uhr drehen.

Fazit

Die Installer von Debian, Ubuntu und anderen Distributionen haben klar ein Defizit, Linux verschlüsselt neben Windows installieren zu können. Indem man sie an die Hand nimmt und die schwierigen Passagen Schritt für Schritt mit ihnen durchläuft, gelingt es aber trotzdem – bei Debian sogar ohne Eingriffe im Terminal, sofern Sie unserer Anleitung penibel folgen. Vielleicht animiert dieser Artikel die Entwickler ja dazu, ihre Installer um die wenigen fehlenden Pirouetten zu ergänzen, damit sich Linux künftig ohne großen Zinnober neben Windows einfügt. (*mid@ct.de*)

Das Beste beider Welten

Praxis: Gemeinsame

verschlüsselte Datenpartition optimal nutzen

Videobearbeitung unter Windows, Server-Administration unter Linux, Surfen und E-Mails überall: Mit einer gemeinsamen Datenpartition können Sie für jede Aufgabe die am besten geeignete Anwendung nutzen. Mit unserem VeraCrypt-Setup werden Ihre Daten zudem automatisch ver- und entschlüsselt, ohne dass Sie sich ein Passwort merken müssen.

Von Mirko Dölle

Obwohl Windows und Linux unterschiedliche Dateisysteme benötigen und verschiedene Verschlüsselungstechniken einsetzen, bedeutet die Parallelinstallation nicht zwangsläufig doppelte Datenhaltung. Mit VeraCrypt und NTFS gibt es einen gemeinsamen Nenner für eine verschlüsselte Datenpartition, mit der beide Betriebssysteme zurechtkommen. So vermissen Sie nie wieder Hörbücher, die Sie unter Windows heruntergeladen hatten, wenn Sie unter Linux programmieren oder Server warten.

Dieser Artikel beschreibt, wie Sie die gemeinsame Datenhalde durch angepasste Standardpfade und symbolische Links so in die Desktop-Umgebungen beider Betriebssysteme einbinden, dass Ihre Bilder, Dokumente, Downloads, Musik und Videos standardmäßig auf der gemeinsam genutzten Partition landen und diese beim Systemstart auch ohne zusätzliche Eingabe eines Passworts eingebunden wird. So verhält sich die Datenpartition transparent, Sie bekommen kaum mit, dass es sie überhaupt gibt, und können unter beiden Betriebssystemen wie gewohnt arbeiten.

Wir haben uns für VeraCrypt entschieden, weil sich das Programm unter Linux und für Windows bewährt hat. Mit der Einrichtung einer VeraCrypt-verschlüsselten Datenpartition

beginnen Sie idealerweise, nachdem Sie wie auf Seite 16 beschrieben Windows verkleinert haben: Öffnen Sie erneut die Datenträgerverwaltung von Windows, klicken Sie mit der rechten Maustaste auf den zuvor freigegebenen Speicherbereich und wählen Sie aus dem Kontextmenü „Neues einfaches Volume…“ aus. Bedenken Sie bei der Größe der künftigen Datenhalde, dass Sie ja noch Platz für die Linux-Installation benötigen – 50 GByte sollten das mindestens sein, mit vielen Anwendungen besser 100 GByte. Falls Sie viele native Linux-Anwendungen oder Spiele installieren wollen, brauchen Sie vielleicht noch mehr. Was Sie nicht für Linux benötigen, geben Sie der neuen Partition und wählen „Keinen Laufwerksbuchstaben oder -pfad zuweisen“ sowie „Dieses Volume nicht formatieren“, damit Windows die Partition in Ruhe lässt und nicht etwa zusätzlich mit BitLocker verschlüsselt.

Als Nächstes laden Sie die Windows-Version der kostenlosen Verschlüsselungssoftware VeraCrypt von veracrypt.fr herunter und installieren diese mit den Standardeinstellungen. Den Abschluss bildet ein Neustart von Windows, danach starten Sie VeraCrypt zum ersten Mal.

Fast unsichtbar

Damit VeraCrypt später nahezu unsichtbar arbeitet und die Datenpartition automatisch einbindet, verwenden Sie anstatt eines Passworts einen Schlüssel zum Entschlüsseln; der ist auf der mit BitLocker oder ebenfalls mit VeraCrypt verschlüsselten Windows-Systempartition und später auf der LUKS-verschlüsselten Linux-Partition sicher aufgehoben. Diesen Schlüssel erzeugen Sie über das Menü „Tools/Keyfile Generator“ und speichern ihn etwa unter dem Namen „winlin-key“ im persönlichen Ordner des Administrators. Anschließend kopieren Sie den Schlüssel mit dem Explorer auf einen USB-Stick, um ihn später unter Linux einlesen zu können.

Über „Tools/ Volume Creation Wizard“ verschlüsseln Sie die zuvor angelegte Datenpartition, indem Sie dort „Encrypt a non-

system partition/drive“ auswählen und ein „Standard VeraCrypt volume“ anlegen lassen. Als „Volume Location“ wählen Sie die Partition aus und klicken anschließend auf „Create encrypted volume and format it“. Wenn VeraCrypt nach dem „Volume Password“ fragt, lassen Sie das leer und aktivieren stattdessen „Use keyfiles“ und wählen unter „Keyfiles…“ die zuvor erzeugte Schlüsseldatei winlin-key aus. Bei der Frage nach „Large Files“ sollten Sie „Yes“ auswählen und bei „Volume Format“ als „Filesystem“ „NTFS“, außerdem „Quick Format“, damit VeraCrypt den Speicherbereich nicht überschreibt. Sofern sich dort zuvor Ihre mit BitLocker verschlüsselte Windows-Partition befunden hat, ist die Schnellformatierung kein Problem – dort lagerten dann keine Klartext-Daten.

Haben Sie die Partition mit VeraCrypt verschlüsselt und formatiert, wählen Sie dafür einen Laufwerksbuchstaben aus – zum Beispiel V:. Keinesfalls sollten Sie D: oder einen anderen vom Anfang des Alphabets nehmen, der zukünftig einem USB-Stick oder Kartenleser zugeordnet werden könnte, denn dann laufen später die neuen Standardpfade ins Leere. Als „Volume“ wählen Sie über „Select Device…“ die gerade vorbereitete Partition aus und klicken dann auf „Auto-Mount Devices“, damit die Partition künftig bei jedem Start von Windows wieder entschlüsselt und eingebunden wird. Wählen Sie bei der Passwortabfrage wiederum „Use keyfiles“ und unter „Key“ winlin-key als Schlüsseldatei aus.

Um die Datenpartition künftig automatisch bei jedem Systemstart einbinden zu lassen, klicken Sie mit der rechten Maustaste in der Liste der Laufwerksbuchstaben auf V: und wählen „Add to Favourites…“ aus dem Kontextmenü. Aktivieren Sie in der Liste der Optionen „Mount selected volume upon logon“ sowie „Mount selected volume when its host device gets connected“.

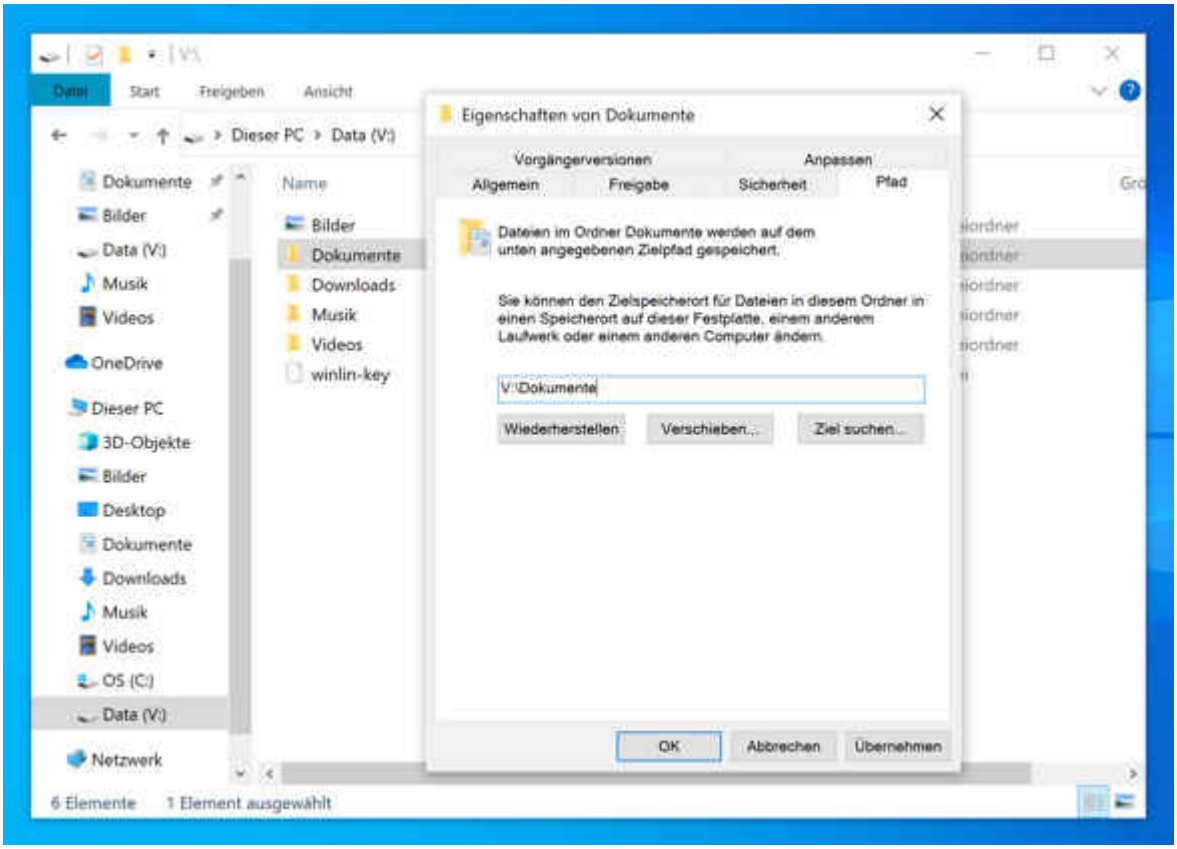
Damit VeraCrypt Sie zukünftig nicht mehr mit der Frage nach dem Passwort oder der Schlüsseldatei behelligt, importieren Sie über „Settings/Default Keyfiles…“ und dort über „Add

Files…“ den Schlüssel winlin-key als Standardschlüssel. Außerdem aktivieren Sie die Option „Try first to mount with an empty password“, ansonsten erwartet VeraCrypt später weiterhin eine manuelle Passworteingabe. Damit ist das Einrichten der verschlüsselten Datenpartition unter Windows abgeschlossen.

Auf neuen Pfaden

Wenn Sie die Windows-eigenen Ordner für Bilder, Downloads und so weiter verwenden, können Sie diese auf die VeraCrypt-Partition verlegen. Zum Ändern der Standardpfade legen Sie zunächst mit dem Explorer auf der VeraCrypt-Partition einzelne Verzeichnisse für Bilder, Dokumente, Musik, Videos und Downloads an. Den Desktop dürfen Sie dort nicht speichern, denn dieser baut sich unter Umständen schon auf, noch bevor die Partition eingebunden ist – das führt dann zu hässlichen Fehlermeldungen.

Um den Standardpfad für Bilder auf V:\Bilder zu ändern, klicken Sie im Explorer mit der rechten Maustaste im linken Navigationsbereich unterhalb von „Dieser PC“ auf „Bilder“ und wählen aus dem Kontext-Menü „Eigenschaften“. Im Register „Pfad“ klicken Sie nun auf „Verschieben“ und wählen das Verzeichnis V:\Bilder als neuen Ort aus. Sobald Sie auf „Übernehmen“ klicken, fragt Sie der Explorer, ob er die vorhandenen Daten dorthin verschieben soll – sagen Sie „Ja“. Genauso gehen Sie mit allen anderen Ordnern vor, die Sie auf die gemeinsame Datenpartition verlegen wollen. Jetzt ist Ihre gemeinsame Datenpartition voll integriert.



Indem Sie die Standardpfade auf die gemeinsam genutzte Datenpartition verschieben, sind Ihre Bilder, Dokumente, Downloads und vieles mehr auch unter Linux abrufbar.

Bei der Einrichtung unter Linux haben Sie die Wahl zwischen VeraCrypt mit GUI, womit Sie dann auch komfortabel USB-Sticks verschlüsseln können, und der reinen Kommandozeilenversion – die genügt, um die Datenpartition einzubinden, die Verwaltung von Partitionen sollten Sie besser unter Windows erledigen. VeraCrypt spielen Sie aber erst ein, nachdem Sie bereits Linux verschlüsselt neben Windows und neben der bereits eingerichteten Datenpartition installiert haben. Der Artikel auf Seite 22 beschreibt, worauf Sie bei Debian 11 und Ubuntu 22.04 LTS achten müssen. Die nachfolgende Anleitung zur Einrichtung von VeraCrypt gilt für beide Distributionen.

Linux schlüsselfertig

Laden Sie sich das zu Ihrer Distribution passende Paket, mit oder ohne GUI, aus dem Download-Bereich von veracrypt.fr herunter. Danach öffnen Sie ein Terminal, um es mit folgenden Befehlen zu installieren:

```
sudo dpkg -i Downloads/veracrypt*.deb
sudo apt -f install
```

Der zweite Befehl dient dazu, die Paketabhängigkeiten automatisch aufzulösen. Im nächsten Schritt legen Sie den Mount Point für die Datenpartition an, außerdem ein Verzeichnis für Schlüssel und kopieren dann den VeraCrypt-Schlüssel winlin-key vom USB-Stick in das neue Verzeichnis:

```
sudo mkdir /data
sudo mkdir -m 700 /etc/crypto
sudo cp /media/*/*/winlin-key \
  /etc/crypto
```

Automagie

Damit ist VeraCrypt betriebsbereit und Sie können sich darum kümmern, dass die Datenpartition künftig beim Systemstart automatisch entschlüsselt und eingebunden wird. Dazu ergänzen Sie folgende Zeile am Ende der Datei /etc/crypttab:

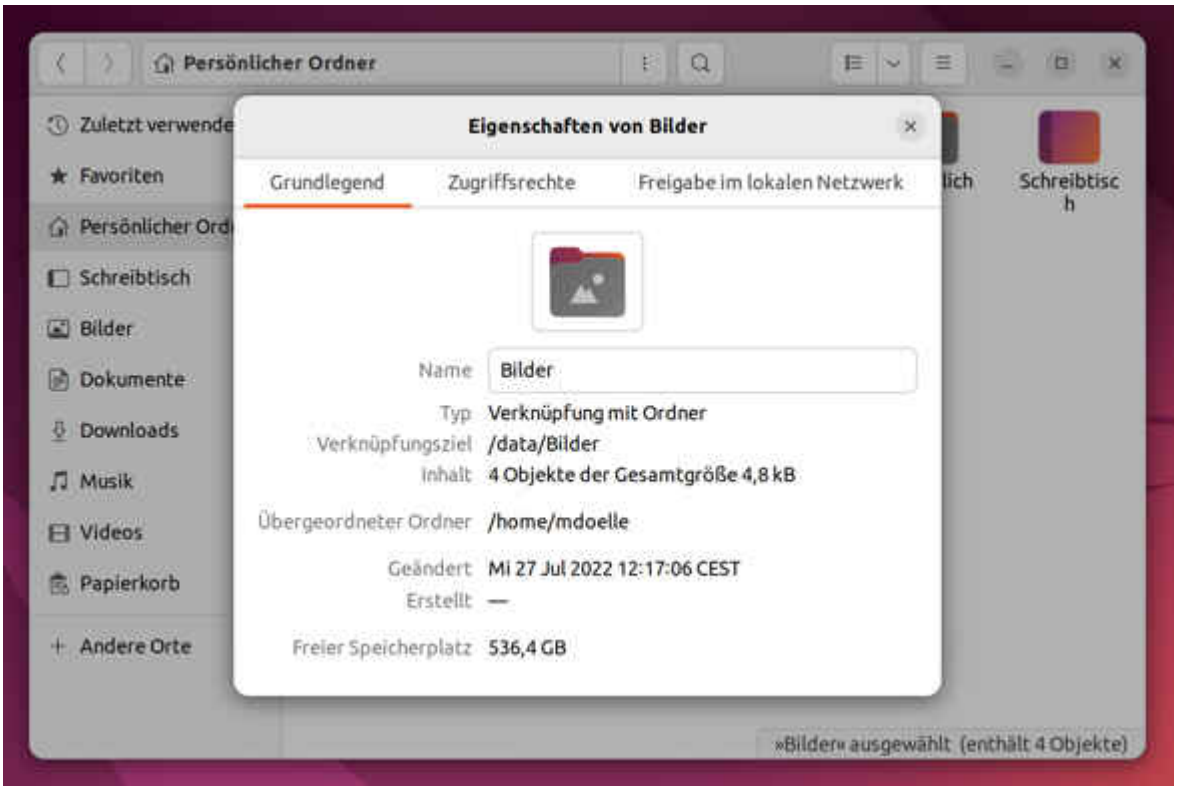
```
winlin-data  /dev/sda3  /dev/nulltcrypt-veracrypt,tcrypt-keyfile=/etc/crypto/winlin-key
```

Den Gerätenamen /dev/sda3 ersetzen Sie durch den Gerätenamen Ihrer Datenpartition, den Sie mit dem Befehl lsblk herausfinden. Damit wird die Datenpartition entsperrt und bekommt den Namen „winlin-data“. Die folgende Zeile am Ende der Datei /etc/fstab bindet die Datenpartition schließlich unterhalb von /data ein:

```
/dev/mapper/winlin-data          /data          auto uid=1000,gid=1000,nodev,nofail 0 0
```

Nach dem nächsten Neustart ist die Datenpartition für den ersten Benutzer im System mit der User-ID 1000 beschreibbar unter /data eingebunden. Verschieben Sie nun den Inhalt des Verzeichnisses „Bilder“ in Ihrem „Persönlichen Ordner“ (Home-Verzeichnis) nach /data/Bilder, etwa per Drag & Drop mit zwei Fenstern des Dateimanagers Nautilus.

Anschließend löschen Sie das nun leere Verzeichnis Bilder. Um einen symbolischen Link zum Bilderverzeichnis auf der gemeinsamen Datenhalde anzulegen, ziehen Sie das Verzeichnis /data/Bilder aus dem anderen Nautilus-Fenster per Drag & Drop in Ihren „Persönlichen Ordner“ und halten dabei die Alt-Taste gedrückt. Beim Loslassen wählen Sie dann aus dem Kontextmenü „Verknüpfung erstellen“. Damit verweist der Ordner Bilder in Ihrem Home-Verzeichnis auf das Verzeichnis /data/Bilder, wo auch Ihre Bilder aus Windows gespeichert sind. Diesen Vorgang wiederholen Sie für Dokumente, Musik, Videos und alle anderen Verzeichnisse, deren Daten Sie künftig auf der gemeinsamen Datenpartition speichern wollen.



Durch symbolische Links für Bilder, Dokumente und andere Verzeichnisse verweisen Sie alle Linux-Anwendungen auf die gemeinsam genutzte Datenpartition als Speicherort, sodass Sie sie auch unter Windows öffnen können.

Welche Anwendung wofür?

Zwei verschlüsselte Betriebssysteme mit gemeinsamer Datenpartition sind eine tolle Arbeitsgrundlage – doch womit arbeitet man konkret? Das hängt davon ab, was Sie individuell

benötigen oder wo Ihre Vorlieben liegen. Falls Sie regelmäßig mit Kollegen an MS-Office-Dokumenten oder Präsentationen arbeiten, werden Sie nicht an Microsoft Office unter Windows vorbeikommen. Unter Linux genügt Ihnen LibreOffice oder OpenOffice, mit denen Sie bei Bedarf einen flüchtigen Blick in ein Office-Dokument werfen können.

Spielt Kompatibilität keine große Rolle, können Sie sich das Geld für Microsoft Office sparen und auch unter Windows zur Open-Source-Variante Ihres Linux-Office-Pakets greifen. Dann haben Sie den Vorteil, dass es keine Konvertierungsprobleme mit Ihren eigenen Office-Dateien gibt und die Bedienung weitgehend einheitlich ist.

Es muss aber nicht immer das gleiche Programm sein: Falls Sie allenfalls mal den Anfang und das Ende eines Screen-Recordings wegschneiden, genügen dazu die jeweiligen Bordmittel von Windows und Linux. Erst wenn Ihre Projekte etwas ambitionierter werden, lohnt es sich, wenn Sie sich in das wesentlich leistungsfähige Kdenlive einarbeiten, das es für beide Betriebssysteme kostenlos gibt. Videoproducer hingegen werden kaum an Adobe Premiere für Windows vorbeikommen, benötigen dann aber unter Linux keinen speziellen Videoeditor.

Ähnlich ist es bei der Foto- und Bildbearbeitung: Wer das beruflich macht oder große Ambitionen hat, wird früher oder später Photoshop und die Adobe Creative Suite benutzen müssen. Dann hat es aber wenig Sinn, sich zusätzlich in Gimp einzuarbeiten – unter Linux genügt dann die Vorschau, um sich Bilder anzusehen. Benötigen Sie hingegen nicht den Leistungsumfang eines Adobe Photoshop, kann Gimp eine Alternative für Windows und Linux sein. Auch dann profitieren Sie von der einheitlichen Bedienung.

Als Browser empfehlen wir Ihnen Firefox: Haben Sie einen kostenlosen Account angelegt, können Sie per Firefox Sync von den Lesezeichen bis hin zu den gerade geöffneten Tabs und Websites alles zwischen Windows und Linux synchronisieren, was

Sie für den Alltag brauchen. Je mehr Sie synchronisieren (und damit verschlüsselt in die Cloud übertragen) lassen, desto leichter fällt es Ihnen später, ad hoc von Windows nach Linux zu wechseln und umgekehrt – denn Sie können nahtlos da weiter surfen, wo Sie auf dem anderen Betriebssystem gerade waren.

Sofern Sie Ihre E-Mails per IMAP bei Ihrem Provider abholen, können Sie genauso gut Thunderbird unter Windows und Linux einsetzen wie zwei verschiedene Programme: Wenn beide Programme die Entwürfe in dem dafür vorgesehenen IMAP-Ordner zwischenspeichern, können Sie sogar E-Mails unter Linux fertig schreiben, die Sie unter Windows begonnen haben – und umgekehrt.

Auch bei manchen Spielen haben Sie die Wahl, die Wikinger-Variante von Minecraft, Valheim, zum Beispiel gibt es im Steam Store sowohl für Windows als auch für Linux. Sie können sich für eine der beiden Varianten entscheiden, oder aber die Spielstände über die Steam Cloud zwischen Windows und Linux synchronisieren lassen. Diese Lösung ist auch besser, als aufwendig die Speicherpfade der Spielstände unter Windows und Linux so zu verändern, dass sie auf der gemeinsamen Datenpartition landen: Nicht alle Windows-Spiele kommen mit den Dateien der anderen Plattformen zurecht, die Cloud-Synchronisation von Steam hingegen ist eigens darauf ausgelegt.

Fazit

Man muss sich nicht zwischen Windows und Linux entscheiden. Beide Betriebssysteme haben ihre Berechtigung und sind letztlich nur die Basis, auf der man seine eigentliche Arbeit erledigt – mit dem am besten dafür geeigneten Werkzeug. Die gemeinsame verschlüsselte Datenpartition und Funktionen wie Firefox Sync machen es Ihnen leicht, für eine bestimmte Aufgabe das jeweils andere Betriebssystem zu booten und dabei an der gleichen Stelle weiterzuarbeiten, an der Sie aufgehört haben. *(mid@ct.de)*

Python im Web

Python im Web

Dynamisches HTML im Browser mit PyScript statt JavaScript

Browser führen nur JavaScript aus? Nicht mehr! PyScript tritt als Alternative zu JavaScript auf. Wir erklären, wie das möglich ist, und programmieren als Beispiel ein Spiel mit der neuen Technik.

Von Pina Merkert

kompakt

- PyScript nutzt die maschinennahe Sprache WebAssembly, um Python mit der JavaScript-Engine eines Browsers auszuführen.
- Über PyScript-Funktionen kann der Python-Code auf das DOM zugreifen, was dynamisches HTML ermöglicht.
- PyScript kann JavaScript ersetzen, es lädt aber wesentlich langsamer.

Beim Versuch, auf eine Objekteigenschaft zuzugreifen, wird die Eigenschaft nicht nur in dem Objekt selbst, sondern auch in seinem Prototyp und dem Prototyp des Prototyps gesucht. Wenn Ihnen Sätze wie dieser auch rätselhaft vorkommen, ist JavaScript wohl auch nicht Ihre Muttersprache. Python ist da oft zugänglicher, der Code hat weniger Zeilen und das Sprachdesign ist auf Lesbarkeit optimiert. Nur leider muss

Python immer lokal installiert sein, die allgegenwärtigen Webbrowser verarbeiten nur JavaScript. Oder etwa nicht?

Dass Python nicht im Browser läuft, stimmt nicht mehr: Mit einer trickreichen Software namens „Pyodide“ interpretieren Webseiten auch Python-Code. Python-Entwickler können auf diesem Weg JavaScript durch Python ersetzen. Sie programmieren dann in Python mit PyScript-Funktionen statt in JavaScript. Wir zeigen, wie Sie mit PyScript loslegen.

