Checkliste – E-Mail-Sicherheit

Checkliste: Mails so verschicken, dass man Ihnen vertraut

Damit Ihre Mails nicht aussortiert werden, sollten Sie es dem Empfänger so leicht wie möglich machen. Wenn Sie die folgenden Tipps beherzigen, gelingt das.

Lesezeit: 4 Min.

(Bild: Andreas Martini)

26.08.2022 06:00 Uhr

c’t Magazin

Von

- Ronald Eikenberg

Damit Ihre Mails nicht ungeöffnet als Spam oder Phishing aussortiert werden, sollten Sie es dem Empfänger so leicht wie möglich machen. Wenn Sie folgende Tipps beherzigen, verschicken Sie Mails, die einen guten Eindruck hinterlassen und auch tatsächlich gelesen werden.

Absender, Betreff und Anrede

Der erste Eindruck zählt. Stellen Sie sicher, dass Sie einen aussagekräftigen Absendernamen in Ihrem Mailkonto eingestellt haben, etwa Vorname Nachname (Firma). Geben Sie Ihrer Mail einen sinnvollen, möglichst konkreten Betreff: anstatt „Anfrage“ beispielsweise „Kundenanfrage Ersatzteil XY für Modell Z“.

Beginnen Sie die Mail nach Möglichkeit mit einer individuellen Ansprache mit Person oder Firma, die Sie erreichen möchten. Stellen Sie eine Signatur mit Ihrem Namen, der Firma und Rufnummer für Rückfragen ein. So können die Adressaten Ihre Mails zumindest von plumperen Fälschungen leicht unterscheiden.

Auf Empfänger achten

Überprüfen Sie vor dem Abschicken die Empfängerfelder „An“, „CC“ und „BCC“. Durch die automatische Vervollständigung Ihres Mailclients schleicht sich hier schon mal ein falscher Empfänger ein. Beim Beantworten von Mails sollten Sie in den Feldern gründlich ausmisten. Das gilt insbesondere für Antworten auf Mails, die an einen großen Empfängerkreis gerichtet waren. Denn die Antwort auf die Rundmail des Chefs muss in vielen Fällen nicht erneut die große Runde machen.

Wenn Sie mehrere Empfänger anmailen, die nichts miteinander zu tun haben, sollten Sie die Empfängeradresse unbedingt in das Feld BCC (Blindkopie) eintragen, damit die Empfänger nicht die gesamte Adressliste einsehen können. Wenn Sie „An“ oder „CC“ nutzen, geben Sie die Empfängerliste preis und handeln sich ein Datenschutzproblem ein.

Text statt HTML

HTML-Mails bergen unnötige Risiken: Der Empfänger sieht nicht auf den ersten Blick, auf welche Webadresse ein Link wirklich zeigt und von externen Servern eingebettete Inhalte sind entweder ein Datenschutzrisiko oder werden vom Empfängerclient nicht angezeigt. Verfassen Sie Ihre Mails daher besser im Textformat. Falls Sie auf eine URL verweisen möchten, sollten Sie Linkverkürzer wie TinyURL meiden, damit der Empfänger der Mail auf Anhieb weiß, wohin Sie ihn schicken möchten.

Vorsicht bei Anhängen

Von Mailanhängen geht eine große Gefahr aus. Phisher verschicken insbesondere Office-Dokumente und ausführbare Dateien, um neue Opfer in die Falle zu locken. Verschicken Sie Dokumente deshalb am besten im PDF-Format. Es hat sich als risikoarmes Austauschformat durchgesetzt. Microsoft Office und viele andere Anwendungen können Ihre Dokumente im PDF-Format speichern, zum Beispiel über die Druckfunktion. Falls es doch

mal ein Office-Format sein muss, dann wählen Sie bevorzugt die Formate, die auf X enden: DOCX, PPTX, XLSX. Diese können keine Makros enthalten.

Vermeiden Sie insbesondere ausführbare Dateiformate wie EXE. Dabei handelt es sich häufig um Malware, weshalb Mails mit ausführbaren Anhängen oft aussortiert werden. Kündigen Sie unerwartete und ungewöhnliche Mailanhänge am besten über einen anderen Kommunikationskanal an. Vermeiden Sie große Anhänge, da diese oft nicht ankommen.

Mails signieren

Im besten Fall signieren Sie ausgehende Mails digital vor dem Versand mit OpenPGP oder S/MIME. So hat der Empfänger die Chance, zu verifizieren, dass die Mail tatsächlich von Ihnen stammt. Mailverschlüsselung sollten Sie nur nutzen, wenn Sie sicher sind, dass der Empfänger die Mail tatsächlich entschlüsseln kann. Die Verbindung zum Mailserver sollte in jedem Fall transportverschlüsselt sein (möglichst SSL/TLS), was bei den meisten Mailanbietern inzwischen jedoch Standard ist.