Als Beispiel haben wir uns von dem Worträtsel „Wordle“ inspirieren lassen und ein Rätsel für Nerds mit dem Namen „Nerdle“ programmiert. Die Spielregeln sind einfach: PyScript wählt aus einer langen Liste mit Begriffen aus der Technikwelt mit fünf Zeichen (Nerdle ist schwieriger als Wordle, weil unser Rätsel Wörter mit Ziffern und Sonderzeichen enthält) einen zufälligen aus, den Sie erraten müssen. Dafür tippen Sie über die Bildschirmtastatur zunächst einen Begriff. Jeder geratene Begriff muss in der Liste stehen, damit das Spiel die Eingabe akzeptiert. Wenn ein Zeichen des geratenen Begriffs an der gleichen Stelle steht wie im gesuchten Begriff, wird es grün. Kommt ein Zeichen irgendwo im gesuchten Begriff vor, wird es gelb. Zeichen, die gar nicht vorkommen, werden grau. Die Tasten der Bildschirmtastatur verfärben sich genauso. Diese Farben geben Hinweise für den nächsten Begriff, sodass Sie mit zusätzlichen Versuchen immer mehr über den gesuchten Begriff erfahren. Wenn Sie spätestens beim sechsten Versuch richtig raten, gewinnen Sie das Spiel. Wenn Sie zu oft falsch raten, sollten Sie mehr c’t lesen *zwinkersmiley*. Ohne selbst zu programmieren, können Sie das Spiel sofort unter nerdle.pinae.net ausprobieren; den Code finden Sie als Open Source (GPLv3) über ct.de/ynk9.

WebAssembly

Browser integrieren weiterhin keinen Python-Interpreter. Sie führen aber in ihrer virtuellen Maschine schon länger WebAssembly aus. WebAssembly ist eine maschinennahe Sprache, die der Browser innerhalb von Millisekunden in Maschinencode übersetzt. Das funktioniert so gut, dass WebAssembly meist nur wenige Prozent langsamer läuft als gleicher Code, den ein Compiler direkt in Maschinencode übersetzt hat. Da der Code aber in der Browser-Sandbox läuft, ist nicht jedes Programm WebAssembly-tauglich. Beispielsweise verbieten Browser direkten Zugriff aufs Dateisystem oder Hardware wie Netzwerkkarten.

Das Pyodide-Projekt hat die Python-Referenzimplementierung CPython so modifiziert, dass sie nach WebAssembly kompiliert. Damit läuft Python zwar im Browser, man sieht davon aber noch nichts. An dieser Stelle kommt PyScript ins Spiel: PyScript bringt Funktionen mit, um vom Browser-Python auf den DOM-Tree zuzugreifen, also auf die HTML-Struktur der Webseite. Außerdem stellt es eigene HTML-Tags bereit, die den Code aufnehmen, Module nachladen und Eingabefelder bereitstellen. Das Projekt steht noch am Anfang: Release-Nummern sind im Datumsformat, die Versionen auf GitHub als „Pre-release“ getaggt. Manchen Funktionen sieht man den frühen Entwicklungsstand noch an. Beispielsweise muss man per Hand Funktionen einkapseln, um sie ins Ereignissystem von JavaScript einzuklinken. Trotzdem funktioniert der Code bereits gut genug für ein Browserspiel.

Einbinden

PyScript bindet man wie ein JavaScript-Framework ein, indem man zwei Tags im <head> der Webseite ergänzt:

```
<link rel="stylesheet"
    href="https://pyscript.net/alpha/pyscript.css" />
<script                                          defer
src="https://pyscript.net/alpha/pyscript.js"></script>
```

Den Code lädt der Browser dann aus dem Content Delivery Network (CDN) der PyScript-Entwickler, man bekommt also immer die aktuellste Version. Um Probleme bei Updates zu umgehen, könnte man PyScript auch selbst übersetzen und hosten. Momentan raten wir aber noch davon ab, PyScript produktiv einzusetzen, weil sich in den kommenden Monaten sicherlich noch einiges an den Funktionssignaturen ändern kann.

Danach kann man einfach irgendwo im HTML der Seite den <py-script>-Tag einfügen und in dem Python-Code platzieren. Für ein Hallo-Welt-Programm braucht man nur drei Zeilen:

```
<py-script>
  print("Hallo Welt.")
</py-script>
```

Module

Python funktioniert im Browser wie gewohnt. Das bezieht sich auch auf Module, die man wie üblich mit import ins Programm einbindet:

```
import random
wordlist = ["CT.DE", "RULEZ"]
word = random.choice(wordlist)
```

Da dem Browser der Python-Paketmanager pip fehlt, packt man externe Module mit Spiegelstrichen in den <py-env>-Tag und PyScript kümmert sich ums Nachladen:

```
<py-env>
  - numpy
  - matplotlib
</py-env>
```

Es stehen schon einige beliebte Module wie numpy und matplotlib zur Verfügung, solche mit Hardwarezugriff wie requests können aber nicht funktionieren. Gibt man ein Modul im <py-env>-Tag an, muss man es trotzdem im Code mit einem import einbinden.

Wortlisten per Ajax asynchron laden

Damit wir die Begriffe zentral verwalten können, wollten wir sie nicht als ellenlange Liste hardcoden, sondern lieber mit Ajax nachladen. In normalem Python-Code würde man für so etwas eine Bibliothek wie requests nehmen. Die läuft aber im Browser nicht. Der kann jedoch von sich aus Daten laden, was die Funktion pyfetch() aus dem pyodide-Modul anstößt.

Ajax-Anfragen sind von Natur aus asynchron, weshalb pyfetch() nur in asynchronen Funktionen funktioniert. Die erzeugt man mit async def statt def. Da sie dem normalen Code nicht im Weg stehen, kann man in so einer Funktion problemlos mit await auf Antworten warten, ohne das ganze Programm auszubremsen:

```
from pyodide.http import pyfetch
from pyodide import JsException
from js import console

async def load_wordlist():
  try:
    response = await pyfetch(
url="https://raw.githubusercontent.com/pinae/Nerdle/main/nerdl
e-begriffe.txt",
      method="GET",
      headers={"Content-Type":
               "text/plain"})
    if response.ok:
      data = await response.string()
      console.log(data.split())
      return data.split()
  except JsException:
    return None
```

Die JsException ist die Basisklasse aller JavaScript-Fehler, die PyScript automatisch kapselt. Man könnte hier auch spezifische Exceptions fangen, um aussagekräftige Fehlermeldungen anzuzeigen.

Das Speichern der Liste und das Auswählen des zufälligen Worts übernimmt die Funktion pick_word(). Auch sie ist asynchron,

weil sie mit await auf die Rückgabe von load_wordlist() warten muss:

```
async def pick_word():
  global wordlist, word, accept_input
  wordlist = await load_wordlist()
  word = random.choice(wordlist)
  console.log("Wort: ",
              " ".join(list(word)))
  accept_input = True
```

Um die asynchronen Funktionen so aufzurufen, dass sie den Code nicht blockieren, kann man einen alten JavaScript-Trick benutzen:

```
setTimeout(create_proxy(pick_word), 0)
```

Der Timeout von 0 zwingt den Code nicht zum Warten, bei 0 Millisekunden Verzögerung gibt es aber auch keine Wartezeit. Die Timeout-Funktion sorgt dabei automatisch für eine nebenläufige Ausführung.

Nerdle-HTML

Nerdle benutzt ein Spielbrett aus 30 Quadraten (6 Zeilen mit je 5), die je ein Zeichen aufnehmen. Das geht hervorragend mit einem Grid-Layout. Und da alle Felder gleich aussehen, kann man sie bequem im Quellcode erzeugen. Der fügt alle hintereinander in ein und merkt sich die Divs in einer Liste aus Listen (eine pro Zeile):

```
tiles=[]
board=document.getElementById("board")
for row in range(6):
  tiles.append([])
  for col in range(5):
    tile=document.createElement("div")
    board.appendChild(tile)
    tiles[-1].append(tile)
```

Form und Farbe legt die Datei nerdle-styles.css fest, die Sie

zusammen mit dem Rest des Codes im Repository über ct.de/ynk9 finden.

Die Funktionen getElementById() und createElement() funktionieren genau wie in JavaScript, sodass Sie dort die Dokumentation konsultieren können, solange PyScript noch keine eigene dafür hat. Die Funktionen gehören zum document-Objekt, das Sie mit from js import document laden.

Die Tasten der Bildschirmtastatur sind ganz ähnliche , allerdings von Anfang an im HTML. Es gibt einen Unterschied: Das umrahmende hat die ID "keyboard". Der Python-Code kann sich anhand der Beschriftung der Tasten dann selbst ein Dictionary zusammenbauen, das jedem Zeichen das passende DOM-Objekt zuordnet:

```
key_objects = {}
for row in document.getElementById(
                "keyboard").childNodes:
  for key in row.childNodes:
    key.addEventListener("click",
                         js_key_clicked)
    if len(key.textContent) == 1:
      key_objects[
                 key.textContent] = key
```

childNodes ist dabei die JavaScript-Datenstruktur NodeList, die aber das Iterator-Interface implementiert, sodass sich damit fast wie mit einer Python-Liste arbeiten lässt. addEventListener() ist die von Python aufrufbare JavaScript-Funktion, die den JavaScript-Function-Pointer js_key_clicked annimmt. Den muss man allerdings etwas umständlich erzeugen.

Verpackte Funktionen

Funktionen definiert man im Python-Code wie üblich mit def. Heraus kommt dabei eine Python-Funktion, die im Python-Code ganz normal funktioniert. Will man aber mit dem DOM interagieren, muss man die von PyScript gekapselten

JavaScript-Funktionen benutzen, die man an den Namen in CamelCase erkennt. Diese JavaScript-Funktionen sehen die Python-Funktionen nicht, weshalb man eine Funktionsreferenz beispielsweise nicht einfach an addEventListener() übergeben kann.

Die Sprachbarriere überwindet das pyodide-Modul, das PyScript standardmäßig mitbringt (kein Eintrag in <py-env> nötig).

```
from pyodide import create_proxy
def key_clicked(e):
  print(e.target.textContent)

js_key_clicked = create_proxy(
                           key_clicked)
```

Mit create_proxy() packt man die Python-Funktion so ein, dass JavaScript sie sehen kann. Die so erzeugte Referenz kann man wie eine JavaScript-Funktion an addEventListener() übergeben.

Dabei funktionieren wiederum alle von JavaScript bekannten Datenstrukturen, sodass die Python-Funktion über den Parameter e das Event-Objekt bekommt. Das verweist unter e.target auf das DOM-Objekt, von dem das Ereignis ausging, und das verrät mit e.target.textContent, was innerhalb des HTML-Tags steht.

Noch ein Hinweis auf eine mögliche Fehlerquelle beim Konvertieren von JavaScript-Code von StackOverflow: Die Python-Funktion muss alle Parameter nennen, die JavaScript übergibt. JavaScript erlaubt es, Parameter still und heimlich wegzulassen, während Python mindestens einen _ verlangt. Man muss die übergebenen Parameter in der Funktion aber nicht benutzen, wenn man sie nicht braucht.

Raten

Nachdem der Code schon ein Wort zum Erraten ausgewählt und das Dictionary mit den Tasten initialisiert ist, muss er nur noch die Eingaben verarbeiten und bei „Enter“ den geratenen Begriff

auswerten.

Die aktuelle Eingabe speichert das Programm in der Variable guess. Fürs Verarbeiten der Eingaben macht sich die Funktion key_clicked() den Umstand zunutze, dass alle mit einem Zeichen einen textContent mit Länge 1 haben. Das Backspace-Symbol ist ein SVG, weshalb textContent bei dieser Taste ein leerer String ist. Die Enter-Taste dagegen ist mit „Enter“ beschriftet, also mit fünf Zeichen. Die Fallunterscheidung ist eine gute Gelegenheit, das mit Python 3.10 eingeführte Pattern-Matching einzusetzen:

```
match len(e.target.textContent):
  case 0:
    guess = guess[:-1]
  case 1:
    guess += e.target.textContent
  case _:
    check_enter()
display_guess()
```

match…case funktioniert so ähnlich wie switch…case in C, erlaubt aber beispielsweise auch reguläre Ausdrücke hinter case. Statt default: gibt es case _:, der zum Tragen kommt, wenn keiner der anderen Fälle eintrifft. In allen Fällen kümmert sie die Funktion display_guess() darum, den Inhalt von guess auch anzuzeigen. Pattern Matching funktioniert auch mit Objekten, beispielsweise mit re (das Modul für reguläre Ausdrücke) erzeugte Tupel. Ein Beispiel dafür finden Sie im Code auf GitHub.

Die Funktion display_guess() konsultiert die Variable guess_no, die speichert, in welcher Zeile Spieler gerade raten. Zuerst füllt die Funktion überall Leerzeichen ein, um vorherige Eingaben zu löschen:

```
for i in range(5):
  tiles[guess_no][i].textContent = ""
```

Das Eintragen aller Buchstaben aus guess geht fast genauso

einfach, weil Python klaglos mit list() Strings in Listen aus Einzelzeichen verwandelt:

```
for pos, c in enumerate(list(guess)):
  tiles[guess_no][pos].textContent = c
```

Python kann Tupel automatisch auspacken, wenn man der Anzahl entsprechend viele Variablen mit Komma getrennt hintereinander schreibt. enumerate() gibt für jeden Iterator, also für alles, was sich wie eine Liste behandeln lässt, ein 2-Tupel aus der Nummer und dem Element zurück. Im Beispiel landet in pos also die Nummer des Zeichens und in char das Zeichen. Die Schreibweise, die dabei herauskommt, versteht man ganz intuitiv.

Vergleichen

Bei einem „Enter“ muss das Spiel zunächst prüfen, ob der geratene Begriff fünf Zeichen hat und ob er in der Wortliste steht. Wenn nicht, schreibt die Funktion in das mit der ID "info" eine Fehlermeldung:

```
pyscript.write("info", f"„{guess}“ " +
      "steht nicht in der Wortliste.")
```

Die Funktion pyscript.write() nimmt einem dabei die Arbeit ab, das DOM-Element mit der ID "info" herauszusuchen und seinen textContent zu ändern. Wir vermuten, dass PyScript in Zukunft noch weitere Funktionen ähnlicher Art bekommt, die DOM-Zugriffe mit weniger Code erlauben.

Außerdem nutzt die Zeile Pythons seit 3.6 verfügbare f-Strings. Die definiert man mit dem Buchstaben f vor den Anführungszeichen und Python ersetzt dann alle in geschweiften Klammern angegebenen Variablen durch deren Werte. Man kann die Ausgabe mit den gleichen Filtern wie in format() beeinflussen.

Steht in guess ein Begriff aus der Wortliste, vergleicht die Funktion evaluate_guess() den geratenen Begriff mit word, dem zu erratenden Begriff. Dafür macht sie den Begriff wieder zu

einer Liste, holt sich mit enumerate() die Zeichennummer dazu, die sie dann benutzt, um das Zeichen aus dem zu erratenden Begriff zu ziehen und die Zeichen zu vergleichen:

```
for p, char in enumerate(list(guess)):
  if char == word[p]:
    tiles[guess_no][p].classList.add(
                           "nailedit")
    key_objects[char].classList.add(
                           "nailedit")
    correct_counter += 1
```

Damit Spieler Grün und Gelb sehen, ergänzt die Funktion über classList.add() die passende CSS-Klasse, die die Farbe festlegt. Das passiert sowohl bei den Quadraten im Spielfeld als auch bei der Bildschirmtastatur. Dass die Tasten ihre Farbe verändern, ist eine willkommene Hilfe beim Sinnieren über den nächsten Begriff, den man raten könnte.

Bei richtig geratenen Zeichen zählt die Funktion auch die lokale Variable correct_counter hoch. Steigt die nämlich beim Einfärben aller Zeichen-Quadrate auf 5, ist das Ratespiel gewonnen. Ist die Variable kleiner und zusätzlich guess_no >= 5, ist das Spiel verloren.

Usability

Der vollständige Code, den Sie über das Repository über ct.de/ynk9 finden, enthält noch einige zusätzliche Zeilen. Die dienen der besseren Bedienbarkeit, damit man beispielsweise statt per Bildschirmtastatur auch mit der normalen Tastatur tippen kann. Das geht mit einer key_down()-Funktion, die den onkeydown-Event-Handler von document überschreibt:

```
js_key_down = create_proxy(key_down)
document.onkeydown = js_key_down
```

Der Code ist mitsamt HTML kaum mehr als 200 Zeilen lang, die bis auf einen regulären Ausdruck leicht zu lesen sind.

Exceptions sind in der Entwicklerkonsole sichtbar, die Browser mit F12 öffnen. Die Darstellung ist leider nicht so übersichtlich, weil PyScript alles in JavaScript-Objekte einpacken muss.
Fürs Debugging lohnt es sich, mit F12 die Entwickler-Konsole zu öffnen. Dort landet auch alles, was Sie mit console.log() ausgeben. Die Fehlermeldungen sind leider nicht gut lesbar, weil es in JavaScript-Exceptions verpackte Python-Exceptions sind. Das müssen die Entwickler noch stark nachbessern.

Eine weitere Baustelle sind die Entwicklungsumgebungen. Beispielsweise erkannte die Entwicklungsumgebung PyCharm den Code in <py-script>-Tags nicht als Python-Quelltext, sodass

weder Farben noch Code-Vervollständigung funktionierten.

Spielen

Das selbst programmierte Nerdle starten Sie, indem Sie einfach die Datei index.html im Browser öffnen. Ein Webserver ist dafür nicht notwendig, zum Nachladen des PyScript-Codes und der Wortliste aber eine Internetverbindung. Installieren müssen Sie gar nichts. Falls Sie das Spiel doch mit einem Webserver hosten wollen, muss der nur eine statische Seite ausliefern können.

Unser Worträtsel „Nerdle“ ist wegen der Tech-Begriffe mit Abkürzungen deutlich schwerer als „Wordle“ von der New York Times.
Unsere Liste mit Begriffen finden Sie im Repository in der Datei nerdle-begriffe.txt. Momentan stehen da schon mehr als 1500 Begriffe zum Raten bereit. Mit dem Skript word_list_filter.py können Sie die Liste aber bequem erweitern. Es liest die Datei neue-begriffe.txt, filtert nach den richtigen Zeichen und fragt für alle neuen Begriffe einzeln, ob Sie die hinzufügen wollen. So können Sie mit wenig Arbeit ganze Listen aus Kreuzworträtsel-Datenbanken ergänzen.

Kritik

Wir sind von PyScript begeistert. Python-Code ohne Installation im Browser ausprobieren? Grandios!

Noch ist PyScript aber nicht an dem Punkt angelangt, darauf bestehenden Code zu portieren und über Experimente hinausgehende Projekte damit umsetzen zu wollen. Außerdem muss eine Webseite mit PyScript mehr als 14 Megabyte an Code laden, bevor sie überhaupt starten kann. Danach muss die JavaScript-Engine den WebAssembly-Code zunächst in Bytecode für die Prozessorarchitektur übersetzen, was selbst auf einer schnellen Desktop-CPU fast eine Sekunde dauert. Erst danach läuft der Code der Seite los. Bei normalem JavaScript lädt der Browser nur die winzige Skriptdatei und führt diese sofort aus, weil die JavaScript-Engine längst warm gelaufen ist.

PyScript hat trotz allem sinnvolle Anwendungen: Hat beispielsweise eine Statistikerin ihre Daten schon mit Python ausgewertet und mit Matplotlib ein Diagramm gezeichnet, müsste sie normalerweise alles in JavaScript nachprogrammieren, um das Diagramm in eine Webseite einzubinden. PyScript senkt die Hürde für Pythonisten, mal eben schnell aus einer Idee eine Webanwendung zu basteln – wie unser Beispiel zeigt. *(pmk@ct.de)*

Code bei GitHub, PyScript-Dokumentation: ct.de/ynk9

QR-Codes

Bithaufen

QR-Codes verstehen und ohne technische Hilfsmittel dekodieren

QR-Codes enthalten zusätzlich zu den Nutzdaten Informationen, aus denen man fehlende Pixel wiederherstellen kann. Wenn der Code mal so stark beschädigt sein sollte, dass selbst eine App ihn nicht mehr erkennt, dann können Sie versuchen, ihn manuell zu entschlüsseln. Wir zeigen Ihnen, wie das geht.

Von Wilhelm Drehling

kompakt

- QR-Codes folgen einem strikten Aufbau, in dem Informationen bestimmten Arealen zugeteilt werden.
- Die Nachricht sowie viele andere Details kommen mehrfach und teilweise auch maskiert im Code vor.
- Mit dem in diesem Artikel erlangten Wissen können Sie einen beschädigten QR-Code per Hand dekodieren.

Smartphone raus, entsperren und die Kamera-App über einen QR-Code halten. Im Bruchteil einer Sekunde wandelt sich der verwitterte Sticker am Laternenmast in einen Strom von Bits

um, welchen das Smartphone in eine lesbare Zeichenkette dekodiert. Bereit zum Antippen ploppt die gescannte Information auf dem Bildschirm auf.

QR-Codes sind ein häufig benutztes Mittel für Außenwerbung, weil sie eine Menge Schaden aushalten. Wenn aber mal der Code am Laternenmast mehr als 30 Prozent beschädigt ist und technische Hilfsmittel nicht weiterhelfen, dann können Sie versuchen, den QR-Code per Hand zu dekodieren. Kleine Codes mit 20 Zeichen sind problemlos in ein paar Minuten geschafft, bei den wirklich großen sollten Sie es sich zweimal überlegen, ob es sich lohnt. Denn diese können bis zu 2953 herkömmliche Zeichen speichern. In der Theorie lassen sich damit sogar die sämtlichen Web-Tipps von Seite 56 in einen QR-Code packen.

Das ist übrigens nicht das erste Mal, dass wir uns QR-Codes genauer anschauen: Wir haben uns vor einiger Zeit schon mal näher mit den quadratischen Codes beschäftigt und Seiten empfohlen, die zuverlässig für Sie QR-Codes erstellen [1]. Dieser Artikel fokussiert sich dagegen auf den Aufbau von QR-Codes. Dazu zerlegen wir den Code wortwörtlich in seine Bestandteile: in seine Felder und Masken. Schritt-für-Schritt zeigen wir die kleinen Finessen, die sich die Erfinder ausgedacht haben. Mit dem dadurch erlangten Wissen können Sie QR-Codes per Hand dechiffrieren. Das ist zwar nicht sonderlich hilfreich im Alltag, macht aber Spaß und ist ganz nebenbei noch lehrreich!

Geschichtsstunde

Als Kopf hinter den QR-Codes gilt der Ingenieur Masahiro Hara, der für die japanische Firma Denso Wave arbeitete. Denso erhielt 1992 den Auftrag, die Lesbarkeit von Barcodes zu verbessern.

Das Unternehmen hat die Leitung Masahiro Hara übertragen, der

sich des Problems prompt annahm und schnell feststellte: Selbst wenn er den Barcodescanner verbessert, die fehlende Unterstützung der Barcodes für das japanische Schriftsystem Kanji und die kleine Speicherkapazität löst das grundlegende Problem der Ineffizienz nicht.

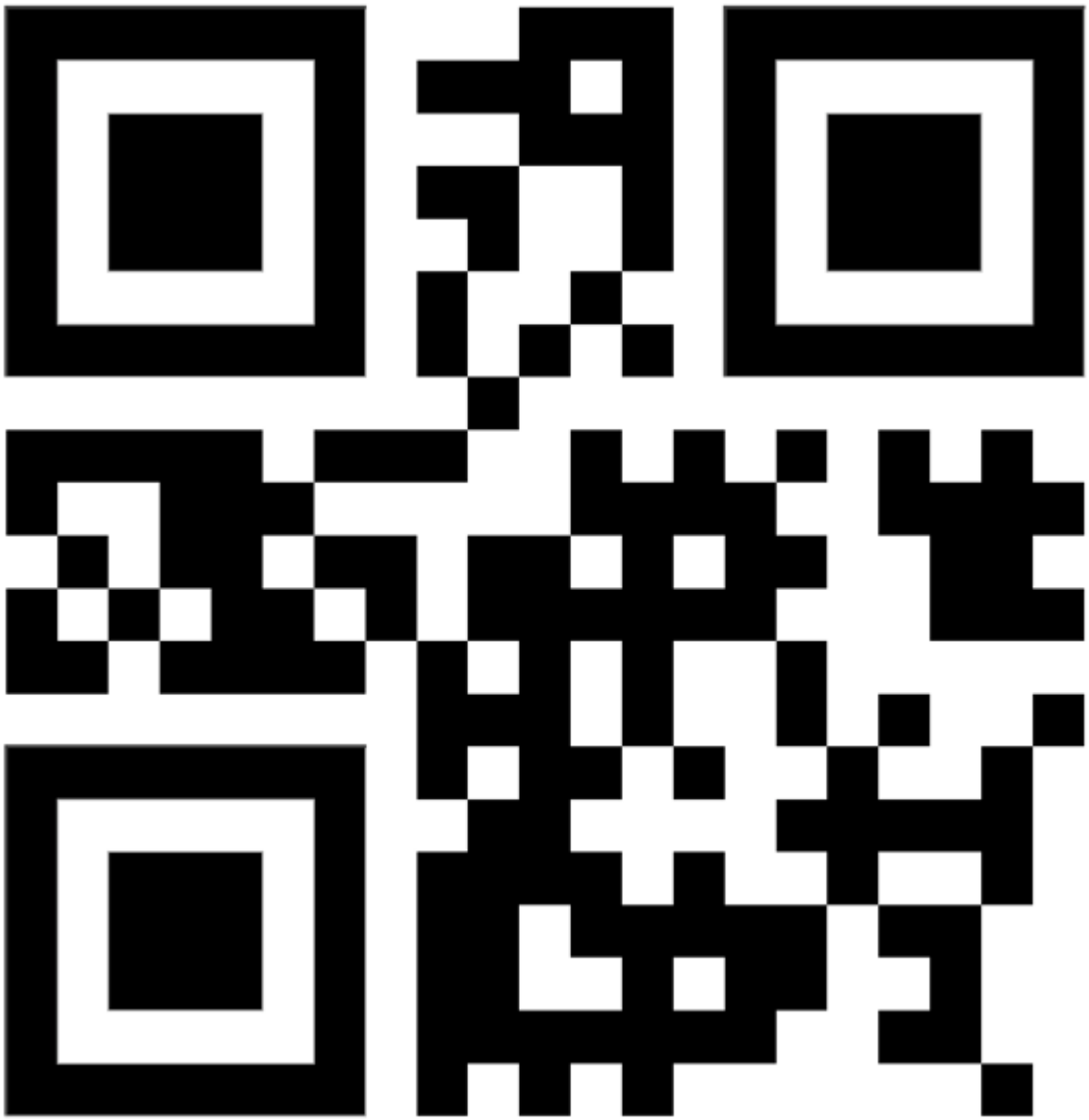
Mit seinem Team entwickelte er in zwei Jahren einen zweidimensionalen Code, mit mehr Kapazität und schnellerer Lesbarkeit: der Quick-Response-Code, kurz QR-Code. Unter ct.de/yvy2 haben wir Ihnen die ausführliche Herkunftsgeschichte verlinkt. Dort geht der Erfinder unter anderem auf die genauen Gründe und Schwierigkeiten ein, die das Team im Laufe der Entwicklung überwinden musste.

Massig

Die Idee von zweidimensionalen Codes ist nicht neu, schon vor dem QR-Code spukten unterschiedliche Entwürfe herum. Zum Beispiel stapelte „Code 16k“ Barcodes aufeinander, um mehr Zeichen abspeichern zu können. Der QR-Code und sein ehemaliger Kontrahent gehören zu den sogenannten Matrix-Codes. Das ist eine Gruppe von Codes, die Informationen zweidimensional abspeichern, im Unterschied zu eindimensionalen Liniencodes wie Barcodes. Der QR-Code ordnet dabei jede Fläche einem Bit zu, Schwarz einer 1 und Weiß einer 0. Der starke Kontrast erlaubt es, auf kleinerem Raum größere Datenmengen abzuspeichern.

Wie viel in einen QR-Code passt, legt die Standardisierung ISO 18004 fest, die aktuelle stammt aus dem Jahr 2015 (siehe ct.de/yvy2). Diese ist gut 115 Seiten lang und definiert fein säuberlich alle Arten von QR-Codes. Das ist nicht wenig, denn es gibt insgesamt 40 Versionen, die mit aufsteigender Versionsnummer immer größer werden. Die kleinste Version 1 nimmt eine Größe von 21 × 21 Pixeln ein, die größte Version 40 177 × 177 Pixel. Die Obergrenze der Speicherkapazität liegt bei 7089 Zahlen (numerisch), 4296 alphanumerischen Zeichen (Großbuchstaben und Ziffern, zzgl. Schrägstrich, Punkt, Komma

u. a.), 2958 Bytes mit beliebiger Kodierung wie UTF-8 oder bei respektablen 1817 Zeichen des japanischen Schriftsystems Kanji.



Mithilfe unserer Vorlage dechiffrieren Sie im Laufe des Artikels einen QR-Code der Version 1 mit 7 Prozent Fehlerkorrektur, der als Nachricht „ct.de“ enthält.

Fehler

QR-Codes enthalten darüber hinaus fehlerkorrigierende Bereiche. Sie sorgen dafür, dass der Code trotz Schäden scanbar bleibt. Insgesamt gibt es vier Stufen der Fehlerkorrektur, die niedrigste L sichert gerade mal 7 Prozent ab, während H einen Schaden von bis zu 30 Prozent ausgleichen

kann. Für die Erfinder des QR-Codes bei der Firma Denso Wave war dieser Umstand besonders wichtig: Da die QR-Codes für ein Lagersystem gedacht waren, sollten diese von Scannern erkannt werden, selbst wenn Schmutz oder Kratzer den Code verunzieren.

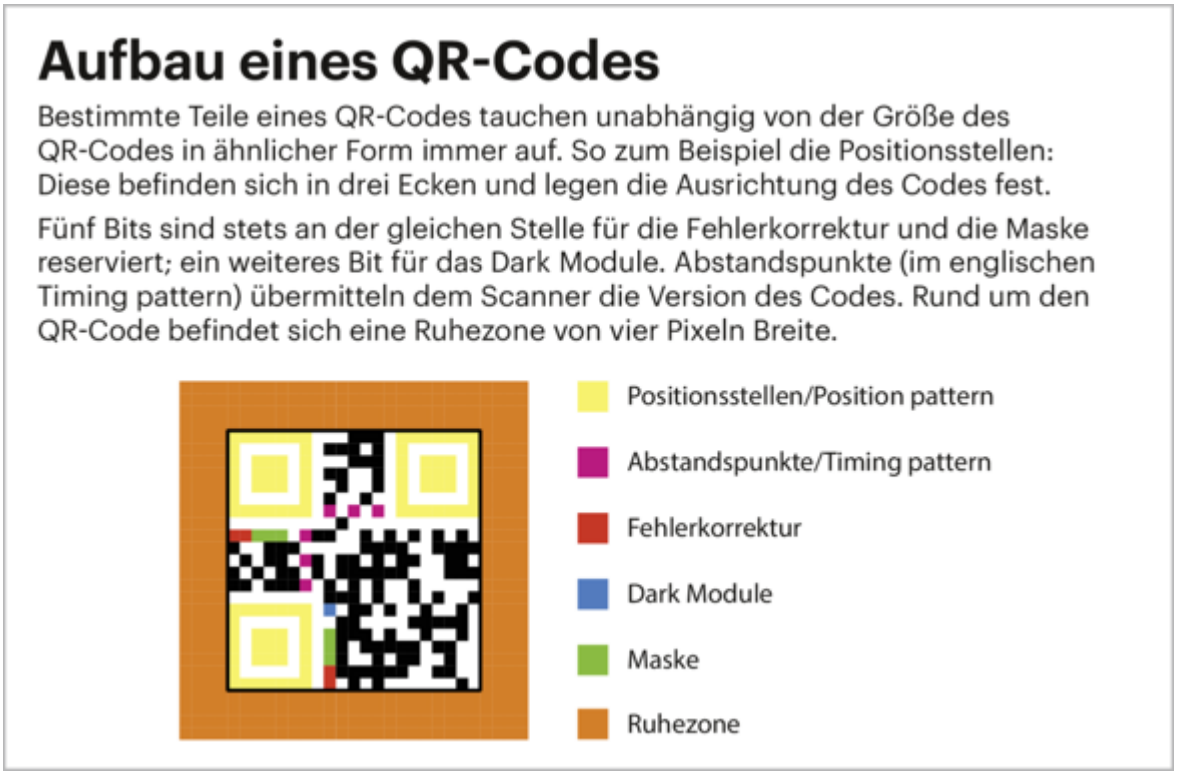
Darum kümmert sich die sogenannte Reed-Solomon-Fehlerkorrektur, benannt nach den Mathematikern und Ingenieuren Irving S. Reed und Gustave Solomon. QR-Codes können damit einen gewissen Grad an Schaden überstehen, weil in dem Code zusätzlich Informationen eingeflochten sind, die eine Wiederherstellung des Codes ermöglichen. Die Methode kommt auch bei CDs oder DVDs zum Tragen, ist aber alles andere als trivial.

Da der Fehlerkorrekturalgorithmus für die Dekodierung des vollständig lesbaren Beispielcodes keine Rolle spielt, gehen wir nachfolgend nicht näher darauf weiter ein. Sie können auch ohne den Algorithmus einen QR-Code dekodieren – das liegt am speziellen Aufbau des Codes, doch dazu im Verlauf des Artikels mehr. Eine ausführliche Erklärung der Methode haben wir unter ct.de/yvy2 verlinkt.

Aufgrund der großen Speicherkapazität und der fehlerkorrigierenden Parts findet der QR-Code in allen möglichen Gebieten Anwendung: beispielsweise im digitalen Impfausweis [2] oder bei der Weitergabe von Transaktionsdaten für Online-Überweisungen [3].

Querschnitt

Das Folgende befasst sich wegen der leichteren Nachvollziehbarkeit mit der kleinsten Version 1, die 21 × 21 Felder misst.



Bestimmte Abschnitte des QR-Codes tauchen unabhängig von Inhalt und Version des Codes immer auf (siehe Schaubild). Einige Elemente sind eher versteckt, wie die Abstandspunkte (im Englischen „Timing pattern“), andere wiederum sehr auffällig, wie die markanten Positionsstellen an den drei Ecken („Position pattern“). Die Konstellation und genaue Größe der Positionsstellen sind kein Zufall: Die Erfinder haben damals herkömmliche Zeitschriften auf besonders selten vorkommende Schwarz-Weiß-Abstände untersucht. Heraus kam ein Verhältnis von 1-1-3-1-1, also einmal Schwarz und Weiß, gefolgt von dreimal Schwarz, und zum Abschluss wieder einmal Weiß und Schwarz. Die direkten Pixel-Nachbarn rund um die Position bleiben abgetrennt weiß.

Bei größeren QR-Code-Versionen gibt es zusätzlich kleinere Positionsstellen an fest definierten Stellen. Der direkte Bereich rund um die Positionsstellen ist dem 15 Bit langen Formatstring vorbehalten (siehe Kasten „Formatstring“), der aus der Maske und dem Level der Fehlerkorrektur besteht.

Es gibt außerdem noch ein Pixel, das immer schwarz ist und in jeder Version an seinem festgeschriebenen Platz verharrt – dieser nennt sich „Dark Module“. Er schreibt vor, welche Farbe

die dunklen Pixel haben sollen, üblicherweise also schwarz.

Maske aufsetzen

In keinem der QR-Codes, den Sie in freier Wildbahn entdecken, entspricht ein schwarzes Pixel immer einer 1 und ein weißer immer einer 0 der kodierten Information. Über ihr liegt nämlich eine Maske, die die schwarzen und weißen Felder visuell so modifiziert, dass die entstehenden Einsen und Nullen möglichst gleichmäßig verteilt sind. Es gibt dadurch keine Anhäufungen von Bereichen, in denen kaum Unterschiede erkennbar sind. Scanner können aufgrund der Maske die Codes leichter erkennen und auslesen, die Wahrscheinlichkeit von Fehlerkennungen sinkt drastisch.

Es kommen acht Masken infrage, die ein QR-Code-Generator auf einen QR-Code anwenden kann. Wenn Sie zum Beispiel auf einer Webseite einen QR-Code zu „ct.de“ erstellen möchten, erzeugt der Generator zunächst einen rohen QR-Code, der jedoch noch nicht optimal lesbar ist. Dann probiert der Generator alle Masken auf dem rohen Code aus und bewertet die Ergebnisse anschließend nach vier Regeln. Welche Maske am Ende der glückliche Gewinner sein darf und auf den QR-Code gelegt wird, entscheidet der sogenannte „Penalty Score“. Das ist eine Art Konto für die Strafpunkte.

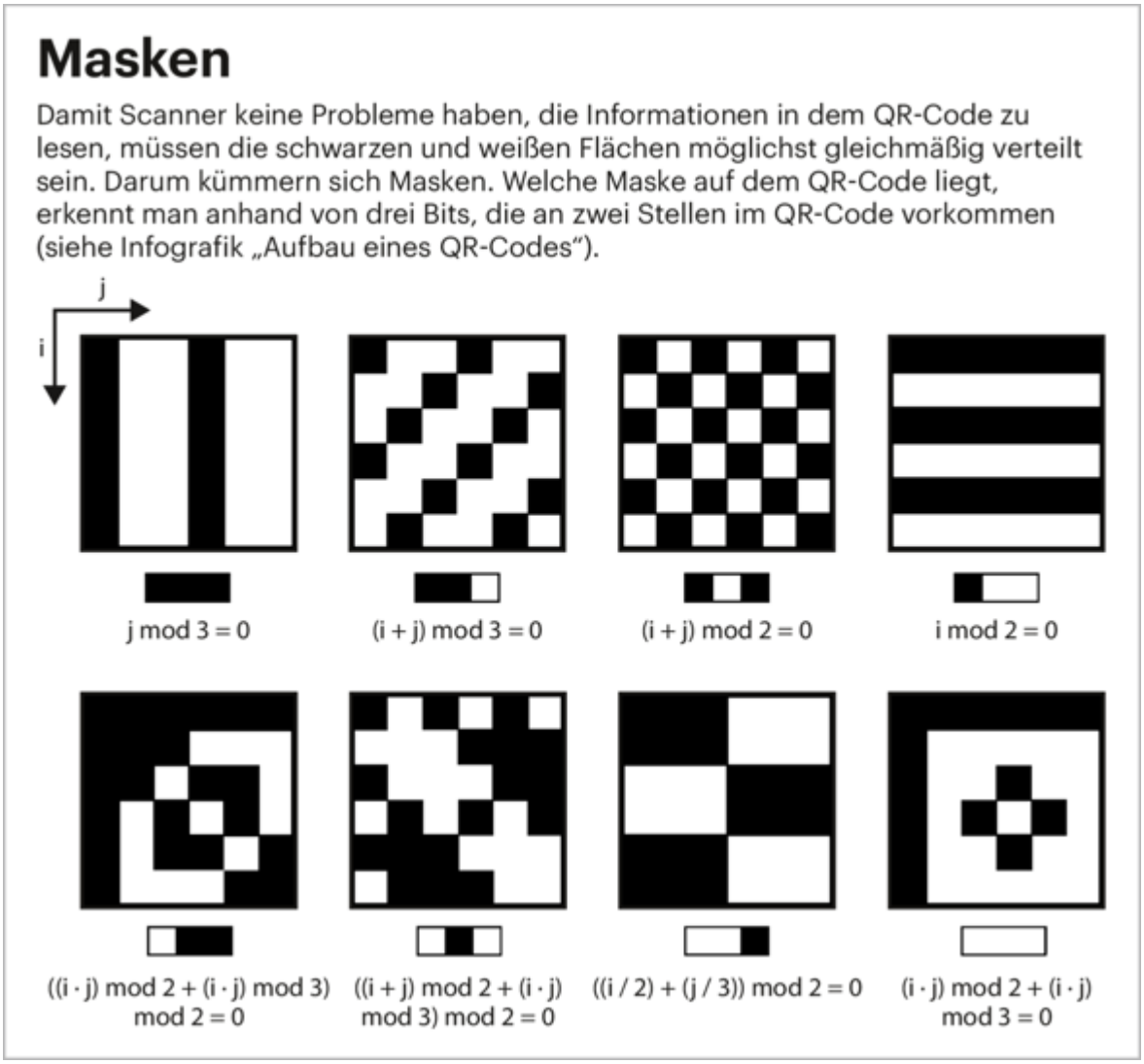
Die erste Regel schreibt vor, dass es Strafpunkte für hintereinander gereihte Pixelketten der gleichen Farbe gibt. Fünf Pixel kosten 3 Strafpunkte, plus 1 für jedes gleichfarbige Pixel, das dahinter folgt. Als Nächstes durchsucht der Generator den Code nach viereckigen Ansammlungen gleichfarbiger Pixel. Für jede gibt es weitere 3 Strafpunkte. Harsche 40 Punkte landen auf dem Konto, wenn der Generator eines der folgenden beiden Muster im Code findet: In binärer Schreibweise lauten die unerwünschten Pixelketten 10111010000 und 00001011101 (0 = weiß, 1 = schwarz). Das entspricht dem Verhältnis der Positionsstellen (1-1-3-1-1), mit vier weißen Pixeln vor oder nach der speziellen Abfolge.

Das letzte Kriterium macht den Kohl nicht fett, zählt aber trotzdem in die Bewertung hinein: das Verhältnis der Anzahl schwarzer Pixel zu der maximalen Pixelanzahl. Ein Version-1-QR-Code enthält 21 · 21 = 441 mögliche Pixel. Wenn beispielsweise 219 davon schwarz sind, entspricht das einem Anteil von gerundet 49,7 Prozent. Der Generator verteilt anschließend geringfügig Strafpunkte, wenn das Verhältnis größer als 5 Prozent zur Mitte ist. Am Ende wählt der Generator die Maske aus, welche die wenigsten Strafpunkte gesammelt hat.

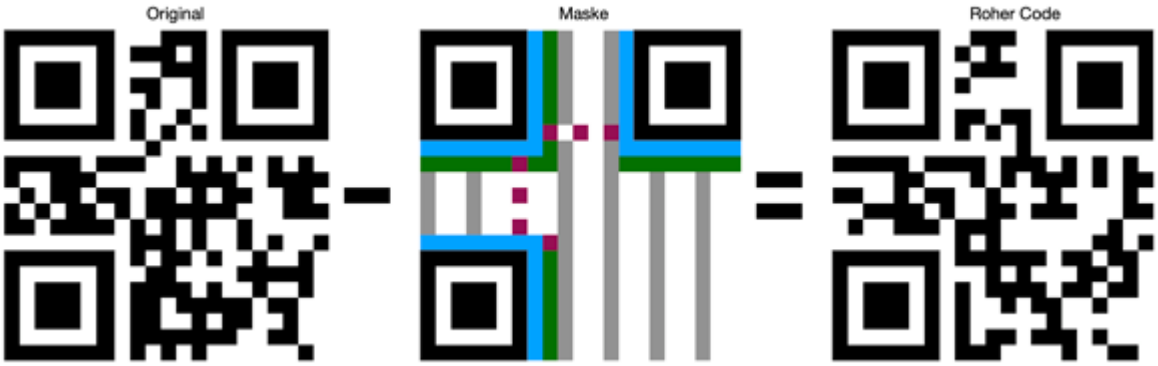
Maske lüften

Als Beispiel dechiffrieren wir im Folgenden einen QR-Code, der die Zeichenkette „ct.de“ enthält. Damit Sie den Schritten leichter folgen können, haben wir für Sie eine Vorlage in Excel vorbereitet, die Sie unter ct.de/yvy2 herunterladen können. Dort befindet sich bereits unser Beispiel-QR-Code, außerdem noch alle acht Masken und weitere Kleinigkeiten, die Ihnen bei der Dekodierung helfen. Die Vorlage eignet sich auch dazu, mal einen anderen QR-Code zu knacken; wie zum Beispiel im Rätsel am Ende des Artikels.

Zurück zu den Masken: Die Information, welche Maske zum Einsatz kam, verbirgt sich im Formatstring (siehe Kasten „Formatstring“). Jede der acht möglichen Masken besitzt eine dreistellige Kombination an Bits, die Sie an zwei Orten im QR-Code ablesen können. Die Infografik „Masken“ schlüsselt für Sie auf, welche Bits für welche Maske stehen.



Für den Beispielcode lauten die Bits 111, was der ersten Maske und der mathematischen Formel j mod 3 = 0 entspricht (j steht für die Spaltennummer, beginnend bei 0, „mod“ liefert den Rest einer Division). Das bedeutet, dass Sie jede dritte senkrechte Zeile invertieren müssen, beginnend mit der ersten. Das können Sie in unserer Vorlage per Hand erledigen, indem Sie die einzelnen Felder umfärben. Dann sieht es ungefähr so aus wie auf dem Bild oben. Obacht: Sie können nicht einfach alle Pixel austauschen, denn es gibt Bereiche, die Sie nicht anfassen dürfen. Das trifft auf die Positionsstellen und direkten Nachbarpixel zu, den Formatstring, die Abstandspunkte und das Dark Module.

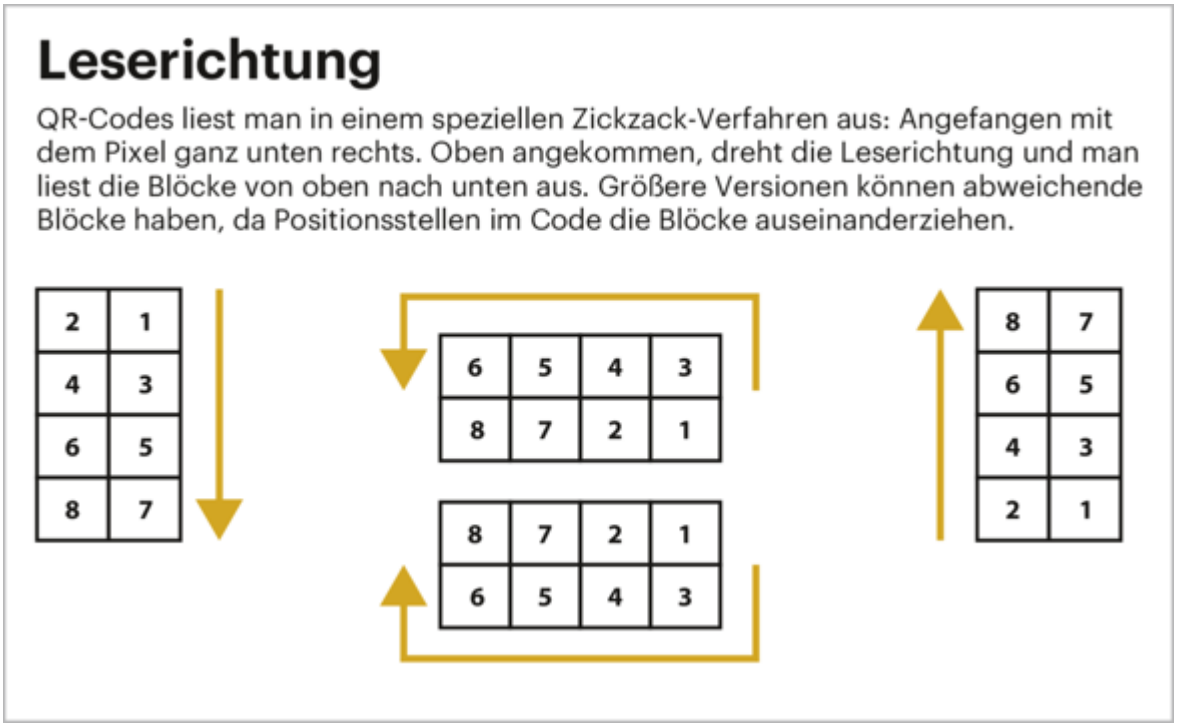


Mit unserer Excel-Vorlage können Sie spielend leicht erkennen, welche Felder Sie bei dem QR-Code invertieren müssen.

Kodierung

Jetzt liegt der QR-Code nackt und unmaskiert dar. Sie benötigen aber noch zwei weitere Informationen, um den Code endlich dekodieren zu können. Zuerst müssen Sie herausbekommen, wie die Nachricht kodiert wurde. Außerdem noch, wie lang die Nachricht ist.

Je nachdem, welches Verfahren der Generator verwendet hat, unterscheidet sich, wie viele Bits hintereinander ein Zeichen darstellen. Denn QR-Codes speichern die Nachricht nicht als Ganzes ab, sondern zerlegen sie in einzelne Zeichen und verpacken die dann beispielsweise binär in einem Block der Größe 2 × 4. Welche Kodierung also der Generator benutzt hat, erkennen Sie an den vier Pixeln ganz unten rechts in der Ecke. Den 2-×-2-Block sowie alle folgenden müssen Sie übrigens ganz speziell auslesen (siehe Infografik „Leserichtung“), angefangen ganz unten rechts. Ein weißes Feld steht für 0, ein schwarzes für eine 1.



Es gibt hierfür acht Möglichkeiten, aber relevant sind nur vier davon: Der numerische Modus (0001) liegt vor, wenn der QR-Code ausschließlich aus den Dezimalzahlen 0 bis 9 besteht. Alphanumerisch (0010) nimmt die Großbuchstaben von A bis Z ohne Umlaute hinzu und ein paar Sonderzeichen wie Dollar, Plus, Minus oder Punkt. Über ct.de/yvy2 finden Sie eine Übersetzungstabelle.

Der am häufigsten vorkommende Encoding-Modus ist 0100 und steht für den Byte-Modus. Damit kann man beliebige Daten in binär kodieren; handelt es sich um Text wie in URLs, dann kommen die verfügbaren Zeichen aus der Zeichentabelle ISO 8859-1. Der Modus bringt das klein geschriebene Alphabet mit, eine große Anzahl an Umlauten und eine ganze Palette an Sonderzeichen. Den letzten Modus treffen Sie vermutlich seltener an, denn hinter 1000 verbirgt sich das japanische Schriftsystem Kanji.

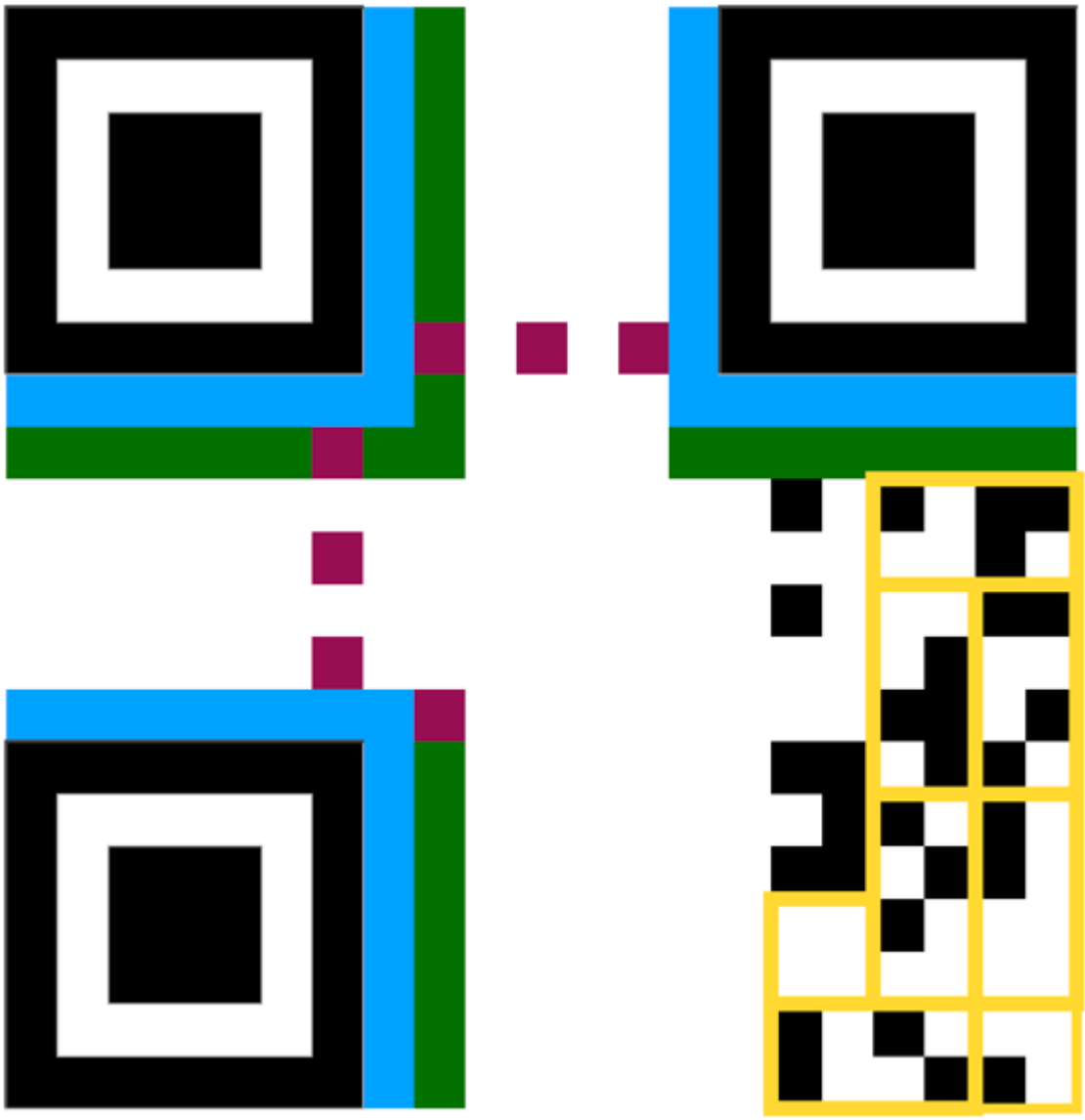
Der Beispiel-QR-Code benutzt den Byte-Modus (0100), was bedeutet, dass jedes Zeichen einem 2-×-4-Block entspricht. Jetzt brauchen Sie nur noch die Länge der Nachricht, um herauszubekommen, wie viele Blöcke Sie hintereinander dechiffrieren müssen. Im Falle des Beispiels wissen Sie die Antwort schon (ct.de = 5 Zeichen), bei einem unbekannten QR-

Code aber nicht. Daher erklären wir noch mal, wo sich die Information befindet und wie sie Sie auslesen.