E-Mail-Sicherheit

Gute Mails, böse Mails

Gefahrloser Umgang mit E-

Mails

Gefährliche Mails sollte man nicht öffnen – aber ob eine Mail harmlos ist oder nicht, weiß man oft erst, nachdem man sie geöffnet hat. Und manchmal nicht mal dann. Damit Sie trotzdem nicht in die Phishing-Falle tappen, müssen Sie ein paar Sicherheitsvorkehrungen treffen, die wir Ihnen hier geben.

Von Ronald Eikenberg

EMails zu öffnen ist wie Russisch Roulette – man weiß nie, ob es knallt. Meist hat man keine Wahl, ob man mitspielen möchte. Versuchen Sie doch mal, Ihrem Chef zu erklären, dass Sie ab sofort keine E-Mails mehr öffnen. Schlagkräftige Argument hätten Sie zuhauf: E-Mails sind gefährlich und der wichtigste Verbreitungsweg für Schädlinge. Allein die berüchtigte, hauptsächlich per Phishing-Mail verbreitete Emotet-Malware hat weltweit unzählige Unternehmen, Behörden, Krankenhäuser & Co. lahmgelegt und dabei Schäden in Milliardenhöhe angerichtet.

Ein weiteres Argument ist, dass Sie Ihrem Chef nicht versprechen können, dass Sie alle Phishing-Mails aussortieren und nicht darauf reinfallen. Denn die Zeiten, in denen man solche Mails schon von Weitem erkennen konnte, sind längst vorbei. Angreifer nutzen immer häufiger echte – gestohlene – Daten, um Sie in die Falle zu locken, zum Beispiel plausible Absender, mit denen Sie bereits Kontakt hatten. Phishing-Mails zitieren mitunter sogar aus vorangegangenen Mailwechseln mit Kollegen, Partnerfirmen oder Kunden.

Zwickmühle E-Mail

Wer beruflich mit Mails arbeitet, muss nicht selten Dutzende oder gar Hunderte davon Tag für Tag bearbeiten – und genauso viele Entscheidungen treffen. Das ist ganz schön viel Verantwortung, denn jede Fehlentscheidung, jeder falsche Klick kann die ganze Firma über Wochen lahmlegen. Die Krux ist, dass man es sich aber auch nicht leisten kann, eine Kundenanfrage oder eine Auftragsmail zu übersehen. Jede Mail muss daher gecheckt werden.

Sie ahnen es vielleicht bereits: Auch mit den besten Argumenten kommen Sie aus der Nummer nicht raus. E-Mail ist der kleinste gemeinsame Nenner bei der Online-Kommunikation und daher weiterhin unverzichtbar. Die interne Kommunikation kann man inzwischen gut über moderne Kollaborationssoftware wie Rocket.Chat, Slack oder Teams abwickeln, für die Kommunikation mit der Außenwelt gibt es jedoch keinen Ersatz mit breiter Akzeptanz.

Im Privatleben sieht es ähnlich aus: Freunde und Verwandte können Sie problemlos über Messenger-Apps wie WhatsApp oder Signal erreichen – Ende-zu-Ende-verschlüsselt nach Stand der Technik und mit überprüfbarem Absender. Für die Kontaktaufnahme mit Firmen, Behörden und vielen mehr müssen Sie jedoch oft noch eine Mail schreiben. Rechnungen, Versandbestätigungen, Benachrichtigungen über verdächtige Aktivitäten et cetera landen in Ihrem Posteingang, neben Phishing-Mails aller Art. Und es bleibt an Ihnen hängen, die guten Mails von den bösen zu unterscheiden.

Aber was tun? Phishing zählt zur Angriffskategorie „Social Engineering“ – die Angreifer zielen also nicht auf technische Sicherheitslücken ab, sondern auf die Schwachstelle Mensch. Genau hier setzen die folgenden Artikel an: Wir möchten Ihnen das nötige Wissen und einige praktische Tipps an die Hand geben, damit Sie leicht die Spreu vom Weizen trennen können und für Phishing-Mails nur noch ein müdes Lächeln übrig haben.

Phishing auf den zweiten Blick: Mittlerweile muss man genau hinsehen, um die Rechtschreibfehler von Online-Ganoven zu finden. In der Anrede wird hier sogar ein bisschen gegendert.