Die 8 Pixel (2-×-4-Block) direkt über dem 2-×-2-Block mit der Encoding-Information sind für die Länge der Nachricht reserviert. Beachten Sie auch hier wieder die spezielle Leserichtung der Blöcke (siehe Infografik „Leserichtung“)! Sie fangen also wieder unten rechts im Block an, lesen im Zickzack nach oben und schreiben jede neue Zahl rechts dazu. Für die Länge kommt die Bit-Reihenfolge 00000101 heraus. Die Umrechnung können Sie einem entsprechenden binär zu dezimal Rechner überlassen oder es selbst per Hand versuchen. Spoiler: Die Lösung lautet 5; so viele Blöcke müssen Sie dechiffrieren, um an die Botschaft zu gelangen.

Nachricht

Jetzt können Sie, ausgehend von den schon fertigen zwei Blöcken, fünf weitere Blöcke in der korrekten Leserichtung markieren (das sollte ungefähr so aussehen wie auf dem Bild aus unserer Vorlage auf S. 147). Stellen Sie sich vor, als würden Sie von dem allerersten Block unten rechts mit der Encoding-Information eine Zickzacklinie durch alle Blöcke ziehen. Dabei dürfen Sie nicht in die reservierten Bereiche hineintappen. Zu den verbotenen Zonen gehören wie zuvor erklärt der Formatstring, die Positionsmuster, das Dark Module und die Zeilen mit den Abstandspunkten. Ein 2 × 2 Pixel großer weißer Block nach den fünf Blöcken signalisiert das Ende des Klartextes. Alle folgenden Blöcke brauchen Sie nicht zu entschlüsseln, da es sich um die Fehlerkorrektur handelt.



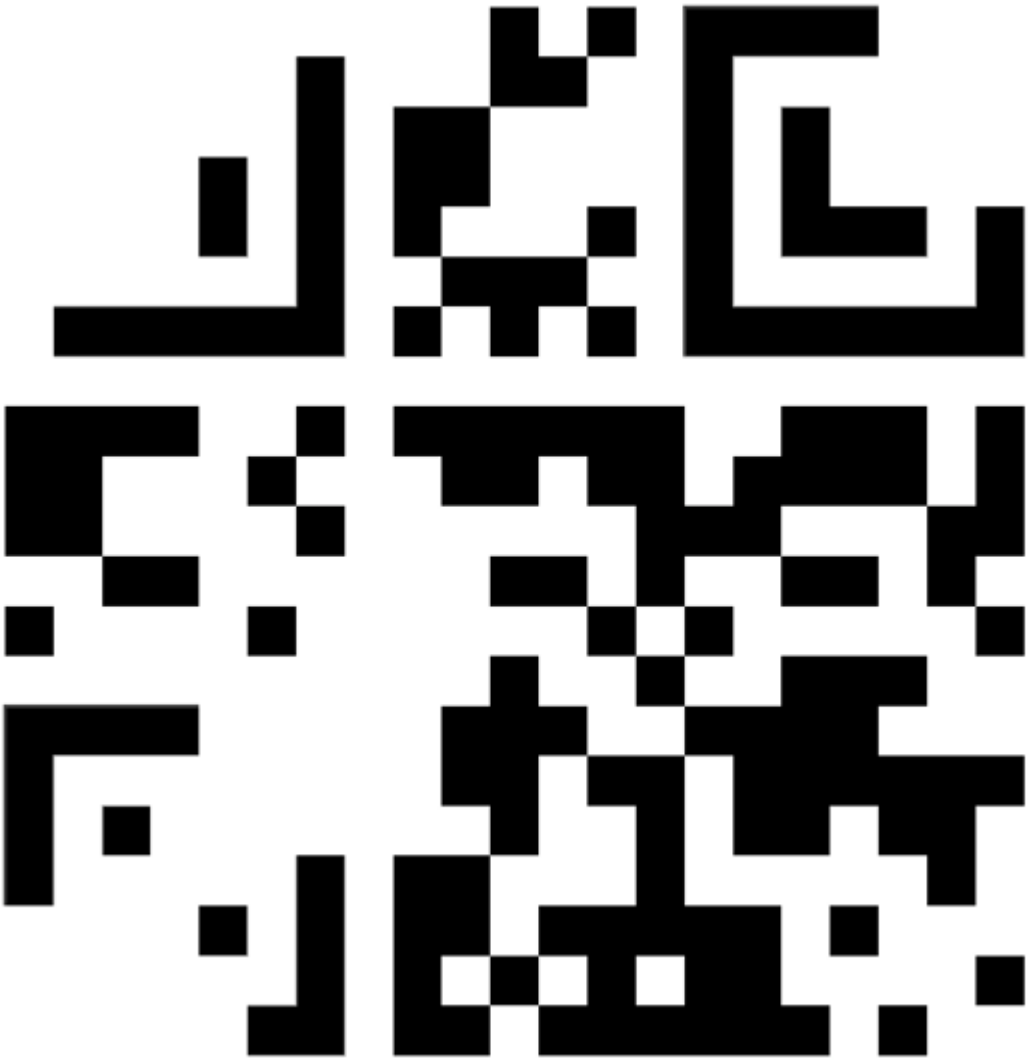
Ganz unten rechts sitzt der Encoding-Block, darüber ein 2-×-4-Block mit der Länge der Nachricht. Daraufhin folgt die Nachricht („ct.de“) aus fünf Blöcken, die bei einem 2 × 2 großen Block aus weißen Pixeln stoppt.
Im ersten Block der Nachricht steht die binäre Zahl 01100011, was in Dezimal umgerechnet 99 ergibt. Ein Blick in die ISO 8859-1 Tabelle verrät (siehe ct.de/yvy2), dass es sich um den Buchstaben „c“ handelt. Der zweite Block liegt seitwärts, passen Sie daher auf, dass Sie den Block korrekt auslesen (siehe Infografik „Leserichtung“). Diesmal kommt binär kodiert 01110100 heraus. Das ist 116 im Dezimalsystem und laut der Tabelle ein „t“.

Bleiben Sie aufmerksam, die Leserichtung ändert sich wieder! Jetzt lesen Sie die nächsten beiden Blöcke von oben nach unten

aus. Für den dritten Block sollten Sie 00101110 herausbekommen; an Stelle 46 in der Tabelle steht dann wie erwartet ein Punkt. Damit haben Sie schon mal mehr als die Hälfte erfolgreich dekodiert. Hinter dem vierten Block verbirgt sich der Buchstabe „d“ (01100100, in dezimal 100), beim letzten Block müssen Sie wieder die geänderte Leserichtung beachten. Für die binäre Darstellung 01100101 (Dezimal: 101) kommt der Buchstabe „e“ heraus. Wenn Sie alles richtig aufgeschrieben haben, sollten Sie gegen einen weißen 2-×-2-Block stoßen, dem Ende des Klartextes. Damit haben Sie die Botschaft „ct.de“ erfolgreich dekodiert.

Letztes Bit

Einen QR-Code per Hand zu entziffern, wird niemals schneller sein als der mobile Begleiter in der Hosentasche. Nichtsdestotrotz lernen Sie auf diese Weise eine Menge über die Funktionsweise der QR-Codes kennen und können sie ohne technische Hilfsmittel dekodieren. Das ist zwar im Alltag nicht wirklich nützlich, hat aber einen hohen Nerd-Faktor! Sudokus kann schließlich jeder lösen, aber QR-Codes?



Rätsel: Diesen QR-Code haben wir absichtlich so weit zerstört, dass er nicht mehr scanbar ist. Schaffen Sie es, die Botschaft im QR-Code zu retten?
Wenn Sie nach der Lektüre nun das Gefühl haben, einen QR-Code per Hand dekodieren zu können, dann probieren Sie Ihr frisch erlangtes Wissen ruhig an unserem kleinen Rätsel aus (der Code befindet sich ebenfalls in der Excel-Vorlage). Wir haben den QR-Code im Bild unten absichtlich so stark beschädigt, dass er nicht mehr scanbar ist. Mit den obigen Schritten können Sie die verlorene Botschaft trotzdem entschlüsseln. Viel Spaß! *(wid@ct.de)*

Formatstring

Bei QR-Codes kommt außer Reed-Solomon ein weiterer Fehlerkorrekturalgorithmus namens Bose-Chaudhuri-Hocquenghem

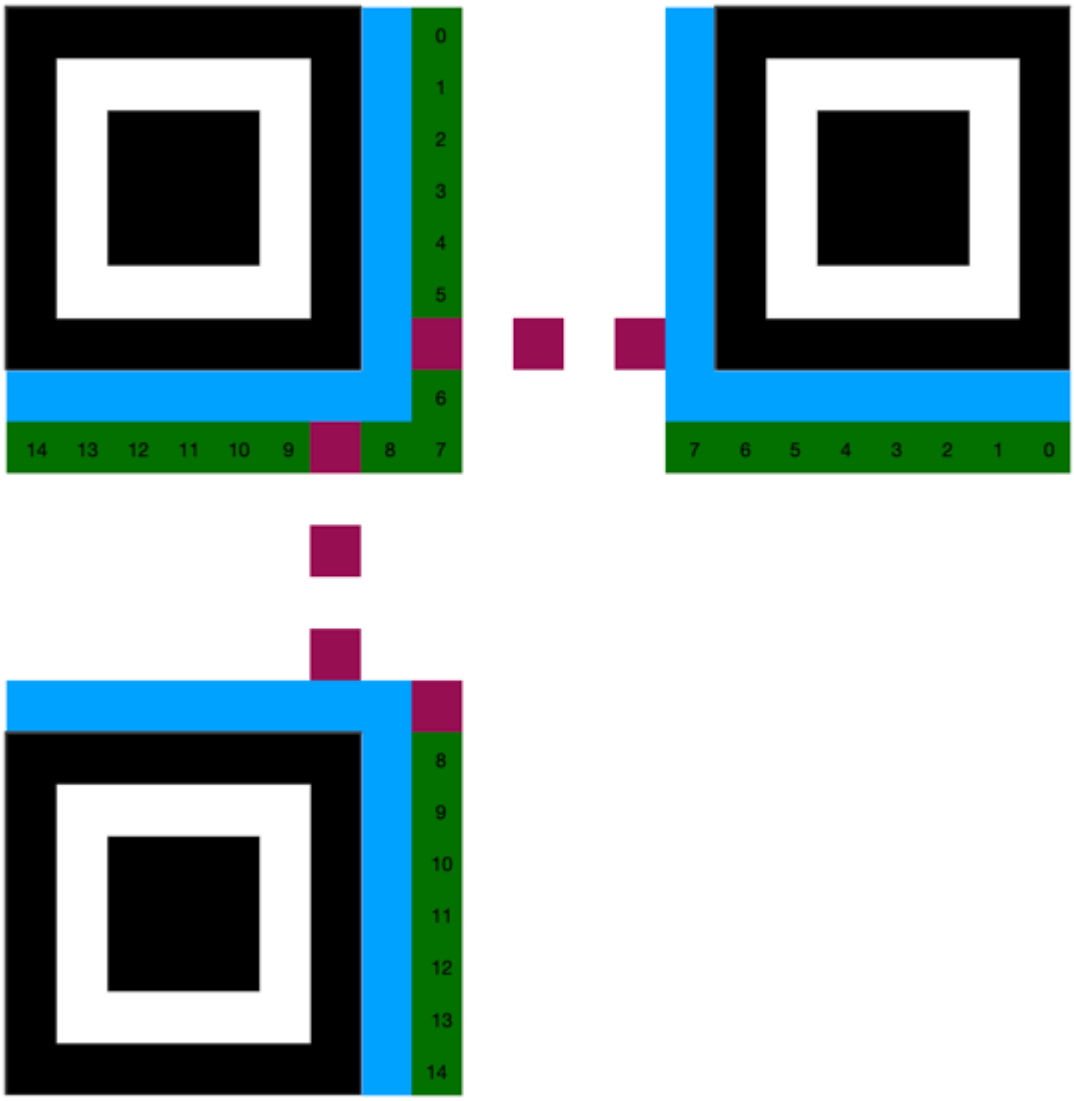
(BCH) zum Einsatz, der den Formatstring schützt. Der String kommt an zwei Orten im QR-Code vor und setzt sich aus insgesamt 15 Bits zusammen: zwei Bits für den Level der Fehlerkorrektur und drei Bits für die Maske. Die restlichen zehn sind für die Fehlerkorrektur. Im Folgenden erklären wir, wie die Fehlerkorrektur mit BCH berechnet wird.

Falls Sie einen Blick in den ISO-Standard werfen, stellen Sie fest, dass sich die Reihenfolge und Nummerierung der Masken von der in unserer Infografik unterscheidet. Das liegt daran, dass auf dem Formatstring eine spezielle Maske aufliegt, die verhindern soll, dass irgendeine Kombination von Level der Fehlerkorrektur und Maske fünf Nullen hintereinander ergibt. Dadurch ergeben sich für die Infografik eine andere Reihenfolge und Kennzeichnung, als es der ISO-Standard vorschreibt. Unsere Infografik berücksichtigt im Grunde also nur die draufgelegte Maske, wodurch sich zwar andere Reihenfolgen ergeben, aber so brauchen Sie nicht den Formatstring lernen, um einen QR-Code zu dekodieren. Für den Formatstring dagegen benötigt man die originale rohe Maskeninformation, und die stammt aus dem ISO-Standard (siehe ct.de/yvy2).

Für die Fehlerkorrektur kommen folgende vier Level infrage: L lässt 7 Prozent Schaden zu (01), M 15 Prozent (00), Q 25 Prozent (11) und H 30 Prozent (10). Je nachdem, wie der rohe QR-Code aussieht, kann sich der Generator für eine von acht Masken entscheiden, die von 000 bis 111 binär durchnummeriert sind (eine Liste finden Sie unter ct.de/yvy2). Der QR-Code mit der Nachricht „ct.de“ verwendet die Fehlerkorrektur L (01) und die Maske 010 (aus dem ISO-Standard), kombiniert ergibt das 01010. Als Nächstes berechnet man aus dem 5-Bit-Original 10 Bit an Fehlerkorrektur. Doch dafür braucht man einen Generator.

Für jede Version eines QR-Codes gibt es eine festgelegte Generator-Gleichung; für Version 1 lautet er $x^{10} + x^8 + x^5 + x^4 +$

$x^2 + x + 1$. Keine Angst, die Gleichung brauchen Sie sich nicht zu merken. Die Gleichung übersetzt man in binär von links nach rechts: Jedes x^n ergibt eine 1, fehlende Exponenten wie x^9, x^7 oder x^6 eine 0. Somit kommt 10100110111 als der Generator heraus.



Gegen Schäden geschützt: An zwei Stellen im QR-Code können Sie den Formatstring ablesen.
Danach bringt man das Original 01010 auf eine Länge von 15 Bits, indem man zehn Nullen anhängt. Danach werden vorne überstehende Nullen entfernt. Der Formatstring lautet damit vorerst 101000000000000, mit einer Länge von 14 Bits. Man verrechnet nun so lange den Formatstring mit dem Generator, bis das Ergebnis zehn Bits oder kürzer ist. Damit man beide Zahlen verrechnen kann, bringt man den Generator ebenfalls auf

eine Länge von 14 Bits, indem man die fehlenden drei Nullen anhängt (10100110111000).

Für die Kalkulation beider Zahlen braucht man den XOR-Operator: Jede Kombination von 0 und 1 ergibt 1, während bei 0 und 0 sowie 1 und 1 eine 0 herauskommt. Das ist bei dem Beispiel gleich beim ersten Versuch erreicht: 10100000000000 XOR 10100110111000 = 00000110111000. Manchmal benötigt man aber mehrere Durchläufe. Schneidet man die Nullen auf der linken Seite alle ab, kommt ein 9 Bit langer String heraus. Da der String aber 10 Bits lang sein soll, muss man eine Null auf der linken Seite übrig lassen. Der rohe Formatstring besteht jetzt aus dem Original 01010 und der gerade berechneten Fehlerkorrektur 0110111000.

Zuletzt legt man die Maske 101010000010010 via XOR auf den rohen Formatstring. Der finale Formatstring lautet also 010100110111000 XOR 101010000010010 = 111110110101010. Das entspricht den exakten 15 Bits, wie Sie sie auf dem Aufmacher oder dem Beispiel-QR-Code sehen.

1. Literatur
2. André Kramer, Quadratisch, praktisch, Code, Erfinderische und praktische Anwendungen für QR-Codes, c’t 7/2013, S. 140
3. Gerald Himmelein, Multipass, Inhalt, Apps und Datenschutz: So funktioniert das digitale Impfzertifikat, c’t 15/2021, S. 34
4. Jan Mahn, Schöner zahlen, Rechnungen schneller überweisen mit QR-Codes, c’t 7/2022, S. 138

QR-Code Linksammlung: ct.de/yvy2

E-Mails sichern und archivieren

E-Mails sichern und archivieren

[expand title="mehr lesen…"]

Praxis Mails archivieren

Bild: Albert Hulm

Postlagernd

E-Mails sichern und archivieren

Posteingang und Ordner des E-Mail-Programms sind häufig ein wertvoller Datenschatz. Es ist keine schlechte Idee, ihn von Zeit zu Zeit zu sichern. Von Stefan Wischner

Das wichtigste und wertvollste Sammelbecken für Informationen ist für viele Nutzer nicht etwa das Verzeichnis mit den Arbeitsdokumenten, sondern die Postfächer und Ordner im Mailprogramm. Sie dienen häufig als Projekt- und Kontakthistorie, sogar als Dateisammlung in Form von ansonsten nicht abgelegten Anhängen.

Eigentlich müsste man sich um diese Datensammlung keine großen Sorgen machen: Zumindest bei per IMAP oder Exchange angebundenen Mailkonten liegt alles sicher auf dem Mailserver, meist bei einem großen Provider, wird dort regelmäßig gesichert und ist geschützt vor jedweden Problemen des eigenen Rechners. Der Hüter dieses Schatzes ist also der Mailprovider; das Tor dorthin das Mailprogramm. Genau das ist nicht nur beruhigend. Was ist zum Beispiel, wenn der Provider das Konto sperrt oder man ihn einfach wechseln will? Oder wenn das E-Mail-Programm gerade dann zickt, wenn man dringend eine Info aus einer älteren Mailnachricht braucht?

Beruhigend wäre in jedem Fall ein lokales Backup aller Mails und Ordner, am besten in einem Format, das möglichst jedes beliebige Mailprogramm lesen kann oder – noch besser – das notfalls auch ganz ohne Mailclient seine Inhalte preisgibt. Die gute Nachricht: Das geht mit fast jedem Mailprogramm, wenn auch nicht automatisch. Die schlechte: Es gibt keine einheitliche Methode, einzelne Nachrichten, Ordnerinhalte und

komplette Ordnerstrukturen zu sichern und zudem unterschiedliche Dateiformate. Denen wollen wir uns zuerst widmen.

Formate

Die Formate, in denen man Mails und Ordner exportieren kann, teilen sich in zwei Gruppen: Die eine umfasst Formate wie PST, MBOX, EML und MSG. Diese Dateien lassen sich verlustfrei auch wieder in ein Mailprogramm importieren. Für die Software- und Plattform unabhängige „Einweg"-Archivierung bieten sich allgemeine Formate wie PDF oder HTML an.

OST, PST: Dabei handelt es sich um binäre, proprietäre Formate von Microsoft Outlook. OST wurde mit Outlook 2016 eingeführt und kommt nur bei IMAP- und Exchange-Konten zum Einsatz. OST-Dateien dienen als lokaler Offline-Cache für Nachrichten, die vom Mailserver heruntergeladen wurden. Outlook verwaltet OST-Dateien selbstständig und erlaubt weder deren Ex- noch Import; als Datensicherung oder für die Migration taugen sie daher nicht.

Anders verhält es sich mit PST-Dateien. Diese dienten früheren Outlook-Versionen als lokaler Speicher für Nachrichten inklusive Dateianhängen, Terminen, Aufgaben und Kontakten, bis sie von den erwähnten OST-Dateien weitgehend abgelöst wurden. Nur für POP3-Postfächer nutzt Outlook weiterhin PST-Dateien – und für den Im- und Export. Outlook erlaubt es, Ordnerinhalte – auch verschachtelte Strukturen – als PST-Dateien zu exportieren und kann diese auch wieder einlesen. Das gilt unabhängig davon, ob es um Mails auf einem POP3-, IMAP oder Exchange-Konto geht. Damit eignen sich PST-Files sehr gut zur Datensicherung. Der Haken: Es handelt sich um ein Binärformat, das nur Outlook selbst, einige andere E-Mail-Clients (zum Beispiel Thunderbird mit dem Add-on ImportExportTools NG und eM Client[1]) und einige Spezialprogramme (etwa MailStore, dazu später mehr) lesen können.

MBOX: Ähnlich wie Outlooks PST-Format kann eine MBOX-Datei komplette Ordnerstrukturen nebst aller enthaltenen Nachrichten speichern. MBOX kommt ursprünglich aus der UNIX-Welt und unterscheidet sich von PST in einem wesentlichen Punkt: MBOX-Dateien liegen im Textformat vor und lassen sich auch ohne Mailprogramm mit einem beliebigen Editor lesen. Das ist aber anstrengend, denn die Nachrichtentexte verstecken sich zwischen Metadaten, HTML-Code und großen Textblöcken mit Zeichensalat. Letztere sind eingebettete Dateien, per Base64 in druckbare Zeichen kodiert. Nahezu alle E-Mail-Programme (Outlook ausgenommen) können MBOX-Dateien importieren und wieder in die ursprüngliche Nachrichtenform mit Anhängen bringen. Alternativ gibt es etliche MBOX-Viewer-Tools im Netz, wenngleich deren kostenlose Versionen meist eingeschränkt sind. Die Flexibilität und Verbreitung machen MBOX zum sinnvollsten Backup- und Archivformat für Mails.

```
68      T9YafQW4mGhlpKkDntCpCFLDTHZUavP8b91JtWpFGCd0S0NCsltvMQJcTYa7ey47cPZ/kL2rLPd
69      aJkGF+od2nOWvHPToSwwcGKLTYEc=
70  X-TMASE-SNAP-Result: 1.821001.0001-0-1-12:0,22:0,33:0,34:0-0
71  X-TMASE-INERTIA: 0-0;;;;
72  X-Spam-Score: (-) -1.9
73  X-Sender: [redacted].net
74  X-Scan-Signature: 57630e95f7146bb794c33d98cfd5f6df
75
76  ------=_NextPart_000_2749_01D6C4D9.C9507950
77  Content-Type: text/plain;
78      charset="iso-8859-1"
79  Content-Transfer-Encoding: quoted-printable
80
81  Hallo Stefan
82
83  =20
84
85  Mails, die im EML- oder MBOX-Format gespeichert sind, lassen sich zwar mit
86  einem Editor lesen. Es ist aber nicht einfach, den Nachrichteninhalt
87  zwischen all den Header-Daten, dem HTML-Code und eingebetteten Dateien zu
88  finden. Besser ist es, die Dateien in einen E-Mail-Client zu laden.
89
90  =20
91
92  [redacted]
93
94  Alter Ego
95
96  =20
97
98  =20
99
100
101 ------=_NextPart_000_2749_01D6C4D9.C9507950
102 Content-Type: text/html;
103     charset="iso-8859-1"
104 Content-Transfer-Encoding: quoted-printable
```

MBOX-Dateien enthalten Nachrichten und Dateianhänge in reiner

Textform und lassen sich mit jedem Editor lesen. Die relevanten Textinhalte der Mails zu finden, kann aber mühsam sein.
EML: Wie beim MBOX-Format stecken in EML-Dateien Mailnachrichten im Textformat nebst Headern, Formatangaben, HTML-Code und Base64-kodierten Anhängen. Allerdings enthält jede EML-Datei immer nur genau eine Nachricht. Genutzt wird das Format zum Beispiel von Thunderbird. Interessanterweise kannte auch das längst eingestellte Outlook-Express EML-Dateien. Die zu Microsoft Office gehörenden Outlook-Versionen unterstützen das Format jedoch nicht.

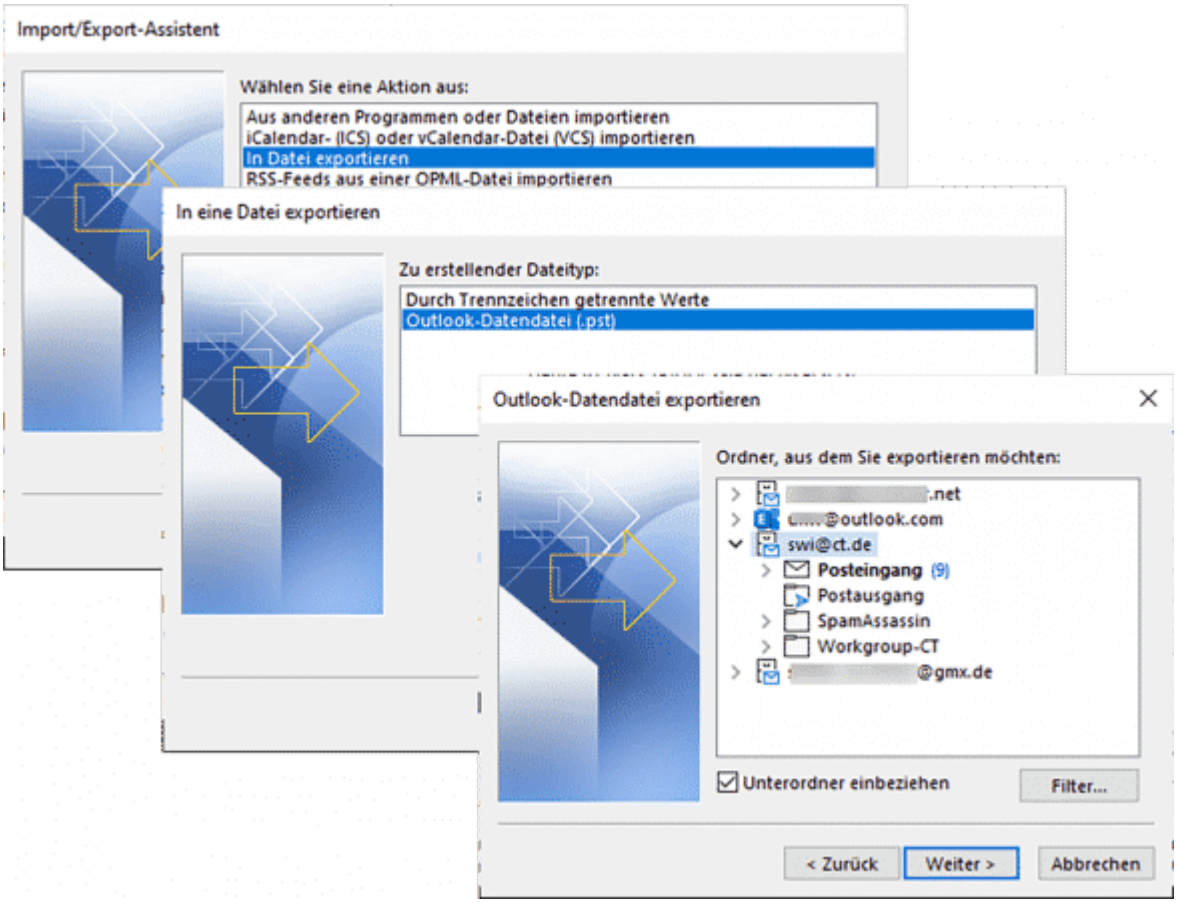
MSG: Das Outlook-Gegenstück zu EML sind MSG-Dateien, die zum Beispiel dann entstehen, wenn man aus Outlook eine Nachricht per Drag & Drop in einen Ordner oder auf den Desktop zieht oder „Datei/Speichern unter“ verwendet. MSG ist zwar wie PST ein Binärformat, das sich nur in Outlook öffnen lässt. Lädt man eine solche Datei in einem Texteditor, finden sich aber Text- und Headerinhalte gut lesbar zwischen Blöcken von Sonderzeichen.

Die Konvertierung von EML- in MSG-Dateien und umgekehrt erlaubt zum Beispiel das für Einzeldateien kostenlose Tool E-Mail-Converter von IN MEDIA (siehe ct.de/yjr5).

PDF: An sich gäben PDF-Dateien ein hervorragendes Archivformat für E-Mails ab, sind sie doch plattformunabhängig und von vielen Programmen lesbar. Zwar exportiert nur Thunderbird mit passendem Add-on (dazu gleich mehr) Ordnerinhalte im PDF-Format, man kann sich aber bei allen anderen mit einem PDF-Drucker behelfen. Windows 10 bringt sogar schon einen mit (Microsoft Print to PDF). Die Methode hat aber einige Haken: So bleiben nicht nur extern nachgeladene Inhalte (Bilder) auf der Strecke, sondern auch angehängte Dateien. Komplette Ordnerstrukturen kann man nicht per PDF-Drucker exportieren, sondern maximal alle Nachrichten eines einzelnen Ordners. Je nach Mail-Client entsteht dabei entweder ein einziges großes PDF-Dokument (etwa bei Outlook) oder Sie werden bei der

Ausgabe für jede einzelne Nachricht nach einem Dateinamen gefragt. Die Sicherung von E-Mails als PDF ist eine Einbahnstraße für Archivzwecke, ein Rückimport in ein E-Mail-Programm ist nicht möglich.

Welche Möglichkeiten und Formate es zum Export und Import von Nachrichten, Ordnern und kompletten Ordnerstrukturen eines Kontos gibt, hängt ganz vom verwendeten E-Mail-Client ab [1].



Microsoft Outlook erlaubt den verlustfreien Ex- und Import von Ordnern und Nachrichten nur in seinem eigenen PST-Format. Nur bei POP3-Konten nutzt es das auch als lokalen Datenspeicher.

Microsoft Outlook

Intern nutzt Outlook das PST-Format für POP3-Konten. Um die Ordner eines POP3-Kontos zu sichern, reicht es daher, Kopien der zugehörigen PST-Dateien anzulegen. Deren Speicherort finden Sie in Outlook unter „Datei/Kontoeinstellungen/Kontoeinstellungen …“ im Karteireiter „Datendateien“. Deutlich komfortabler und auch

für IMAP- und Exchange-Konten geeignet ist die Export-Funktion von Outlook, die auch eine Auswahl der zu exportierenden Ordner erlaubt: Wählen Sie „Datei/Öffnen und Exportieren/Importieren/Exportieren“ und im folgenden Dialog „In Datei exportieren“. Nach einem Klick auf „Weiter“ wählen Sie „Outlook-Datendatei (.pst)“ und im nächsten Fenster die Daten, die Sie exportieren möchten. Sie können ein komplettes Konto oder einzelne Ordner mit oder ohne Unterordnern auswählen. Über den „Filter …“-Button lassen sich die Export-Daten weiter begrenzen, etwa durch einen Datumsbereich. Zuletzt legen Sie noch den Zielspeicherort und Dateinamen fest und starten den Export mit „Fertig stellen“.

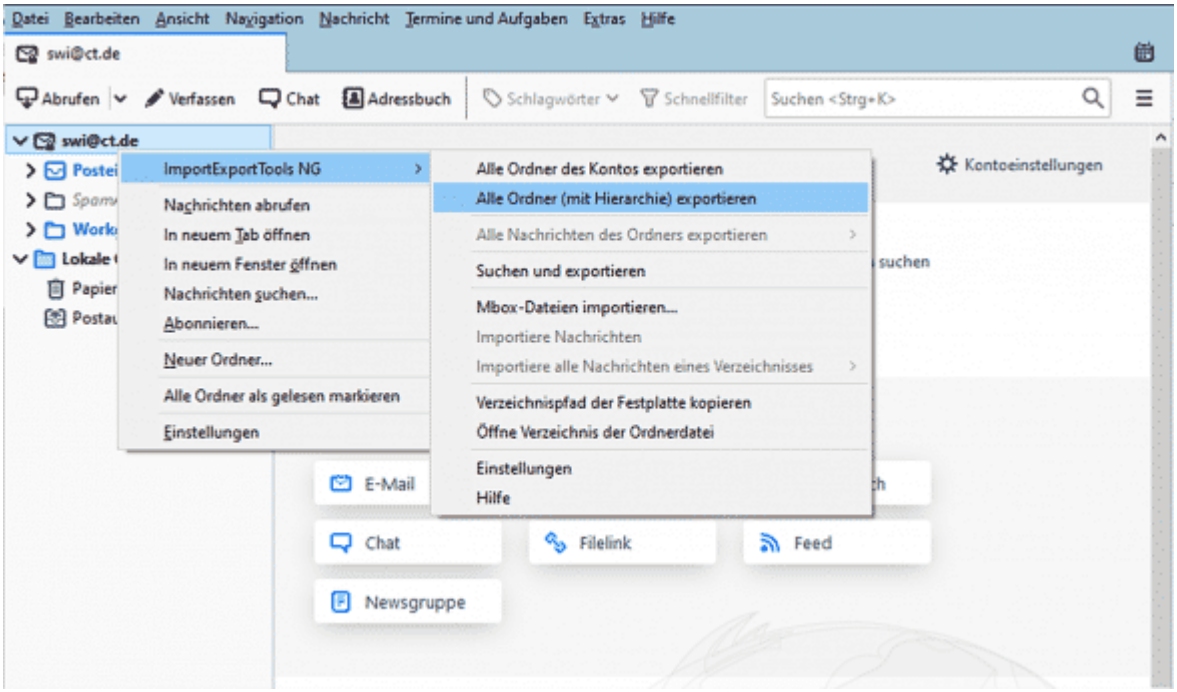
Die erzeugte PST-Datei lässt sich später wieder in Outlook importieren. Einige andere Programme unterstützen das Format ebenfalls.

Mozilla Thunderbird

In der Grundausstattung fehlt Mozilla Thunderbird auch in der aktuellen Version 78 die Möglichkeit, komplette Ordnerstrukturen zu exportieren. Lediglich einzelne (oder gesammelt etwa mit Strg+A markierte) Nachrichten lassen sich im EML-Format speichern. Dazu klicken Sie die entsprechende Nachricht (oder eine der markierten) mit der rechten Maustaste an und wählen aus dem Kontextmenü „Speichern unter“. Nach der Auswahl eines Zielverzeichnisses landen alle selektierten Nachrichten als einzelne EML-Dateien mit der jeweiligen Betreffzeile als Dateiname darin.

Um komplette Ordnerstrukturen und -inhalte zu exportieren, benötigen Sie das Add-on „ImportExportTools NG“. Das fügen Sie am besten aus Thunderbird heraus über „Extras/Add-ons“ hinzu. Danach steht im „Extras“-Menü sowie in den Kontextmenüs von Konten und Ordnern in der Navigationsliste ein neuer Befehl „ImportExportTools NG“ mit diversen Untermenüs zur Verfügung. Darüber können Sie MBOX-Dateien im- und exportieren und über „Einstellungen“ vieles anpassen, wie zum Beispiel die

Namensvergabe oder automatische Backups. Einzelne Ordner lassen sich über den Menüpunkt „Alle Nachrichten des Ordners exportieren“ nicht nur im MBOX-Format, sondern auch als separate PDF-, HTML- oder Textdateien speichern, optional mit Anhängen. Die landen in separaten Unterverzeichnissen mit Links (HTML) oder mit Pfad- und Dateinamen (TXT) in den jeweiligen Nachrichten. Beim PDF-Export hingegen gehen sie verloren.



Thunderbird erlaubt den Export von Ordnerstrukturen und Mailkonten nur mit dem Add-on „ImportExportTools NG“, unterstützt dann aber sehr viele, teils auch ohne Mailprogramm nutzbare Formate.

eM Client

Der an sich funktionsreiche eM Client erlaubt zwar den Import von MBOX- und PST-Dateien, nicht aber deren Export. Es lassen sich jedoch einzelne oder als Gruppe markierte Nachrichten über „Menü/Datei/Exportieren …“ im EML-Format speichern. Das klappt auch mit kompletten Mailkonten und allen enthaltenen Ordnern, die man beim Export lediglich einzeln auswählen muss. Im Zielverzeichnis entstehen dann entsprechende Unterordner mit den EML-Dateien. Es gibt zudem auch eine integrierte Backup-Funktion für komplette Konten, die sichert aber nur im

vom eM CLient auch für die interne Datenhaltung genutzten Datenbankformat. Wer eine einzelne MBOX-Datei archivieren möchte, muss das mit einem anderen Client tun oder alternativ mit Mailstore Home (siehe unten).

Webmailer

Statt eines dedizierten Mailprogramms nutzen viele einen Webmailer, also das Browser-Frontend des jeweiligen Providers. Nicht alle davon bieten die Möglichkeit, Nachrichten und Ordner als Kopie auf den lokalen Rechner herunterzuladen. GMX beispielsweise erlaubt das nicht bei einem Freemail-Konto, wohl aber in Verbindung mit DE-Mail. Im Zweifel konsultieren Sie die Hilfsfunktion des Providers oder nutzen zumindest für den Datenexport doch einen Mail-Client oder Mailstore Home (siehe unten).

Zwei der gängigsten Dienste, Google Mail und Outlook.com, erlauben den Download, haben die entsprechende Funktion nur etwas versteckt: Für Gmail-Nutzer führt der Weg zur Seite takeout.google.com. Sie ermöglicht den Download vieler persönlicher Google-Daten, etwa Fotos, Android-Einstellungen und YouTube-Suchverläufe. Da Sie nur die Mailordner herunterladen möchten, klicken Sie am Anfang der Diensteliste auf „Auswahl aufheben“, scrollen dann bis zu „Gmail“ herunter und setzen nur dort das Häkchen. Am Ende der Liste klicken Sie auf „Nächster Schritt“, wählen dann „Einmal exportieren“ und das Archivformat (ZIP). Nach einem Klick auf „Export erstellen“ landet eine Mail in Ihrem Gmail-Postfach, die einen Downloadlink für die gepackte MBOX-Datei enthält.

Nutzer eines Microsoft-Mailkontos klicken im Webmailer auf das Zahnrad rechts oben, dann ganz unten auf „Alle Outlook-Einstellungen anzeigen“. Im folgenden Fenster wählen Sie in der ersten Menüspalte „Allgemeine Einstellungen“ und in der zweiten „Datenschutz und Daten“. Klicken Sie dann rechts auf „Daten exportieren“. Wie bei Google erhalten Sie dann einen Downloadlink für eine gepackte PST-Datei per Mail, was

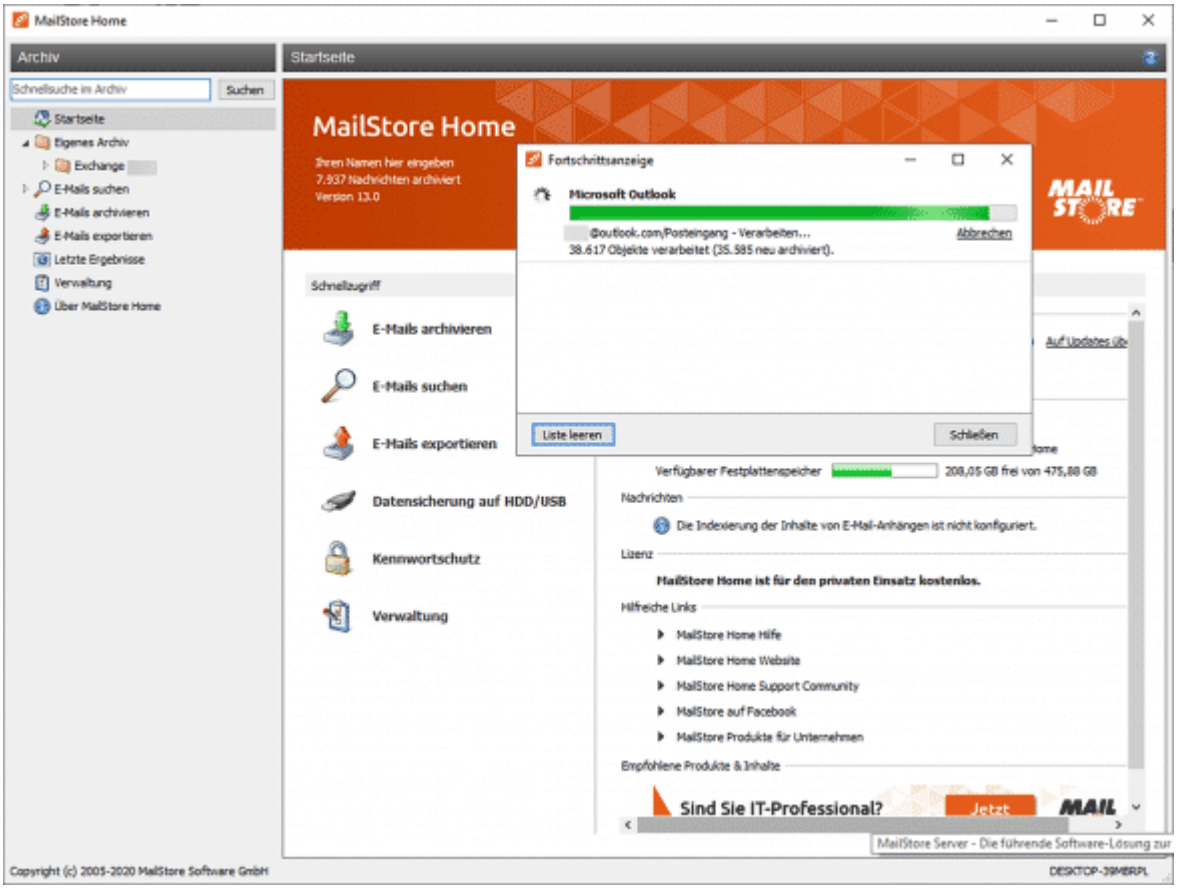
allerdings laut Microsoft bis zu vier Tage(!) dauern kann.

Apple Mail

Der Ex- und Import kompletter Accounts mit allen Ordnern im bordeigenen Mailclient von macOS ist sehr einfach: Klicken Sie in der Navigationsliste den entsprechenden Account mit der rechten Maustaste an, wählen Sie „Postfach exportieren“ und im nächsten Dialog einen Speicherort. Apple Mail speichert grundsätzlich im MBOX-Format und kann solche Dateien über „Ablage/Postfächer importieren“ auch laden.

Komfortable Mail-Sicherung mit Mailstore Home

Abseits der beschriebenen Export- und Backupoptionen mit Bordmitteln der E-Mail-Clients gibt es zumindest für Windows-Nutzer eine elegante Lösung mit einem externen Programm aus deutscher Produktion: Das für die private Nutzung kostenlose Mailstore Home (siehe ct.de/yjr5) holt sich Nachrichten und Ordner inklusive Dateianhängen wahlweise aus lokalen Sicherungsdateien (PST, MBOX, EML, MSG), aus den Profilen von Thunderbird und Outlook und sogar – wenn Sie die zugehörigen Zugangsdaten eingeben – direkt vom Mailserver. Die importierten Inhalte werden in einer lokalen SQLite-Datenbank abgelegt und lassen sich mit dem Programm genauso ansehen wie in einem Mail-Client. Mailstore Home bietet zudem eine leistungsfähige Suchfunktion.



Das für die private Nutzung kostenlose Mailstore Home holt sich Mails und Ordner nebst Anhängen auf verschiedenen Wegen und speichert sie in einer eigenen durchsuchbaren Datenbank.
Es lassen sich beliebige Profile anlegen und so zum Beispiel mehrere Mailkonten in die Datenbank übertragen. Je nach Umfang der Postfächer kann das erstmalige Einlesen recht lange dauern, folgende Imports laufen deutlich schneller, weil das Programm nur noch die Änderungen abgleicht. Umgekehrt können Sie Mails aus MailStore Home exportieren, zum Beispiel direkt auf einen Mailserver, an einen Client oder in eine PST- oder einzelne MSG- oder EML-Dateien.

Tipp: Auch wenn Sie Mailstore Home regulär auf Ihren Rechner installiert haben, rufen Sie das Setup-Programm nochmals auf. Nehmen Sie das Angebot an, eine portable Version einzurichten; die legen Sie am besten auf einen externen Datenträger zusammen mit Sicherheitskopien der Mailstore-Datenbank.

Nicht GoBD-konform!

Ein wichtiger Hinweis zum Schluss: Die beschriebenen Methoden

eignen sich durchwegs für die Sicherung von E-Mails und Ordnern, folgen aber nicht den Vorgaben der GoBD. Diese 2014 vom Bundesministerium für Finanzen herausgegebene und zuletzt Anfang 2020 überarbeitete Richtlinie beschreibt die ordnungsgemäße revisionssichere Archivierung von steuerrelevanten Unterlagen, zu denen auch geschäftliche E-Mails gehören können. Eine GoBD-konforme Archivierung bietet keiner der gängigen E-Mail-Clients; dazu sind entsprechende Dokumentenmanagement-Systeme, Online-Dienstanbieter oder passende Services von Mailprovidern erforderlich. Von Mailstore gibt es auch eine kostenpflichtige Server-Version, die die GoBD-konforme Archivierung von E-Mails verspricht. *(swi@ct.de)*

1. Literatur
2. Jo Bager, Holger Bleich, Sylvester Tremmel, Stefan Wischner, Solide Kuriere, 8 Mailprogramme für den Desktop im Vergleich, c't 25/2020, S. 72

Tools zur Mailsicherung: ct.de/yjr5

[/expand]

Performance-Probleme in Websites erkennen und beseitigen

Performance-Probleme in Websites erkennen und beseitigen

[expand title="mehr lesen…"]

Performance-Probleme in Websites erkennen und beseitigen

Praxis Web-Performance

Bild: Rudolf A. Blaha

Ungebremst

Performance-Probleme in Websites erkennen und beseitigen

Surfer schätzen komplexe Apps, geschmeidige Animationen, Webfonts, Videos und hochauflösende Fotos. Viele Seiten laden, derart aufgemotzt, aber zu langsam. Lahme Websites wieder flott zu machen ist ein Mehrkampf mit vielen Disziplinen – ein Überblick. Von Herbert Braun

Eine durchschnittliche Webseite wiegt heute zwei MByte, die sich auf 75 HTTP-Requests verteilen (siehe ct.de/yp4b). Fast ein halbes MByte JavaScript-Code hat der Browser dabei zu verdauen. Gleichzeitig sind die Nutzer nicht mehr so geduldig wie zu ISDN-Zeiten: Drei Sekunden leerer Bildschirm sind für manchen Besucher schon zu viel. Eine Website, die nach zehn Sekunden noch nicht geliefert hat, wird den überwiegenden Teil ihrer Besucher verloren haben.

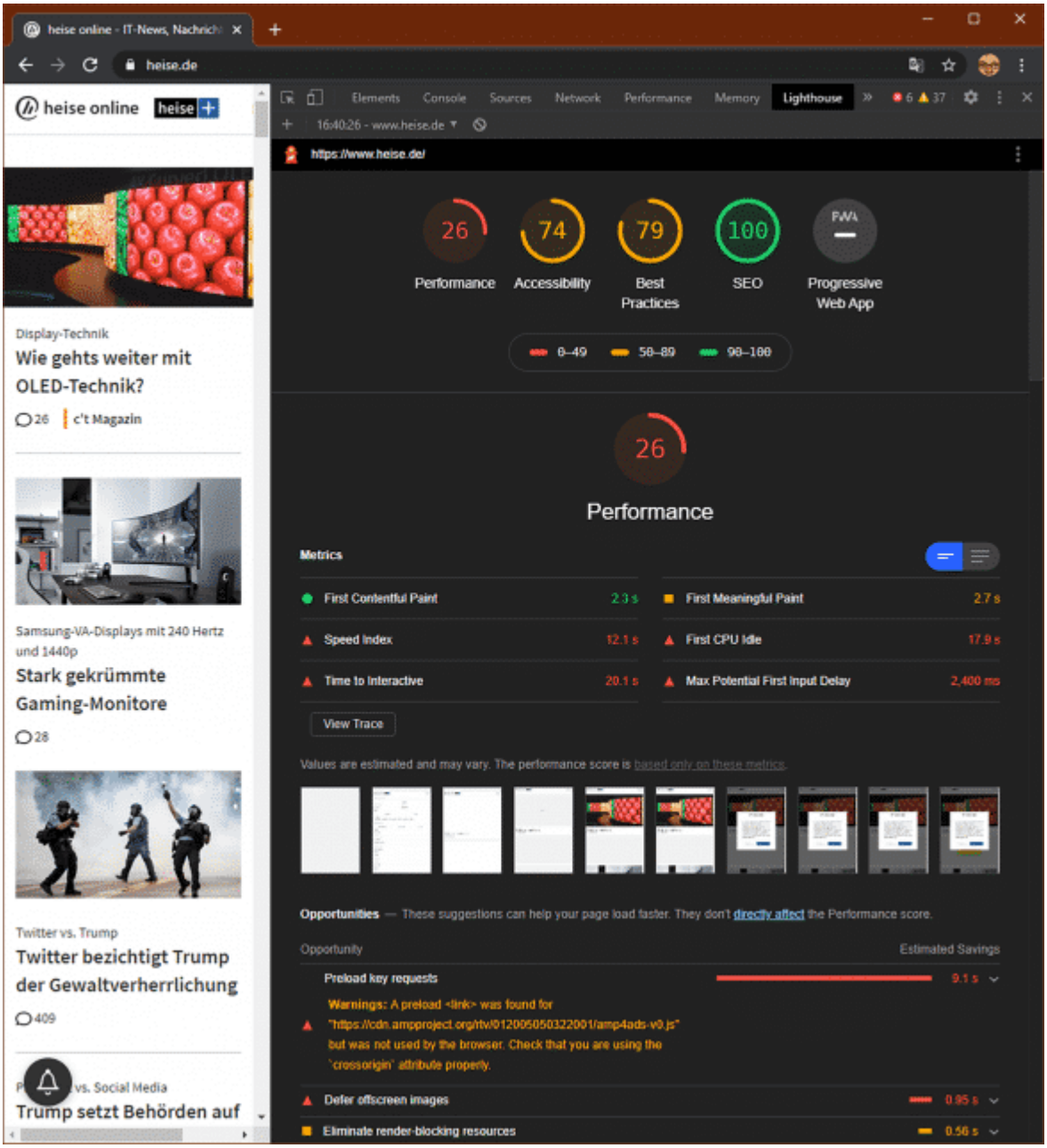
Es gibt viele sehr unterschiedliche Maßnahmen, die Sie als Website-Betreiber umsetzen können, um ihre Seiten flotter zu machen. Dieser Artikel beschreibt Optimierungen für das Frontend. Er gibt einen Überblick über das Spektrum der Möglichkeiten und geht nur vereinzelt in die Tiefe; die Umsetzung im Detail hängt ohnehin stark von den Anforderungen und Problemen der jeweiligen Website ab.