Mails entschärfen

Es geht nicht nur darum, wie Sie verdächtige Mails anhand offensichtlicher und versteckter Merkmale bewerten können (siehe S. 18), sondern auch um die kniffligen Fälle. Manchmal bleiben auch nach einer eingehenden Prüfung Restzweifel, ob es

sich um Spreu oder Weizen handelt und ob die angehängte Datei unentbehrlich ist oder ernstzunehmenden Schaden anrichtet.

In solchen Fällen können Sie den Anhang vor dem Öffnen mit einem Tool wie Dangerzone entschärfen, indem Sie ein harmloses PDF daraus machen – garantiert ohne Office-Makros. Oder Sie analysieren die Datei mit speziellen Tools, um vorab gefahrlos zu überprüfen, ob sich darin Makros oder eingebettete Dateien verstecken (siehe S. 28).

Wir möchten Sie dazu anregen, dieses Wissen auch mit Kollegen, Freunden, Familie und Geschäftspartnern zu teilen – in ihrem eigenen Interesse. Denn den größten Einfluss auf Ihren Posteingang haben nicht Sie, sondern die Absender der Mails. Wenn jeder die wichtigsten Dos & Don’ts kennt und beim Verschicken beherzigt, wird E-Mail für alle sicherer.

Wir haben die wichtigsten Tipps für den Mailversand daher als kompakte und leicht verdauliche Checkliste auf Seite 26 zusammengestellt. Die Checkliste ist online frei abrufbar, damit Sie sie leicht weitergeben können. Wenn Sie mögen, können Sie in Ihrer Mailsignatur darauf verweisen: **https://ct.de/sicher-mailen** (*rei@ct.de*)

Datenschutz Europa und USA

Prekärer Datenfluss

Was sich die USA beim Datenschutz von Europa abschauen

In den USA hatten Datenkraken lange Zeit leichtes Spiel. Doch nun droht der Datenfluss zu versiegen. Joe Biden hat den Datenverkehr mit Europa zur Chefsache erklärt, gleichzeitig arbeiten Demokraten und Republikaner fieberhaft an einem bundesweiten Datenschutzgesetz. Das hat aber seine Tücken, wie unser Überblick zeigt.

Von Falk Steiner

kompakt

- Bislang gelten in den US-Bundesstaaten unterschiedliche Datenschutzgesetze.
- Ein einheitliches Datenschutzgesetz ist in greifbare Nähe gerückt, lässt den Zugriff der Behörden aber außen vor.
- Präsident Biden will darüber hinaus den Datenaustausch zwischen der EU und den USA mit einem neuen Datenschutzrahmen absichern, der EU-Bürgern ein Klagerecht einräumt.

Mit der Datenschutz-Grundverordnung (DSGVO) hat die EU 2016 einen Standard gesetzt, an dem sich Anbieter und Gesetzgeber aus aller Welt orientieren müssen, wenn sie mit dem Recht des 27-Staaten-Bundes in Europa kompatibel sein wollen. Dabei prallen immer wieder Welten aufeinander – insbesondere transatlantische. Die USA gelten mit ihren staatlichen und privatwirtschaftlichen Akteuren immer noch als Land der Datensammler. Dort existiert bis heute kein bundesweites Datenschutzrecht. Stattdessen kocht jeder US-Bundesstaat sein eigenes Süppchen. Weil die transatlantischen Datenflüsse aus Europa zu versiegen drohen, muss die US-Regierung dringend

eine Lösung finden.

Das fehlende Datenschutzrecht auf Bundesebene ist eine von mehreren Hürden: Die DSGVO erlaubt den Export von personenbezogenen EU-Daten nur, wenn im Zielland der Schutz dieser Daten auf einem vergleichbaren Niveau wie in Europa gewährleistet ist. Die EU-Kommission als zuständige Behörde muss dies prüfen und dann eine sogenannte Angemessenheitsentscheidung treffen.

Derartige „Adequacy Decisions“ wurden bislang für 14 Staaten getroffen, darunter Südkorea, Japan, Israel, Uruguay, Kanada und die Färöer-Inseln. Der US-Rechtsrahmen ist hingegen nicht ausreichend. Daher suchten die USA in den vergangenen 20 Jahren immer wieder nach Alternativen, um die Datentransfers rechtlich abzusichern.

Doch sowohl die sogenannte Safe-Harbor-Vereinbarung zwischen EU und US-Regierung aus dem Jahr 2000 als auch die Nachfolgeregelung Privacy Shield von 2016 wurden vom Europäischen Gerichtshof (EuGH) kassiert: Die Absprachen, die keine Verträge im Sinne des Völkerrechts sind, konnten in der EU erhobene Daten nicht ausreichend sichern, befanden die Richter in Luxemburg nach zwei Klagen des österreichischen Aktivisten Max Schrems.