Level 0: Testwerkzeuge

Zunächst gilt es herauszufinden, wo es klemmt. Heute benutzt man für Tests und Tipps meist Google PageSpeed Insights (PSI), Webpagetest.org oder Lighthouse. PSI ist vergleichsweise übersichtlich und eignet sich gut für Einsteiger. Das Open-

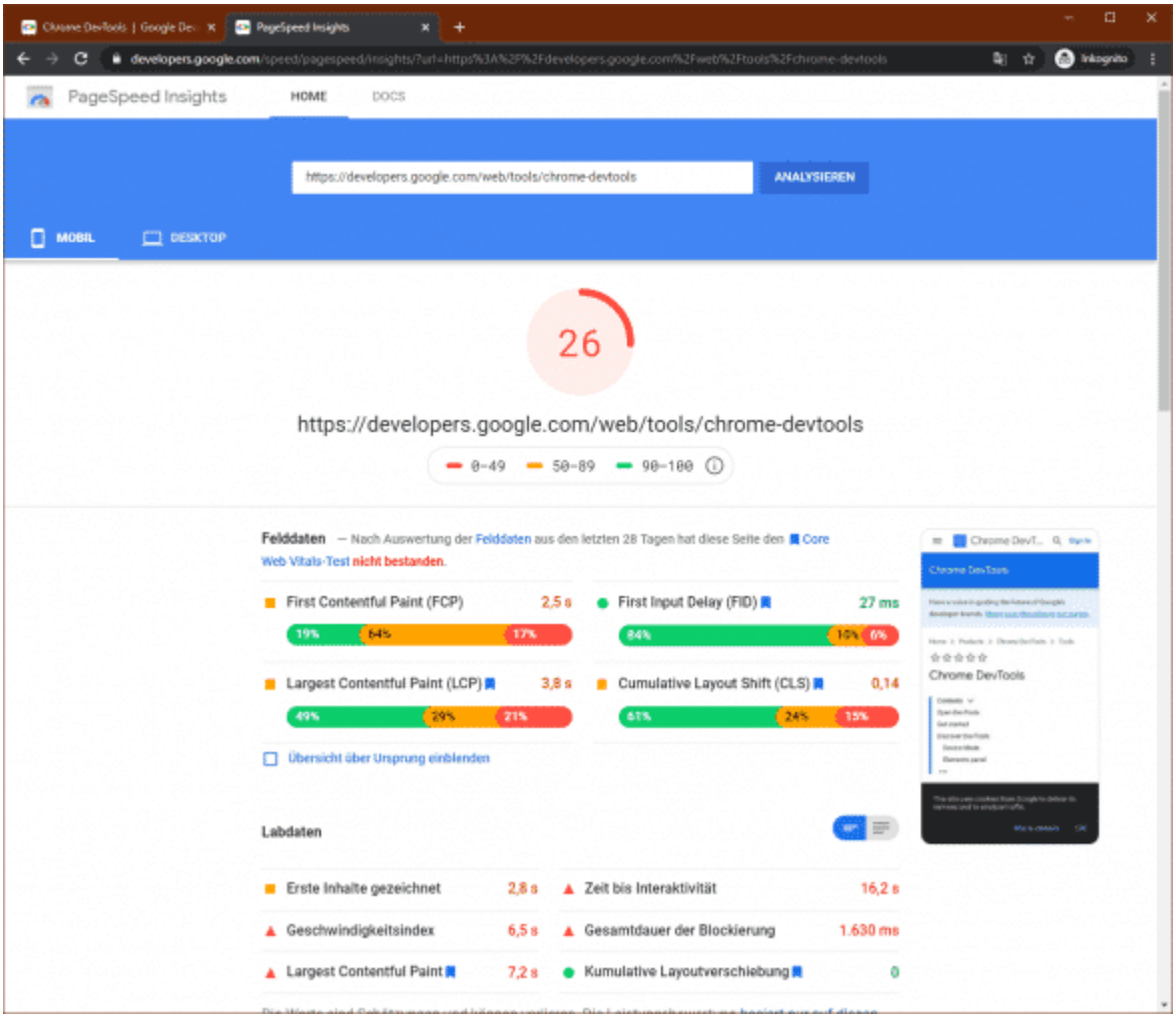
Source-Projekt Webpagetest.org legt den Fokus mehr auf die Aufbereitung der Rohdaten als auf klare Handlungsanweisungen.

Lighthouse – ebenfalls Open Source – stammt wie PSI von Google, testet aber nicht nur die Performance einer Website, sondern etwa auch SEO und Barrierefreiheit; es steckt hinter den Analysefunktionen von PSI, wertet aber anders aus. Lighthouse ist kein Webdienst: Sie finden es in den Chrome-Entwicklerwerkzeugen, können es aber auch als Node.js-Anwendung installieren.



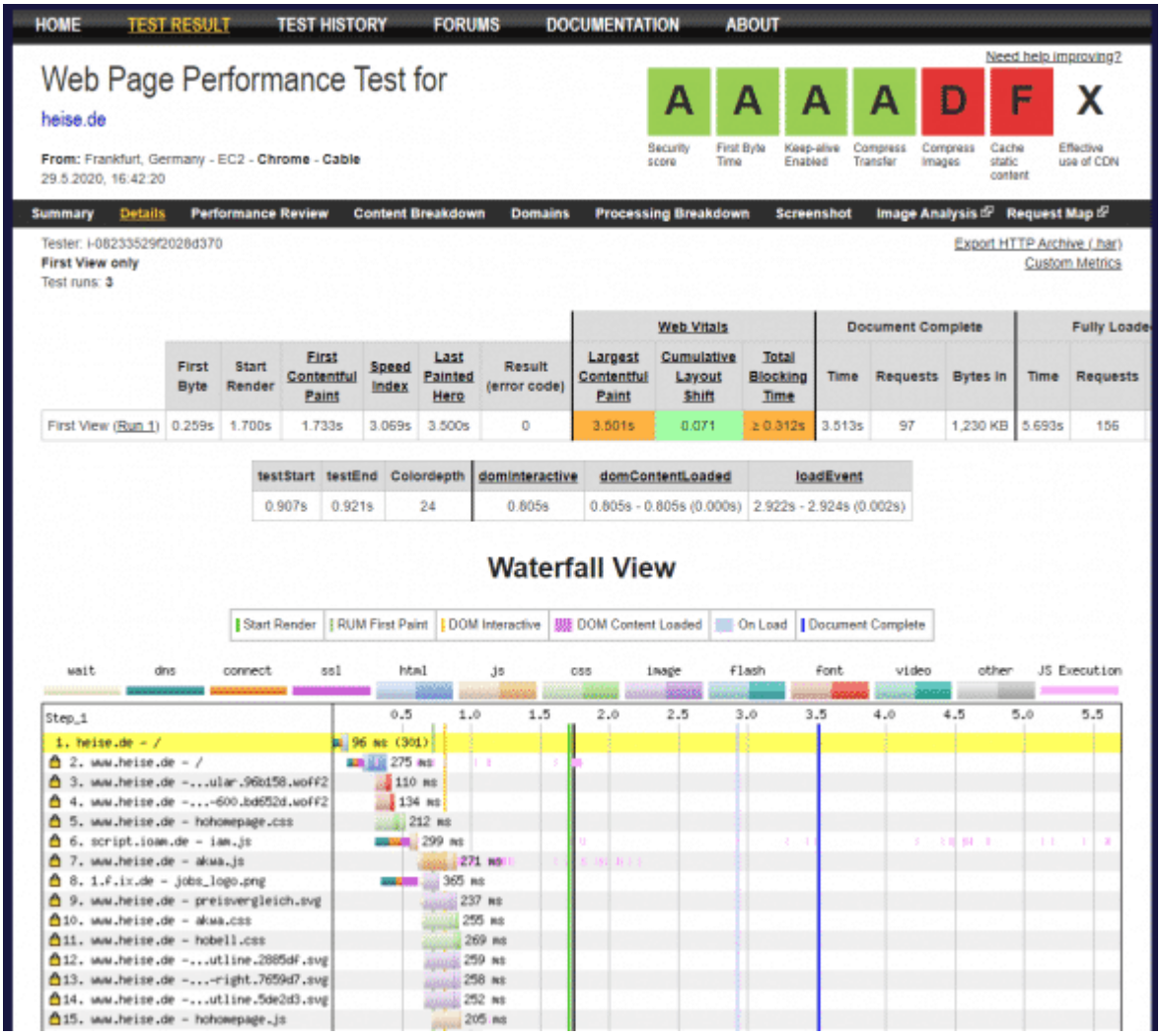
Lighthouse zeigt hübsch gestaltete Messergebnisse und wartet mit konkreten Verbesserungshinweisen auf.

Die Messergebnisse geben Anhaltspunkte, doch sollten Sie sie nicht überbewerten: Sie hängen oft von Zufällen ab und weichen zum Beispiel zwischen Lighthouse und PSI ab. Selbst bei Google-eigenen Seiten fällt der Geschwindigkeitsindex mitunter schlecht aus. Nützlicher sind die Ratschläge („Nicht genutztes JavaScript entfernen“, „Bilder richtig dimensionieren“ etc.), verbunden mit konkreten Angaben zu den betroffenen Dateien und Zeilen.



Googles PageSpeed Insights verwendet eine ähnliche Technik wie Lighthouse, kommt aber zu anderen Ergebnissen.

Unabhängig von Lighthouse finden Sie in den Entwicklerwerkzeugen der gängigen Browser Werkzeuge zum Messen von Netzwerkzugriffen, zur Rendering-Performance und zum Ressourcenverbrauch. Diese zeichnen nach der Aktivierung große Mengen an Daten auf, die Sie anschließend studieren können, um Performance-Engpässe auszumachen. Allerdings sind sie für Website-Tuning-Einsteiger kaum geeignet.



Webpagetest.org ist eine Alternative zu Googles Performance-Werkzeugen.

Level 1: Abspecken

Browser-Entwicklerwerkzeuge erlauben es, den Datendurchsatz zu drosseln, beispielsweise, um die Nutzung im Mobilfunk nachzustellen. Wer das einmal ausprobiert hat, wird sich mit mehr Engagement dem Entrümpeln und Komprimieren der Website widmen.

Das größte Einsparpotenzial haben meist die Bilder – keine andere Maßnahme wirkt so schnell wie deren Optimierung. Klar, dass ein Bild nicht größer sein sollte als das Maximum der Anzeigebreite. Was die Sache kompliziert macht, sind „Retina“-Displays, die Bilder höher auflösen können. Ein iPhone etwa stellt in der Standardskalierung jedes CSS-Pixel mit 2 × 2 Gerätepixeln dar; eine 500 × 300 Pixel große Bilddatei wird in

einem entsprechend großen CSS-Container okay aussehen, aber das Gerät könnte auf dieser Fläche auch 1000 × 600 Pixel unterbringen – ein Bild sieht so einfach schärfer aus.

Um solche Fälle und unterschiedliche Bildgrößen durch responsives Layout abzufangen, stehen Frontend-Entwicklern CSS-Media-Querys und insbesondere die HTML-Attribute srcset und sizes zur Verfügung. Der Browser ermittelt anhand dieser Angaben, welche Bilddatei am besten passt, und lädt nur diese herunter, zum Beispiel:

```
<img alt="Bild" srcset=
  "standard.jpg 1x, retina.jpg 2x">
```

Eine JPEG-Qualitätsstufe von mehr als 80 oder eine verlustfrei komprimierte PNG-Grafik sind im Web meist Bandbreitenverschwendung. Auch das Entfernen von Metadaten oder effizientere Komprimierung holen etliche KByte heraus. Umsetzen lässt sich so was mit üblicher Bildbearbeitungs- und Betrachtungs-Software oder mit Konsolen-Tools wie jpegtran, jpegoptim oder optipng. Diese Tools verarbeiten große Mengen an Bildern und lassen sich in die Build-Pipeline integrieren. Die folgende Anweisung schrumpft manche Fotos auf ein Zehntel ihrer Dateigröße (Achtung, überschreibt Quelldateien!):

```
jpegoptim -o -m75 --strip-all  --all-progressive *.jpg
```

Bei JPEGs empfiehlt sich das progressive Rendering, bei dem das Bild von Anfang an in voller Größe erscheint und während des Ladens immer detailgenauer wird – das fühlt sich für den Benutzer schneller an. Für Icons kommen heute Vektorgrafiken in Form von SVGs oder Iconfonts zum Einsatz. PNGs sind vor allem bei Transparenzen interessant. Das neue WebP-Format wiegt nur etwa 80 bis 90 Prozent einer gleichwertigen JPEG-Datei, aber Sie brauchen gegebenenfalls ein Fallback für Internet Explorer. Bislang nur in Chrome läuft AVIF, das seine Stärken bei hoher Kompressionsrate ausspielt und GIF-ähnliche Animationen erlaubt.

Für Videos setzen viele Websites auf externe Dienstleister, die beim Streamen die Wiedergabequalität an die Bandbreite anpassen. Wo aber ein <video> oder <audio> zum Einsatz kommt, das eine Mediendatei anfordert, kann die richtige Komprimierung Megabytes an Daten einsparen. Tools wie ffmpeg erledigen diesen Job zuverlässig. Leider gibt es keine Entsprechung zu srcset für gestreamte Medien.

Auch den Website-Code sollten Sie zusammenstauchen. Code-Minifizierungswerkzeuge gibt es für CSS und HTML, aber mehr holen Sie bei JavaScript heraus. Das bekannteste Tool dafür heißt „Uglify“ – sein Output ist für den Menschen kaum leserlich, doch der Maschine ist das egal.

Anstrengender, aber lohnender ist es, unnötigen Code komplett rauszuwerfen. JavaScript-Bibliotheken lassen den Code-Umfang enorm anwachsen. Daher sollte sich der Entwickler bei jedem Third-Party-Skript fragen: Brauche ich das wirklich? Muss ich moments.js einbinden, wenn ich einmal ein Datum umrechne? Lohnt sich das Karussell-Plug-in, benötige ich jQuery, weil $(...) so schön kurz ist?

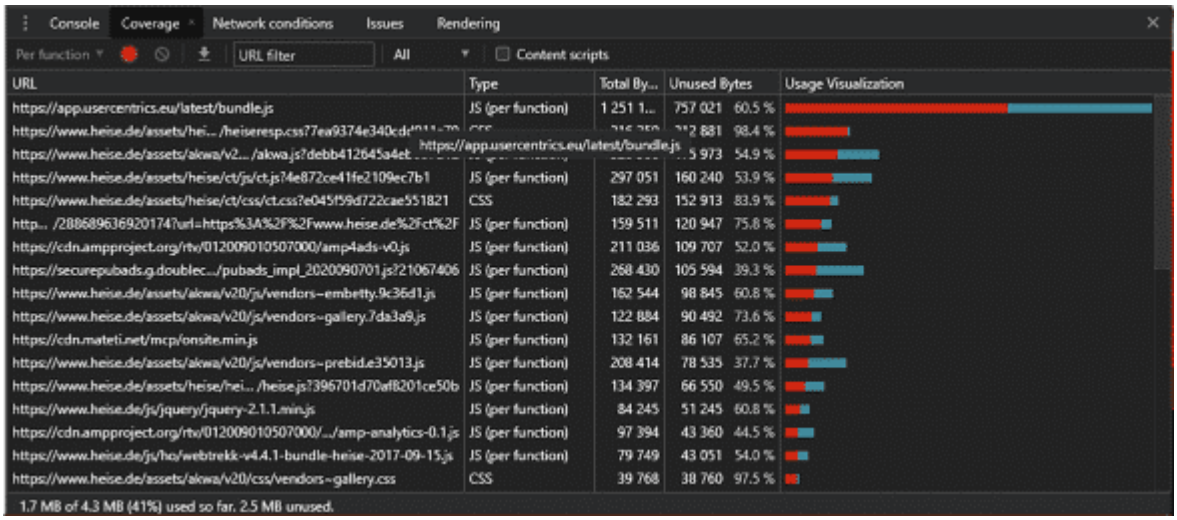
Nicht zu vergessen: Der Browser ist nach dem Download nicht fertig, sondern muss den Code auch noch verarbeiten. Während das etwa bei Bildern eine Frage von Millisekunden ist, leistet er bei JavaScript Schwerarbeit, die den Haupt-Thread oft sekundenlang blockiert. Auf einem leistungsschwachen Gerät kann das Kompilieren und Ausführen länger dauern als der Download. Tests mit realer Hardware bei unterschiedlicher Netzqualität fördern dabei mitunter Überraschendes zu Tage, sind aber aufwendig.

In gewachsenen Projekten findet sich oft erstaunliches Code-Gerümpel wie unterschiedliche jQuery-Versionen oder Polyfills, die seit Jahren keiner mehr braucht. Aber testen Sie die Seite gründlich und schmeißen Sie Code nicht vorschnell raus! Eine JavaScript-Exception stoppt nämlich die weitere Code-Ausführung, und wenn nichts mehr geht, nützt die schönste

Performance-Optimierung nichts mehr.

Chrome hat einen „Coverage“-Reiter (unter „More Tools“), der nicht benutzte CSS-Selektoren und JavaScript-Funktionen rot markiert. Bei den meisten Webseiten liegt deren Anteil bei weit über 50 Prozent. Das Node.js-Werkzeug UnCSS gibt das tatsächlich benutzte CSS aus – auch übergreifend für mehrere Seiten und Bildschirmgrößen.

Beim Import von Modulen ist es oft möglich, sich auf einzelne Komponenten zu beschränken. Moderne Bundler wie webpack oder Rollup beherrschen dieses „Tree-Shaking“ und kopieren mit `import {func1} from 'bigFile.js'` nur den zu func1 gehörenden Code ins Projekt statt der gesamten Skriptdatei.



Wie Chromes „Coverage“-Werkzeug zeigt, braucht man viele eingebundene Skripte und Stile nicht auf der aktuellen Seite.

Level 2: Ausliefern

Trotz Detailverbesserungen hat das Netzwerkprotokoll HTTP seine Wurzeln in den frühen 90er-Jahren, und TCP, auf dem es aufsetzt, ist noch älter. Beide erledigen den Job solide, aber ein bisschen umständlich – für heute übliche Szenarien mit oft mehr als hundert Requests pro Seitenaufruf waren sie jedenfalls nicht gedacht.

Der Overhead, den beide Protokolle verursachen, macht besonders die Übertragung kleiner Dateien teuer. Deshalb gilt

es als Performance-Optimierung, kleine Datenpäckchen zu größeren zusammenzufassen – etwa durch das Bündeln mehrerer Skript- und Stylesheet-Dateien („Bundling“) oder durch Tricks wie CSS-Sprites, bei denen man alle Icon-Grafiken in ein Bild stopft, um mithilfe von CSS das passende herauszufischen.

Außerdem beschränken Browser gemäß der HTTP-Spezifikation die Zahl der gleichzeitigen Verbindungen zu einem Host; typischerweise erlauben sie sechs gleichzeitige Downloads. Um das zu umgehen, setzen manche Websites „Domain-Sharding“ ein – die Aufteilung der Ressourcen auf mehrere Subdomains.

HTTP/2 macht solche Hacks überflüssig. Es benötigt nur eine TCP-Verbindung, um beliebig viele HTTP-Antworten zu liefern – auch solche, die der Client noch gar nicht angefragt hat (Server-Push). HTTP/2 ist inzwischen ein etablierter Standard, der laut W3Techs in 45 Prozent aller Websites zum Einsatz kommt [1].

Tatsächlich findet man das Protokoll bei internationalen Websites wie Google, Facebook, Amazon, eBay, LinkedIn beziehungsweise bei deren Content Delivery Networks (CDN), die diese Technik allesamt beherrschen. Auch manche Shared--Hosting-Angebote von der Stange liefern mit HTTP/2 aus, während andere Hoster den Umstieg bisher gescheut haben. - Wunderdinge sollte man von HTTP/2 allerdings nicht erwarten.

Der schnellste Download ist natürlich der, der nicht stattfindet. Geschicktes Caching kann wiederholte Seitenaufrufe enorm beschleunigen und sogar dafür sorgen, dass der Besucher etwas sieht, wenn er offline ist. Dafür setzt man die HTTP-Header Cache-Control oder Expires ein. Bei heise online zum Beispiel darf der Browser ein Bild für einen Monat im Cache behalten, während das Stylesheet nur zwei Stunden gültig bleibt; die Startseite muss er dagegen schon nach 30 Sekunden neu anfordern. Ist zusätzlich ein ETag-Header gesetzt, können Browser und Server abgleichen, ob sie beide die gleiche Dateiversion haben; in diesem Fall antwortet der

Server mit einem 304-Code, ohne Daten zu übertragen.

Einen Schritt weiter geht der Frontend-seitig programmierbare Cache, der mit Progressive Web Apps (PWA) möglich ist. Hauptzweck ist es, Websites auf Mobilgeräten offline verfügbar zu machen, aber Performance-Optimierung für den Desktop-Browser funktioniert damit ebenso gut. Doch egal, ob PWA oder Cache-Control: Übertreiben Sie nicht, sonst sieht der Besucher zu lange eine veraltete Version der Website!

Level 3: Vor- und Nachliefern

Wenn Sie die Größe des Downloads verringert haben, können Sie darüber nachdenken, wann Sie bestimmte Ressourcen benötigen. Das Standardverhalten – eine HTML-Datei saugt beim Laden sämtliche dazugehörigen Skripte, Stile und Bilder aus dem Netz – ist meistens nicht das schnellste: Manches fordert man besser vorher schon an, anderes erst später.

Aber was heißt eigentlich „Schnelligkeit“ bei einer Webseite? Man kann die Zeit messen, die vom ersten Request bis zum Eintreffen des letzten Bits vergeht, aber das ist nicht unbedingt die relevante Größe. Den Nutzer interessieren eher drei andere Ereignisse: dass irgendetwas auf dem Bildschirm erscheint, dass er im Browser-Viewport ein halbwegs fertiges Layout sieht und dass er mit dieser Ansicht interagieren kann.

Diese Ereignisse sind der „First Contentful Paint“ (FCP), der „Largest Content Paint“ (LCP) oder der „First Meaningful Paint“ (FMP) – sowie die „Time to Interactive“ (TTI).

Wenn also das Laden einer Seite fünf Sekunden dauert, sollte der Benutzer bis zu diesem Zeitpunkt nicht auf einen weißen Bildschirm starren müssen. Idealerweise sieht er innerhalb einer Sekunde relevante Inhalte, die sich anschließend nur noch wenig verändern, und kann die Seite bereits bedienen, während der Browser noch unterhalb des Fensterausschnitts liegende Bilder, Videos und Interaktionen nachlädt.

Meistens stellen Bilder den größten Datenanteil, und so hat sich Lazy Loading etabliert – der Browser fordert die Bilder erst an, wenn er Zeit hat oder sie benötigt. Moderne Browser (mit Ausnahme von Safari) brauchen dafür kein JavaScript mehr: Ein loading="lazy" im <img> genügt. Auch für IFrames funktioniert dies.

Problematisch sind vor allem die Inhalte, die das initiale Rendern blockieren: im Head eingebundene JavaScript- und Stylesheet-Dateien. Trifft der Browser auf solche Inhalte, stoppt er den Seitenaufbau, lädt die Datei herunter und parst sie beziehungsweise führt sie aus, bevor er das Rendern fortsetzt.

Die wenigsten Skripte müssen laufen, bevor die Seite gerendert wurde. Oft verschiebt man daher <script>-Elemente ans Ende des <body>. Den gleiche Effekt erzielen Sie, wenn Sie das <script>-Element im Head lassen und mit dem Attribut defer versehen – allerdings startet der Browser den Download früher, was meist wünschenswert ist. Wenn die Reihenfolge der Skripte egal ist, können Sie stattdessen mit dem Attribut async arbeiten.

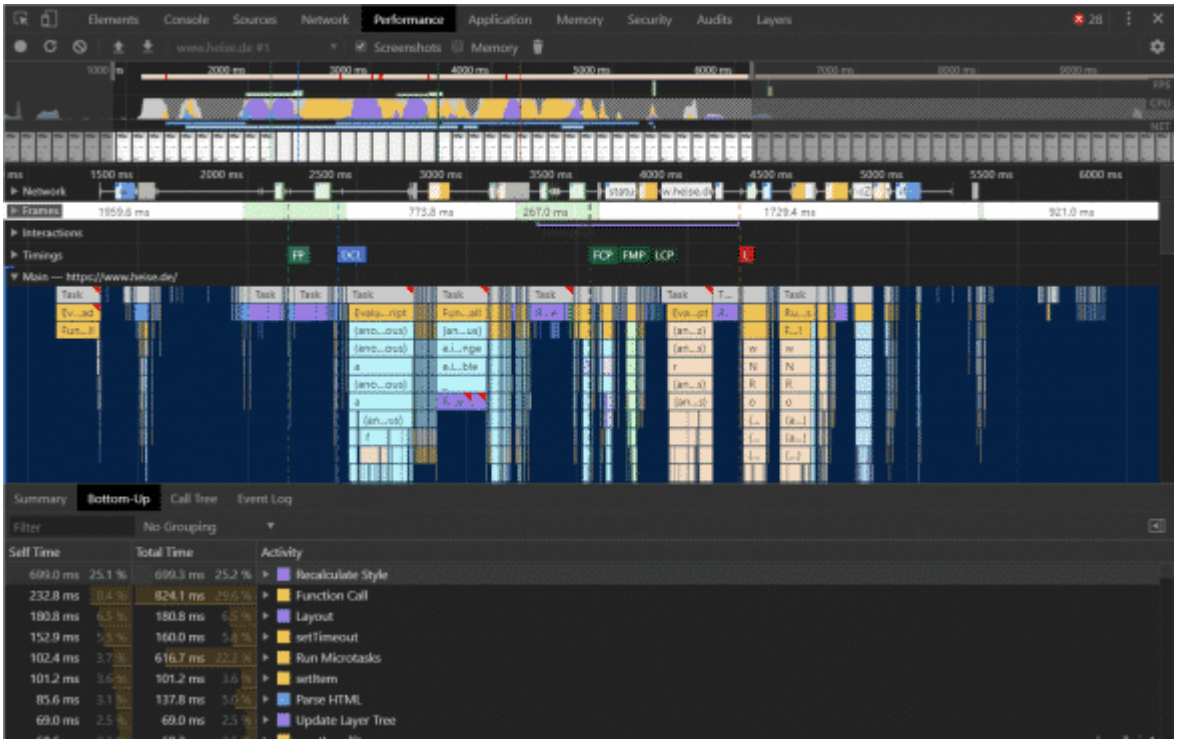
Weniger bekannt ist, dass auch Stylesheets nicht im <head>-Bereich stehen müssen. Sie können beispielsweise das CSS unterhalb des Browserfensters nachladen oder es komponentenweise aufteilen. Wenn Sie Stile für Media-Querys mit <link href="[URL]" rel="stylesheet" media="[Media-Query]"> anfordern, lädt der Browser sie nur herunter, falls er sie braucht. Das Tool Critical extrahiert die sofort benötigten Stile aus dem Stylesheet und fügt sie inline ins HTML-Dokument ein.

Dieses „Code-Splitting“ widerspricht der obigen Forderung nach möglichst großen Datenpaketen. Sie können diesen Widerspruch durch Abwägen und Messen auflösen – oder durch den Umstieg auf HTTP/2. Die technische Seite des Code-Splittings übernehmen gängige Bundler wie webpack, Rollup oder Parcel.js.

HTTP/2-Server-Push ist ein nettes Feature, aber die Frontend-seitigen Möglichkeiten sind flexibler und schicken nicht stumpf Daten durch die Leitung, die der Browser längst im Cache hat. In JavaScript laden Sie mit XMLHttpRequest oder fetch() Dateien, in HTML nutzen Sie das Tag <link href="[URL]" rel="[Typ]">, das besonders differenzierte Optionen bietet.

So spart der Typ dns-prefetch die Zeit für den DNS-Lookup, während preconnect zusätzlich TCP-Verbindung und Verschlüsselung erledigt. preload und prefetch laden eine Datei, allerdings für unterschiedliche Zwecke: prefetch hat niedrige Priorität und eignet sich für noch zu besuchende Seiten, preload dagegen – verpflichtend mit einem as-Attribut, zum Beispiel as="script" – lädt schneller und ist für die aktuelle Seite gedacht. prerender hat den Effekt, als würde man eine Seite im Hintergrund-Tab laden. Aber so mächtig diese Werkzeuge sind: Wie beim PWA-Cache ist Zurückhaltung gegenüber den Ressourcen des Nutzers angezeigt.

Level 4: Code-Feinschliff



Die Performance-Analysewerkzeuge der Browser machen Unmengen von Daten zugänglich, die sich aber erst nach längerer Beschäftigung mit dem Thema erschließen.

Das Laden ist der engste Flaschenhals im Web, deshalb kommt diesem Bereich bei der Performance-Optimierung ein besonderer Stellenwert zu – aber nach dem initialen Laden des HTML und der Render-blockenden Ressourcen muss der Browser binnen Sekundenbruchteilen ein paar Textdateien in Bildschirmpixel verwandeln. Diese Schwerstarbeit heißt „Critical Rendering Path“.

Dahinter verbergen sich mehrere Aufgaben. Der Browser wandelt HTML und CSS in Baumstrukturen (DOM und CSSOM) und führt beide im Rendering-Baum zusammen. Nun wühlt er sich durch alle DOM-Knoten und errechnet für jeden das Layout, also Größe und Position der Inhaltsboxen. In der Paint- oder Raster-Phase füllt der Browser diese Boxen mit Pixeln und ermittelt schließlich in der Compositing-Phase die Anordnung.

Eine offensichtliche Performance-Optimierung ist also, den Arbeitsaufwand überschaubar zu halten, indem man die Zahl der DOM-Knoten drosselt; Lighthouse meckert bei 1500 Elementen.

Der Umfang des CSS ist (abgesehen vom Laden) weniger problematisch, da sich dieses simple Format sehr effektiv verarbeiten lässt. Auch zusammengesetzte CSS-Selektoren (wie nav li:first-child a) ändern daran nichts: Zwar hält sich hartnäckig die Legende, dass diese die Performance beeinträchtigen, aber die Effekte bewegen sich knapp an der Messbarkeitsgrenze.

Eine spürbare Bremswirkung hingegen haben „Reflows“ in umfangreichen Dokumenten – so nennt man es, wenn bereits gerenderte Elemente erneut die Phasen Layout, Paint und Compositing durchlaufen müssen.

In der Praxis passiert dies oft durch nachgeladene Inhalte, zum Beispiel Bilder ohne vorher bekannte Dimensionen oder Webfonts, die nach dem initialen Rendern zur Verfügung stehen. Die dadurch ausgelösten Größenänderungen können eine ganze Kaskade von Reflows hinter sich herziehen. Auch CSS-

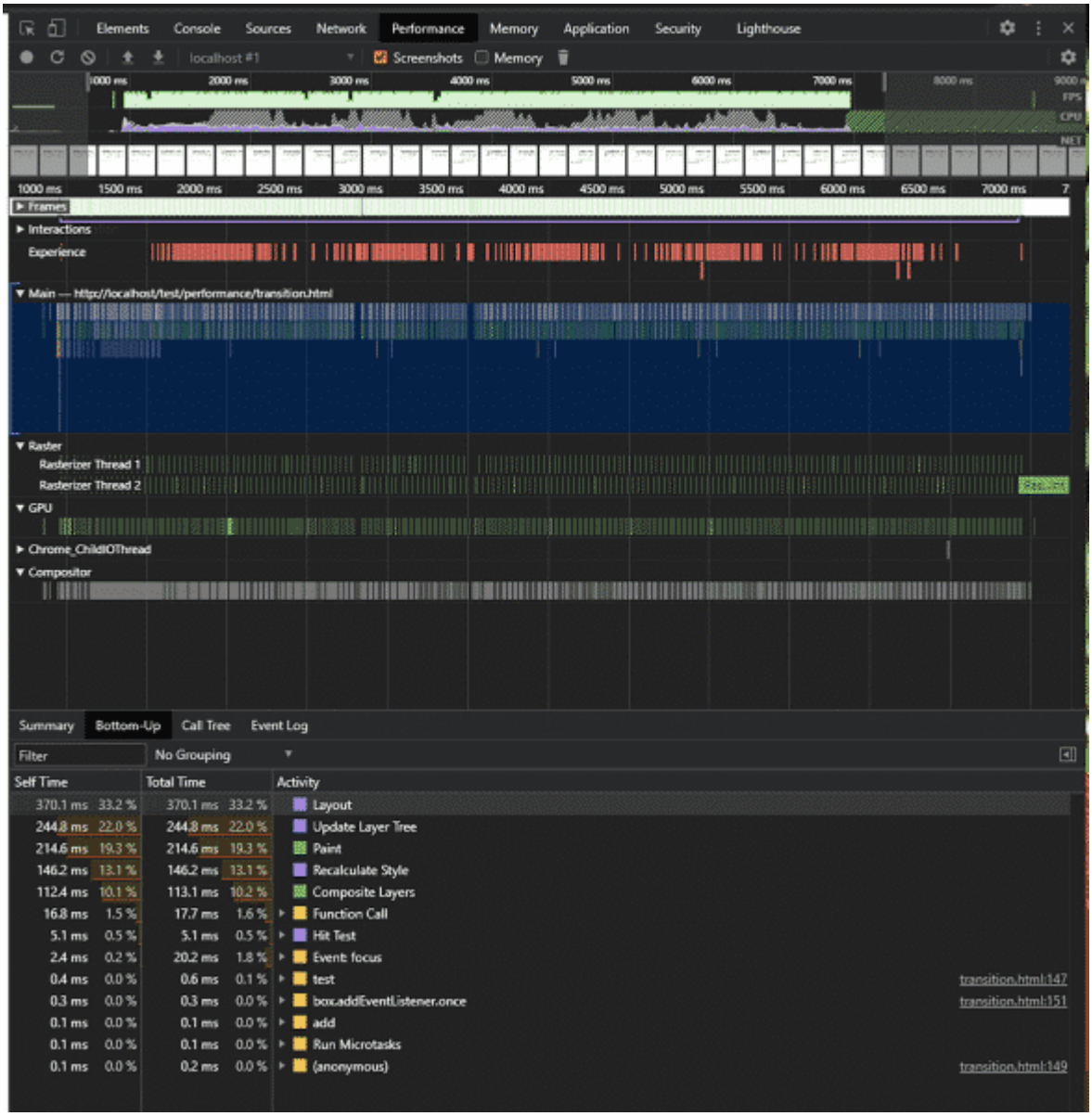
Animationen und -Übergänge sowie JavaScript-Aktionen können das verursachen.

Je nach Art der Änderung und Intelligenz des Browsers muss es nicht immer ein komplettes „Reflow“ sein. Um etwa ein Element animiert zu vergrößern und zu verschieben, bieten sich die CSS-Eigenschaften top, left, width und height an. Wo es möglich ist, sollten Sie dafür jedoch die transform-Eigenschaft mit den Funktionen translate() und scale() verwenden. Die meisten Browser überspringen dann Layout und Paint und gehen gleich zur Compositing-Phase über: Der Grafikprozessor manipuliert die Pixel des schon gerenderten Elements binnen Millisekunden.

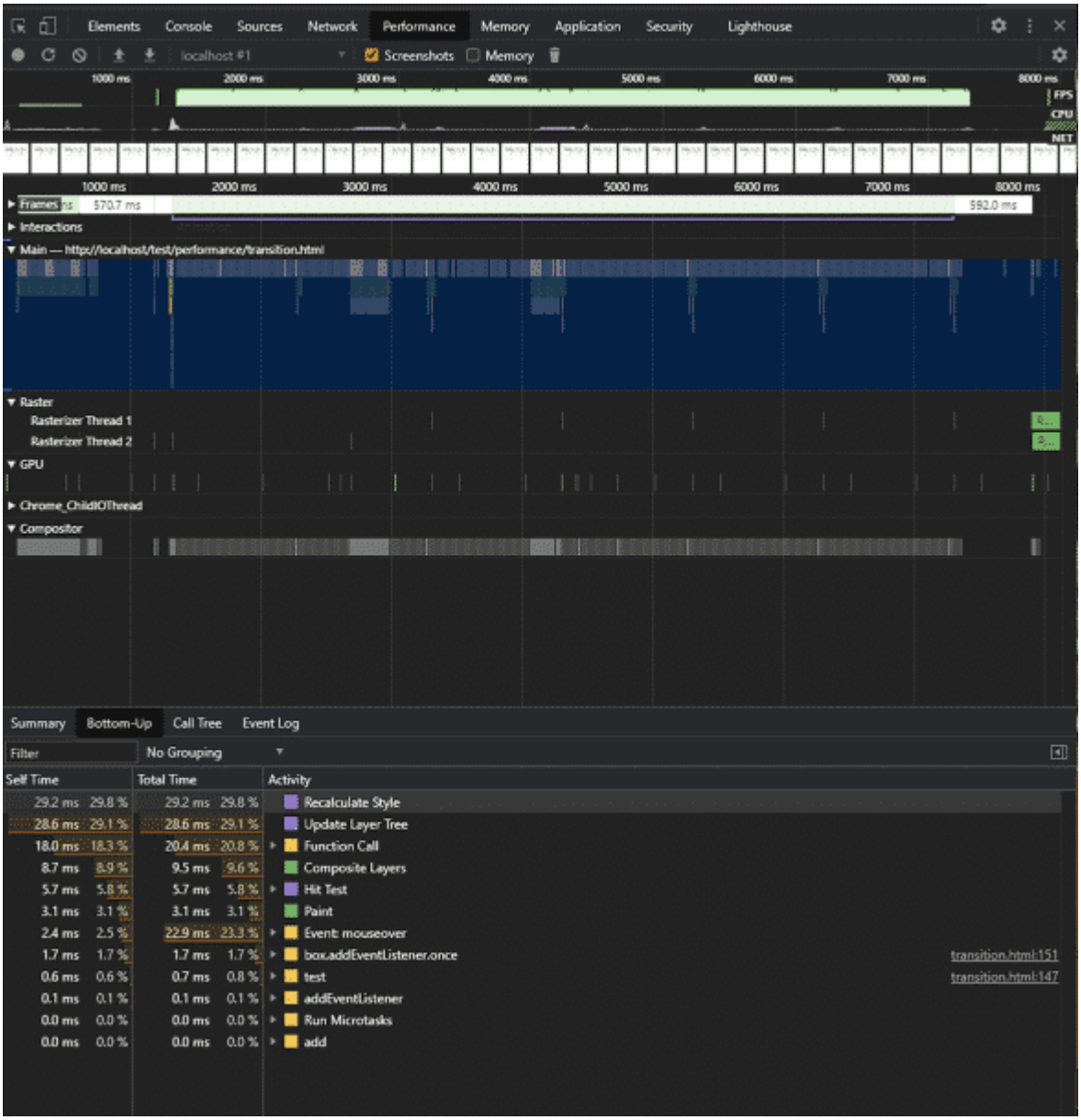
Selbst auf Mobilgeräten laufen derartige Animationen in der Regel flüssig. Wenn Sie Ihren Augen nicht trauen, können Sie die Framerate mit den Entwicklerwerkzeugen messen – in Chrome geht das mit der Kommandopalette (Strg+Umschalt+P) unter „Show frames per second meter“. Maximal erreichbar sind 60 fps.

JavaScript-Code läuft in einem einzelnen Thread. Daher kann eine langwierige Aktion den ganzen Browser zum Stehen bringen. Die Lösung für dieses Problem sind asynchrone Funktionen, was JavaScript in Form von Callbacks, Promises und async/await-Funktionen erlaubt.

Um die Vermeidung unnötiger Wartezeiten geht es auch bei passiven Event-Handlern, die für Scroll- und Touch-Events wichtig sind. Da das Scrolling in einem separaten Thread passiert, kann es auch während aufwendiger Berechnungen flüssig laufen – müsste der Browser nicht vorher prüfen, ob der Code nicht mit preventDefault() das Scrollen stoppt. Mit der Option {passive: true} in addEventListener() verspricht der Entwickler, genau das nicht zu tun.



Eine CSS-Transition, die angrenzenden Text zur Seite schiebt, zwingt den Browser zu harter Arbeit, …



… während ihn eine ähnliche Transition mit Transform-Eigenschaften keine Mühe kostet.
WebWorker können aufwendige Berechnungen in separate Threads auslagern. Das lässt sich gut mit WebAssembly kombinieren, eine auf Performance getrimmte Untermenge von JavaScript, die aus Sprachen wie C++ transpiliert wird. Und schließlich bringt WebGL die Grafikausgabe direkt auf die GPU.

Allerdings braucht man diesen Performance-Turbo außer für Spieleentwicklung nur selten, und für typische Webseiten-Aufgaben nützt er auch nicht viel – denn meistens sind Skripte auf einer Webseite mit DOM-Manipulationen beschäftigt, die mit WebWorkern, WebAssembly und WebGL nicht möglich sind.

Bei DOM-Zugriffen kann es erstaunliche Performance-

Unterschiede geben. Der wohl gängigste Weg, ins Dokument zu schreiben, ist, über die Eigenschaft innerHTML HTML-Quelltext einzufügen:

```
someData.forEach(data => {
  document.querySelector('.my-list').
  innerHTML += `<li>${data}</li>`;
});
```

Umständlicher sind die altmodischen DOM-Methoden wie document.createElement() und appendChild():

```
const list = document.
  querySelector('.my-list');
for (let i = 0;
       i < someData.length; i++) {
  const li = document.
    createElement('li');
  li.textNode = someData[i];
  list.appendChild(li);
}
```

Der Code cacht das Listenelement und hängt neue Elemente erst ins DOM ein, wenn Attribute und Inhalte vollständig sind. Die klassische for-Schleife ist minimal schneller als Array-Methoden wie forEach(). Während Letzteres jedoch wie auch das Caching nur minimale Verbesserungen bringt, beschleunigen die DOM-Methoden das Skript massiv – bei großen Listen bis um das Tausendfache.

Aber wie relevant ist das in der Praxis? „Voreilige Optimierung ist die Wurzel allen Übels“, schrieb Programmiergott Donald Knuth. Tatsächlich wird kaum ein Programmierprojekt am Performance-Unterschied zwischen for und forEach() leiden, während Wartbarkeit und Lesbarkeit vitale Bedeutung haben. Wenn Sie fünf Listenpunkte einfügen, ist es egal, welche Variante Sie wählen. Andererseits häufen sich viele kleine Performance-Sünden an, und das Bewusstsein für -effizienten Code kann entscheiden, ob eine Anwendung benutzbar ist oder nicht.

Gut studieren lässt sich dieser Effekt anhand bekannter Algorithmen, etwa für die Berechnung von Fibonacci-Zahlen – eine Reihe von Zahlen, die aus der Summe der vorherigen zwei gebildet werden (0, 1, 1, 2, 3, 5, 8, …). So könnte man die ersten n Fibonacci-Zahlen wie folgt berechnen:

```
const fib = n => n < 2?
  n : fib(n - 1) + fib(n - 2);
```

Der Algorithmus ruft sich rekursiv selbst auf, um bis zu den ersten Zahlen der Reihe zurückzugehen, die er dann addiert. Simpel, elegant – und extrem ineffizient; irgendwo bei n = 60 wird sich der Browser verabschieden. Der Rechenaufwand steigt mit jeder Iteration exponentiell an, während schlauere Algorithmen das Ergebnis in Sekundenbruchteilen liefern.

Rekursionen und verschachtelte Schleifen können die stärksten CPUs in die Knie zwingen. Wer öfter an komplexen Skripten arbeitet, sollte sich mit der O-Notation („Big O“) vertraut machen, die den Blick für solche Performance-Fallen schärft.

Fazit

Heutige Webanwendungen neigen zum Übergewicht. Aus Frameworks und Bibliotheken kommen Megabytes an oft ungenutztem Code, native Webtechniken wie Buttons, Eingabefelder oder Scrolling werden mit JavaScript nachgebaut. Kann man alles machen, solange die Seite schnell lädt und ruckelfrei läuft – nicht nur auf dem gut ausgerüsteten Entwickler-Laptop, sondern auch auf dem drei Jahre alten Billig-Handy.

Oft sind die naheliegenden Maßnahmen besonders effektiv, aber wer mehr rausholen will, muss tiefer einsteigen – und stößt dabei auf immer mehr Feinheiten beim Laden, Kompilieren und Rendern. JavaScript ist Fluch und Segen zugleich: Es trägt häufig zu Performance-Problemen bei. Funktionen wie Lazy Loading oder Service Worker können aber auch für flüssigeres Surfen sorgen. (*jo@ct.de*)

1. Literatur
2. Jan Mahn, Web-Beschleunigung, Das neue Webprotokoll HTTP/2 in der Praxis, c’t 20/2018, S. 162

Weiterführende Informationen: ct.de/yp4b

[/expand]

Fehler bei Hostern gefährden die Sicherheit von DKIM

[expand title=“mehr lesen…“]

Fehler bei Hostern gefährden die Sicherheit von DKIM

Wissen Konfigurationsfehler bei DKIM

Bild: Thorsten Hübner

DKIM-Fail

Fehler bei Hostern gefährden die Sicherheit von DKIM

Online-Kriminelle versenden regelmäßig E-Mails unter falschem Namen, um Nutzer zur Herausgabe von sensiblen Daten zu bewegen. Mit DKIM sind Spam-Filter in der Lage, solche gefälschten Mails zu erkennen. Doch unsere Analysen zeigen, dass einige Webhoster mit Fehlkonfigurationen Spammern und Phishern Tür und Tor öffnen. Von Leo Dessani und Jan Mahn

Eine neue E-Mail vom Chef. Laut Mailprogramm stammt sie auch von seiner Adresse. Offenbar steckt er im Ausland in Schwierigkeiten, hat seine Kreditkarte verloren und braucht

schnell etwas Geld vom Firmenkonto. Was auf den ersten Blick wie eine authentische E-Mail aussieht, kann sich beim zweiten Blick als Phishing-Versuch offenbaren. Ist die gefälschte Mail gut gemacht, kann sie Filter wie SpamAssassin mit einiger Wahrscheinlichkeit umgehen und landet direkt im Posteingang des Nutzers. Aber selbst wenn der Nutzer vorsichtig ist und die E-Mail-Adresse des Absenders beim Öffnen gewissenhaft prüft, ist das keine Garantie, dass die Nachricht auch tatsächlich von dieser Adresse stammt.

Kriminelle verfolgen mit Phishing-Mails ein konkretes Ziel: das Vertrauen der Nutzer zu gewinnen und sie zu animieren, vertrauliche Daten wie Passwörter preiszugeben (Social Engineering). Senden die Täter ihre Phishing-Mails von einer echten E-Mail-Adresse einer Organisation, auf die sie selbst keinen Zugriff haben, gewinnen sie potenziell mehr Vertrauen der Nutzer, denn vielen Anwendern ist nicht bewusst, dass man Absenderadressen leicht fälschen kann. Möglich ist das durch eine konzeptionelle Schwachstelle im SMTP-Protokoll: Einen Mechanismus für die Authentifizierung der Absenderadresse gibt es im Protokoll selbst nicht.

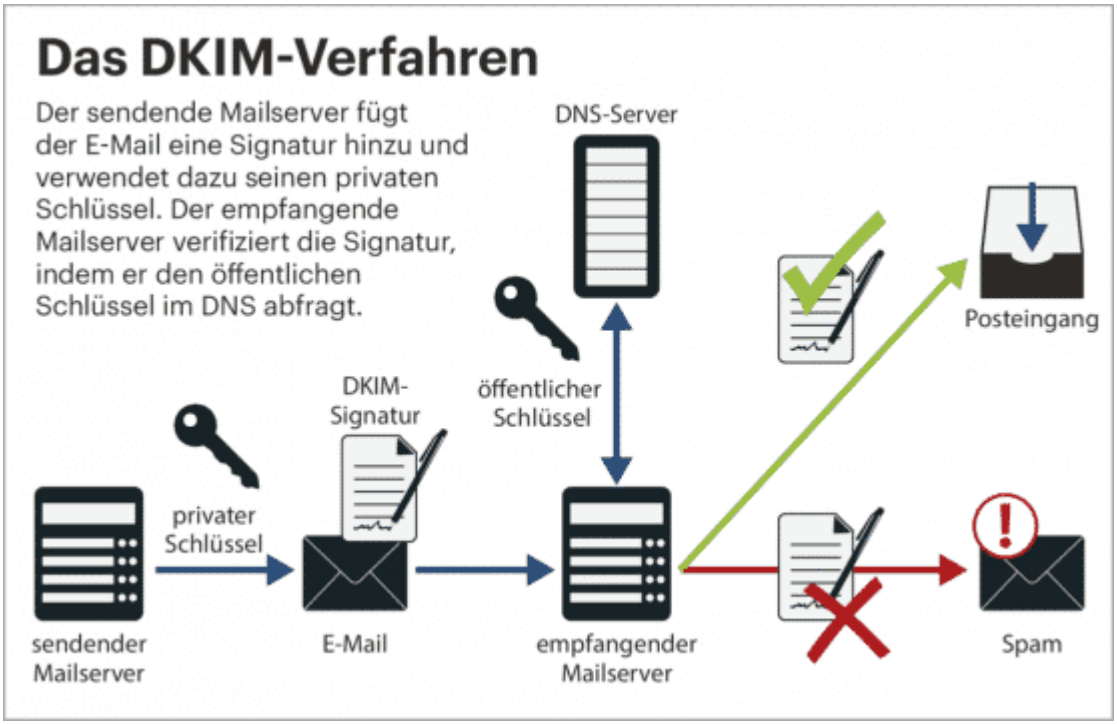
Bereits 2004 haben sich Yahoo und Cisco zusammengeschlossen und gemeinsam einen Standard konzipiert, der das Problem lösen soll: „DomainKeys Identified Mail“ (DKIM). Seit 2011 ist DKIM als Internetstandard von der Internet Engineering Task Force (IETF) anerkannt und wird von vielen Mailserverbetreibern eingesetzt. Das Fälschen von Absenderadressen (Mail-Spoofing) soll dadurch erschwert werden, dass jeder ausgehenden E-Mail eine digitale Signatur als Mail-Header beigefügt wird. Die Signatur im Header kann vom empfangenden Mailserver validiert werden. Mails mit gefälschter Absenderadresse können so erkannt und markiert oder entsorgt werden. Wie DKIM im Detail funktioniert, erfahren Sie im Kasten rechts.

DKIM: Mit Signaturen gegen Betrüger

DKIM ist ein Standard, um die Echtheit der versendenden Domain

einer E-Mail zu prüfen. Anders als zum Beispiel PGP ist für DKIM der Betreiber des Mailservers verantwortlich – als Nutzer kann man das Verfahren nicht einrichten. Ein Serverbetreiber, der DKIM-Signaturen an seine Mails anhängen möchte, generiert ein Schlüsselpaar aus öffentlichem und privatem Schlüssel. Um den öffentlichen Schlüssel bekannt zu machen, kommt DNS zum Einsatz: Den öffentlichen Schlüssel legt der Administrator als TXT-Record in der DNS-Zone seiner Domain ab. Der private Schlüssel darf den Mailserver nicht verlassen.

Beim Versenden von Mails werden zwei Prüfsummen berechnet: eine für ausgewählte Teile des Headers, eine für den Body der Mail. Die Prüfsummen werden mit dem privaten Schlüssel per RSA signiert und als Mailheader DKIM-Signature der E-Mail beigefügt, ergänzt um weitere Informationen. Zu denen zählen unter anderem die Absender-Domain, die Namen aller signierten Header-Felder sowie der sogenannte Selektor. Der Selektor entspricht dem Namen des DNS-Eintrags, in dem der öffentliche Schlüssel liegt. Die Liste der mitsignierten Header-Felder muss mindestens das Feld From: enthalten, also die Absenderadresse, die auch dem Empfänger angezeigt wird. So ist sichergestellt, dass nachträgliche Manipulationen die Signatur ungültig machen.



Empfängt ein Mailserver eine digital signierte E-Mail und ist der Server so eingerichtet, dass er DKIM prüft, fragt er aus dem DNS für die angegebene Domain den öffentlichen Schlüssel mit dem Namen des Selektors ab. Mit dem öffentlichen Schlüssel kann er die Echtheit der digitalen Signatur bestimmen. Ist die Prüfung erfolgreich, ist gewährleistet, dass die E-Mail von einem authentischen Absender stammt und nicht verändert wurde. Schlägt sie fehl, kann das ein Indiz dafür sein, dass die E-Mail gefälscht ist. Was dann passiert, kann der Betreiber des empfangenden Servers bestimmen. Oft führt das Scheitern zur sofortigen Ablehnung der E-Mail, manchmal wird sie nur als Spam-verdächtig markiert. Das Ergebnis der Prüfung fügt der empfangende Mailserver mit dem Header Authentication-Results an die Mail an. dkim=pass zeigt an, dass die Prüfung erfolgreich war, dkim=fail, dass sie fehlschlug.

Fast alle Mailserver verlassen sich nicht auf eine Methode zum Filtern allein und schalten mehrere Filter in Reihe. Mit Inhaltsfiltern reagieren sie zum Beispiel auf typische Spam-Begriffe wie „Casino“ und „Viagra“. In solchen Umgebungen vergibt jeder Filter einen Punktwert für die Einordnung der Mail – überschreitet die Summe aller Punkte einen Schwellwert, wird die Mail aussortiert oder markiert. Eine erfolgreiche DKIM-Prüfung wirkt sich in vielen Konfigurationen positiv auf die Vertrauenswürdigkeit aus und zieht Punkte ab.

Geteilte Server

Seit einigen Jahren bieten immer mehr Webhosting-Anbieter ihren Kunden das Signieren von E-Mails mit DKIM an. Bei einigen Providern ist DKIM sogar standardmäßig für alle Domains aktiviert, bei anderen reicht ein Klick im Kundencenter, um DKIM für einzelne oder alle Domains zu aktivieren. Die Hoster machen es den Kunden leicht und übernehmen das Hantieren mit Schlüsseln und DNS-Einträgen. Ohne Zutun des Kunden erstellen sie ein Schlüsselpaar, legen den öffentlichen Schlüssel im DNS als TXT-Record ab und

richten den privaten Schlüssel auf dem Mailserver ein. Fortan werden alle ausgehenden E-Mails automatisch mithilfe von DKIM signiert.

Bei Webhosting-Paketen sind sogenannte Shared Server verbreitet. Mehrere Kunden teilen sich einen Server, also dessen Ressourcen und Software. Dadurch kann der Anbieter mehr Kunden bedienen, als er tatsächlich physische Server vor Ort hat. Bei solchen Shared Servern muss gewährleistet sein, dass ein Kunde nicht auf die Daten eines anderen zugreifen kann. Für die Webseitendaten und Datenbanken funktioniert das auch sehr zuverlässig.

DMARC: Das Anti-Spam-Trio

Neben DKIM existieren zur Bekämpfung von Spam- und Phishing-Mails zwei weitere Verfahren: Sender Policy Framework (SPF) und Domain-based Message Authentication (DMARC).

SPF beruht auf der Annahme, dass alle E-Mails einer Domain von einer festen Anzahl von autorisierten Mailservern versendet werden. In einem TXT-Record veröffentlicht der Administrator die Adressen dieser Mailserver im DNS. Der Spam-Filter auf dem empfangenden Server kann bei der Entgegennahme der E-Mail durch das Abrufen dieses DNS-Eintrages prüfen, ob der sendende Mailserver zum Verschicken berechtigt ist. Was geschieht, wenn eine E-Mail über einen nicht autorisierten Mailserver versendet wird, kann ebenfalls im DNS-Eintrag festgelegt werden.

DMARC ist keine eigene Technik, sondern kombiniert die Ergebnisse der SPF- und DKIM-Prüfungen: Mit DMARC beschreibt der Administrator, ebenfalls in Form eines DNS-Eintrages, wie der empfangende Mailserver mit einer E-Mail umgehen soll, bei der die SPF- oder DKIM-Prüfungen fehlschlagen, und wen er darüber informieren soll.

Signaturen für fremde Domains

Doch werden auch die privaten DKIM-Schlüssel verschiedener Kunden sauber getrennt? DKIM ist schließlich nur sinnvoll, wenn gewährleistet ist, dass niemand gefälschte Signaturen generieren kann. Was für den Schutz von Kundendaten aufShared Servern gilt, muss auch für Schlüsselpaare gelten: Gültige DKIM-Signaturen auf Grundlage des privaten Schlüssels dürfen ausschließlich für E-Mails generiert werden, die vom Inhaber einer Domain stammen und nicht etwa von anderen Kunden, deren Accounts zufällig auf demselben Server liegen.

Providervergleich

Um herauszufinden, ob Hosting-Anbieter die DKIM-Signaturen ihrer Kunden auf demselben Server sauber trennen, haben wir 37 deutsche Anbieter unter die Lupe genommen und angefragt, ob sie DKIM für ihre Kunden aufShared Servern bereitstellen. Die Antwort: 17 Provider bieten DKIM für ihre Kunden gar nicht an. Vier Provider stellen DKIM nur aufInstanzen bereit, die nicht mit anderen Kunden-Domains geteilt werden (zum Beispiel virtuelle Server oder Managed Server). Übrig blieben 16 Provider für unsere Tests.

DKIM-Konfigurationsfehler bei deutschen Webhostern				
Anbieter	**getestetes Paket**	**DKIM-Unterstützung**	**Ergebnis**	**Reaktion**
All-Inkl.com	Premium	automatisch aktiv	verwundbar	DKIM für die PHP-Mailfunktion deaktiviert
Contabo	Paket L	automatisch aktiv	nicht verwundbar	
creoline	WordPress Hosting S	manuell aktivierbar	verwundbar	Lücke geschlossen
Febas	Professional	manuell aktivierbar	Test nicht möglich[1]	

DKIM-Konfigurationsfehler bei deutschen Webhostern				
Anbieter	**getestetes Paket**	**DKIM-Unterstützung**	**Ergebnis**	**Reaktion**
Hetzner	Level 4	manuell aktivierbar	verwundbar	Lücke geschlossen
hosting.de	Medium	automatisch aktiv	nicht verwundbar	
Hostinger	Premium	manuell aktivierbar	Test nicht möglich[1]	
netclusive	Easy 5.0	manuell aktivierbar	verwundbar	DKIM zunächst deaktiviert, Lücke später geschlossen
netcup	Webhosting 4000	automatisch aktiv	nicht verwundbar	
one.com	Entdecker	automatisch aktiv	nicht verwundbar	
Serverprofis	Private L 5.3	automatisch aktiv	nicht verwundbar	
Strato	Basic	automatisch aktiv	nicht verwundbar	
UD Media	Power 5.0	automatisch aktiv	verwundbar	Lücke geschlossen
webgo	SSD Profi	über den Support aktivierbar	teilweise verwundbar	
webhoster.de	Starter Tarif	manuell aktivierbar	nicht verwundbar	
WebhostOne	Basic	manuell aktivierbar	verwundbar	Lücke geschlossen
[1] keine anderen Kunden mit aktivem DKIM auf demselben Server				

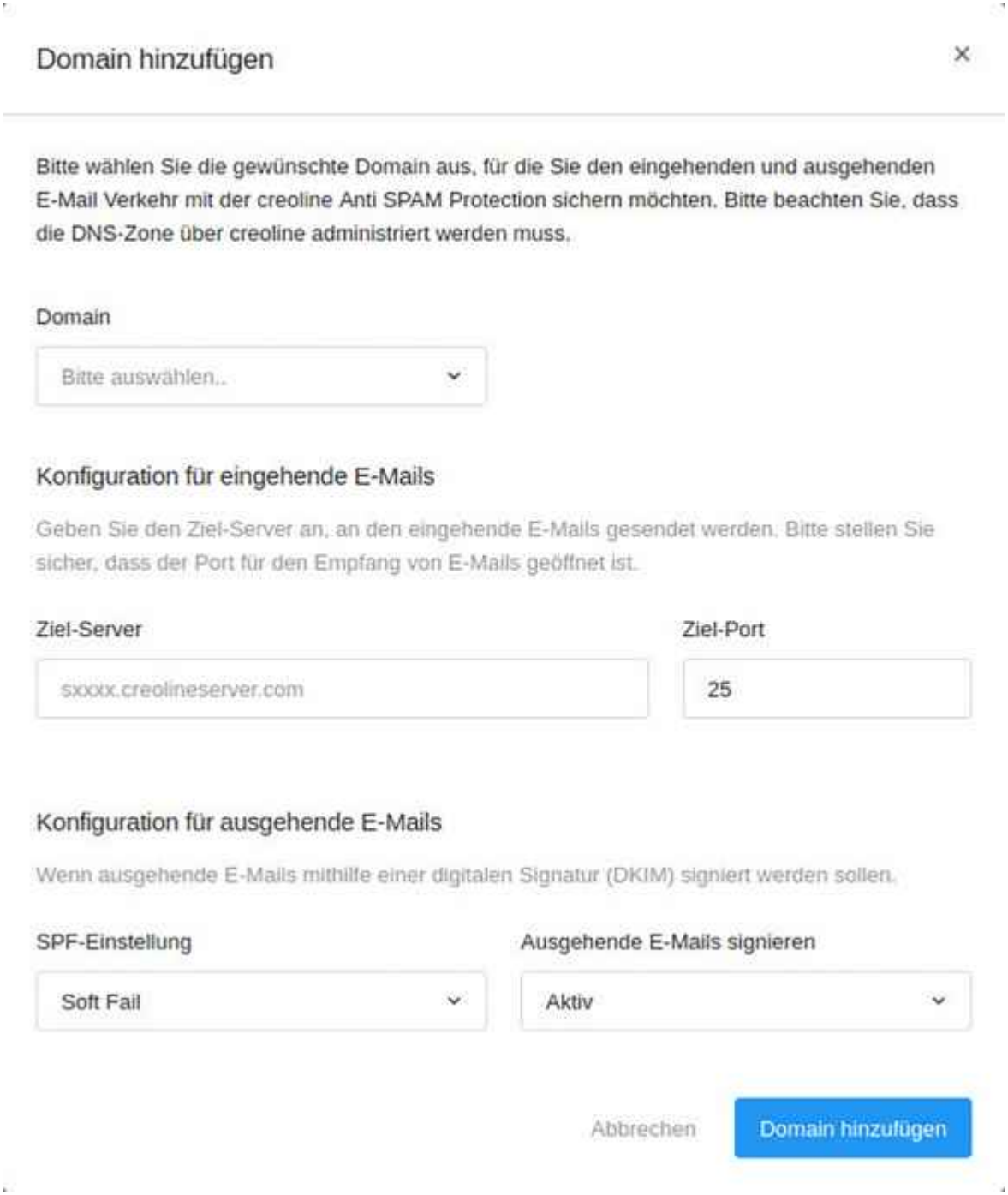
Bei All-Inkl.com, Contabo, hosting.de, netcup, one.com, Serverprofis, Strato und UD Media ist DKIM standardmäßig aktiviert. Bei einigen Anbietern war es notwendig, DKIM im Kundeninterface einzuschalten. Für unseren Test suchten wir den DKIM-Selektor unserer Test-Domains über die DNS-Einstellungen des Kundenportals. Dann gingen wir auf die Suche nach fremden Domains von anderen Kunden, die sich mit uns einen Server teilten. Diese Recherche ist mit einer Reverse--DNS-Suchmaschine im Internet schnell erledigt, indem man nach

der IP der eigenen Domain sucht. Für den Test brauchten wir eine fremde Domain, auf der ebenfalls DKIM aktiv war – ob das der Fall ist, findet man heraus, wenn man deren DNS-Einträge durchsucht. Bei den meisten Anbietern ging das schnell, da die DKIM-Selektoren für alle Domains identisch sind. All-Inkl.com, Hostinger und hosting.de vergeben individuelle DKIM-Selektoren auf Grundlage des Datums, an dem DKIM aktiviert wurde. In diesem Fall war etwas Ausdauer gefragt, da wir die fremden Domains manuell prüfen mussten. Nachdem wir fremde Domains mit aktivierter DKIM-Signatur auf „unseren“ Servern ausfindig gemacht hatten, konnte der Test beginnen.

Hoster ohne DKIM-Unterstützung	
Anbieter	DKIM-Unterstützung
1blu	nicht unterstützt
alfahosting	nicht unterstützt
centron	nicht unterstützt
checkdomain	nicht unterstützt
DM Solutions	nur für Managed Server
dogado	nicht unterstützt
DomainFactory	nicht unterstützt
ESTUGO	nicht unterstützt
goneo	nicht unterstützt
Host Europe	nicht unterstützt
Hostpress	nur für vServer
INWX	nicht unterstützt
IONOS 1&1	nicht unterstützt
manitu	nicht unterstützt
Mittwald	nicht unterstützt
OVH	nicht unterstützt
Packagecloud (D&T Internet)	nicht unterstützt
profihost	nicht unterstützt

Hoster ohne DKIM-Unterstützung	
Anbieter	DKIM-Unterstützung
Raidboxes	nur für vServer
TimmeHosting	nur für vServer
united-domains	nicht unterstützt

In allen getesteten Paketen stand uns PHP zur Verfügung – also nutzten wir die PHP-Funktion mail(), um eine E-Mail mit einer fremden Domain in der Absenderadresse, die auf demselben Server gehostet war wie unsere, an ein externes Postfach zu schicken. Eine glatte Fälschung also, die niemals hätte signiert werden dürfen.



Bei Creoline muss man DKIM im Kundencenter aktivieren. Der Anbieter war beim DKIM-Signaturdiebstahl verwundbar, konnte das Problem nach unserem Hinweis aber abstellen.
Bei sechs von sechzehn getesteten Anbietern war das Experiment erfolgreich: All-Inkl.com, creoline, Hetzner, netclusive, WebhostOne und UD Media hängten eine gültige Signatur mit dem privaten Schlüssel der fremden Domain an, obwohl wir zum Versenden nicht berechtigt waren. Unser empfangender Mailserver stufte die Mail als korrekt DKIM-signiert ein. Bei netclusive betraf dies nur Pakete auf dem Server hst1.ncsrv.de. Neue Pakete auf dem Server hst2.ncsrv.de waren

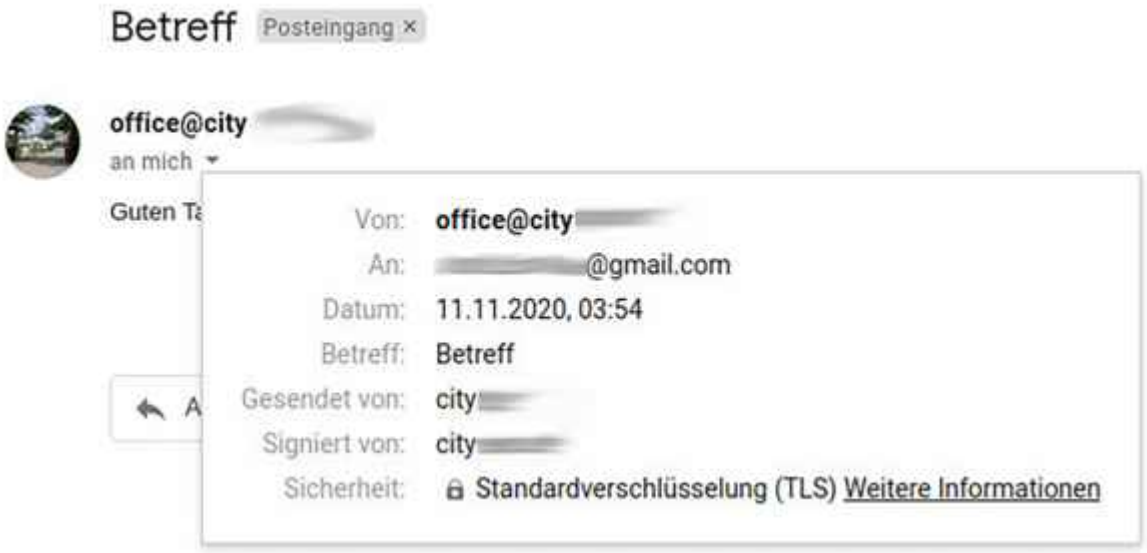
nicht betroffen.

Bei Febas, Hostinger und webgo konnten wir die Recherchen nicht abschließen, weil auf unserem Server keine anderen Domains DKIM aktiviert hatten und somit kein fremdes Schlüsselmaterial zum Testen vorhanden war.

Bei Serverprofis und Strato funktionierte der Angriffsversuch nicht. Beim Versenden aus unserem Account heraus wurde für die fremde Domain entweder eine DKIM-Signatur mit unserem privaten Schlüssel oder gar keine hinzugefügt. Zu einer unbefugt gültigen Signatur kam es nicht. Bei one.com wurden für fremde Adressen gar keine Mails verschickt, ein Angriff war also auch nicht möglich. Bei netcup und hosting.de konnten wir das Problem ebenfalls nicht reproduzieren. Dort werden Mails laut Auskunft des Supports nur dann DKIM-signiert, wenn man sie über den SMTP-Server verschickt und sich bei diesem authentifiziert. Das war hier ein wirkungsvoller Schutz gegen den Angriff.

Vertrauen verspielt

Unsere Untersuchung macht deutlich: Auch wenn das DKIM-Protokoll selbst gut konzipiert ist, haben es einige Webhoster durch fehlerhafte Konfiguration geschwächt. Bei den Anbietern, bei denen wir gefälschte E-Mails versenden konnten, haben wir die Wirksamkeit von DKIM ausgehebelt. Noch mehr: Da wir von einem autorisierten Mailserver verschickten, lieferten auch SPF und damit DMARC keine Fehler. Wir umgingen so auch vergleichsweise streng konfigurierte Spam-Filter und unsere E-Mail landete direkt im Posteingang ohne Spam-Verdacht. Auch sicherheitsbewusste Nutzer, die zum Beispiel mit dem Thunderbird-Plug-in„DKIM Verifier“ arbeiten, das bei jeder Mail das Ergebnis der Signaturprüfung prominent anzeigt, wären auf den Angriff hereingefallen.



Google Mail zeigt an, dass die Mail korrekt signiert wurde. Dabei wurde sie nicht von einem berechtigten Absender verschickt.
Für Spammer und Phisher ist dieser lockere Umgang mit den DKIM-Schlüsseln der Kunden ein großzügiges Angebot, gegen das Betreiber von Maileingangsservern und die Mailempfänger nichts tun können. Abhilfe schaffen können bei dem Problem nur die Hosting-Anbieter.

Nach unseren Experimenten kontaktierten wir die betroffenen Anbieter All-Inkl.com, creoline, Hetzner, netclusive, WebhostOne und UD Media und wiesen auf das Problem hin. Die Hoster, bei denen kein Test möglich war, wiesen wir darauf hin, dass das Problem möglicherweise auch bei ihnen besteht. Webgo bestätigte, dass die Lücke tatsächlich auf einigen Servern existiert – diese ältere Infrastruktur werde in nächster Zeit aktualisiert.

Creoline reagierte schnell mit einer Stellungnahme und wies zunächst darauf hin, dass Versuche, die Absenderadresse zu ändern, spätestens nach fünf Versuchen automatisch unterbunden wurden. Am nächsten Tag hatte man das Problem dann vollständig gelöst und die Manipulation war gar nicht mehr möglich. Netclusive antwortete einen Tag nach dem Hinweis, dass man DKIM vorübergehend ganz abgeschaltet habe, eine Woche später hatte man das Problem dann gelöst und DKIM wieder aktiviert.

Auch bei Hetzner konnte man das Problem bestätigen und stufte es als „mittelschwer“ ein – einen Tag nach der Meldung hatte man den Fehler beseitigt. Weil der Kunde DKIM selbst aktivieren muss, seien nach Angaben von Hetzner nur etwa fünf Prozent der Webhosting-Kunden betroffen gewesen. All-Inkl.com deaktivierte etwa eine Woche nach unserem Hinweis alle DKIM-Signaturen für Mails, die über die PHP-Funktion mail() verschickt wurden.

Private Schlüssel

Bei späteren Untersuchungen bemerkten wir, dass wir teilweise auch per SMTP Mails mit falscher Domain abliefern konnten, die dann signiert wurden – das Problem war bei einigen Anbietern also nicht auf die mail()-Funktion von PHP beschränkt. Die Lücke zeigte wieder ein altbekanntes Problem. DKIM basiert auf asymmetrischer Kryptografie, es gibt also einen öffentlichen und einen privaten Schlüssel. Wirklich sicher sind solche Verfahren nur, wenn der private Schlüssel auch wirklich privat bleibt. Also am besten auf einer Maschine, auf die nur der Inhaber selbst Zugriff hat. Wer DKIM bei einem Shared-Hosting-Dienst nutzt, gewinnt zwar viel Komfort, gibt aber seinen privaten Schlüssel aus der Hand und muss dem Dienstleister vertrauen. (*jam@ct.de*)

[/expand]

PHP 8

[expand title=“mehr lesen…“]

PHP 8 ist da, Version 7.2 ist tot

PHP 8 ist da, Version 7.2 ist tot

Das Entwicklerteam der meistgenutzten Web-Programmiersprache hat PHP 8 veröffentlicht. Gleichzeitig endet der Support für Version 7.2.

Neu in PHP 8 ist vor allem der Just-in-Time-Compiler (JIT), der schnellere Code-Ausführung ohne Änderungen am Code verspricht. Ob er dieses Versprechen in realen Umgebungen halten kann, wird sich erst in den nächsten Monaten zeigen, wenn größere PHP-Anwendungen bereit sind für PHP 8. Wie geplant erscheint die neue Major-Version 8 fast zeitgleich mit dem endgültigen Support-Ende von PHP 7.2. Wer diese Version noch nutzt, muss jetzt handeln, weil es keine Sicherheits-Updates mehr gibt.

Der Wechsel von 7.2 auf 7.3 (Support bis zum Nikolaustag 2021) oder 7.4 (Support bis zum 28.11.2022) verläuft vergleichsweise unspektakulär. Einige alte Konstruktionen werden als „deprecated“ markiert, weil sie in zukünftigen Versionen gestrichen werden sollen – solange man die Deprecation-Warnungen nicht anzeigen lässt, kann man die Seite damit aber problemlos betreiben.

Am besten überführt man seinen Code in eine Testumgebung, aktualisiert dort auf PHP 7.4, lässt sich alle Deprecation--Warnungen (E_DEPRECATED) anzeigen und behebt dann die Probleme – diese Warnungen sind meist recht aussagekräftig. Hinweise zur Problemlösung finden sich im Migrationsleitfaden von PHP (zu finden über ct.de/yc4z). Wer für die nächsten Jahre Ruhe haben möchte, kann es anschließend wagen, die Testumgebung auf PHP 8 umzustellen.

Der Wechsel auf PHP 8 ist durchaus mit Arbeit verbunden. Das liegt vor allem an uralten Zöpfen, die in Version 7 abgekündigt und jetzt endgültig abgeschnitten werden. Die seit

PHP 7 missbilligten Konstruktoren des alten Stils (eine Funktion, die wie die Klasse heißt) werden jetzt nicht mehr erkannt. Stattdessen muss der Konstruktor __construct() heißen (mit zwei Unterstrichen am Anfang). Es hilft nichts: Um das umzustellen, kommt man nicht umhin, sich alle eigenen Klassen nacheinander vorzunehmen. Weil dieses Relikt schon seit PHP 7.0 auf der Abschussliste steht, haben fast alle verbreiteten Open-Source-Bibliotheken die Umstellung bereits erledigt.

Wer ein Framework oder eine fertige Anwendung einsetzt, sollte vor dem Wechseln sicherstellen, dass deren Entwickler grünes Licht für PHP 8 gegeben haben. Die WordPress-Entwickler zum Beispiel wollen mit WordPress 5.6 so weit sein, das im Dezember erscheint; Nextcloud hat noch einige Baustellen vor sich. Die Entwickler des PHP-Frameworks Symfony haben ihre Hausaufgaben schon während der Beta-Phase erledigt. Das Framework kann bereits auf das mit PHP 8 eingeführte Konzept der Attributes zurückgreifen, also Meta-Informationen, die man in einer Kommentarzeile an eine Methode übergibt.

Für viele Serverbetreiber ist ein Wechsel von 7.2 auf eine noch unterstützte 7er-Version oder gar Version 8 aber nicht das dringlichste Problem: Die Statistikseite w3techs.com hat erhoben, dass Ende November 2020 noch immer 41,2 Prozent aller PHP-Websites mit Version 5 (davon rund die Hälfte mit der finalen Ausgabe 5.6) arbeiten. Sicherheits-Updates gab es dafür zuletzt am 1. Januar 2019. (jam@ct.de)

Supportzeiträume von PHP: ct.de/yc4z

[/expand]