Nach Privacy Shield

Lange ist danach wenig passiert. Doch nun läuft den Unternehmen die Zeit davon: Nach und nach fallen die verbliebenen rechtlichen Möglichkeiten weg, doch noch irgendwie legal personenbezogene Daten in die USA zu transferieren. Die irische Datenschutzaufsichtsbehörde DPC Ireland bearbeitet dabei den wichtigsten Fall: Sie könnte Facebook untersagen, personenbezogene Daten von seinem EU-Hauptsitz auf der Insel in die USA zu transferieren. Das steht in einem Entscheidungsentwurf, den die Iren Anfang Juli an ihre Kollegen der übrigen europäischen

Datenschutzaufsichtsbehörden verschickt haben. Obwohl die DPC unter Datenschützern als sehr zurückhaltend gilt, könnte ihr Vorhaben das Aus für datengetriebene US-Unternehmen in Europa bedeuten. Die Facebook-Mutter Meta hat ihre Aktionäre schon mehrfach gewarnt, dass sie aufgrund der dann drohenden empfindlichen DSGVO-Bußgelder womöglich Teile ihres Europageschäfts aufgeben müsste – und damit Milliarden an Umsatz verlöre.

Mark Zuckerberg hat Aktionäre von Meta bereits gewarnt, dass sein Konzern womöglich bald keine personenenbezogenen Daten aus Europa mehr in die USA übertragen darf. *Bild: Eric Risberg/AP/dpa*

Sammelklagen statt Aufsichtsbehörden

Parallel dazu bewegt sich der Datenschutz in den USA: Viele US-Bundesstaaten bereiten Gesetze vor oder haben bereits welche erlassen, die die Privatsphäre besser schützen sollen. Zwei Staaten stehen im Zentrum der Aufmerksamkeit: Kalifornien schärft im Januar 2023 seinen fünf Jahre alten California Consumer Privacy Act (CCPA) mit dem Californian Privacy Rights Act (CPRA) nach. In Illinois gilt seit 2008 der Biometric

Information Privacy Act (BIPA). Das Schutzgesetz für biometrische Daten hatte nach Sammelklagen mehrere Vergleiche mit bemerkenswerten Summen zur Folge: McDonalds zahlte 50 Millionen Dollar, Google 100 Millionen Dollar und Facebook sogar 650 Millionen Dollar an Kläger aus Illinois, weil sie deren biometrische Daten unerlaubt verarbeitet und gegen den BIPA verstoßen hatten. Fast im Monatstakt kommen neue Millionenvergleiche hinzu, der Druck auf die Unternehmen steigt.

Während in Europa Aufsichtsbehörden die Strafen für Verstöße verhängen, schließen sich in den USA Betroffene vor allem in Sammelklagen zusammen. Organisationen sammeln die Rechtsansprüche vieler Bürger und reichen vor Gericht Klage gegen ein Unternehmen ein. In den seltensten Fällen enden diese Verfahren mit einem Urteil. Stattdessen schließen Kläger und Beklagte einen Vergleich. Das kann für die Firmen mitunter teurer sein als ein Gerichtsurteil.

Aufsichtsbehörden haben in den USA deutlich weniger Möglichkeiten, Bußgelder zu verhängen als in Europa. Nur in wenigen Fällen nutzt etwa die Handelsaufsicht, die Federal Trade Commission (FTC), ihre rechtlich begrenzten Möglichkeiten: Zuletzt etwa, weil sich ein Unternehmen nicht an seine Selbstverpflichtung hielt, die es im Zuge der Privacy-Shield-Vereinbarung abgegeben hatte. Auch wenn der EuGH die Privacy-Shield-Angemessenheitsentscheidung inzwischen annulliert hat, behalten die damit verbundenen Selbstverpflichtungen von Firmen in den USA weiterhin ihre Gültigkeit.

Flickenteppich

Für in- und ausländische Unternehmen sind die in einzelnen Bundesstaaten der USA aufploppenden neuen Datenschutzgesetze ein Problem: Statt an einem einzelnen Rechtsrahmen müssten sie sich eigentlich an den Vorgaben jedes Staates einzeln ausrichten und somit Nutzer in Maine anders als in Illinois

oder Kalifornien behandeln. Kein Wunder, dass sich viele der großen Technologiekonzerne ein einheitliches US-Datenschutzrecht wünschen.

Einige der Datenschutzgesetze der Bundesstaaten definieren den Begriff „personenbezogene Daten“ äußerst weitreichend, erläutert Jan Sebisch von der Gesellschaft für Außenwirtschaft und Standortmarketing (GTAI): „Sie räumen den Verbrauchern in Bezug auf ihre Daten durchaus mit EU-Niveau vergleichbare Betroffenenrechte ein, zum Beispiel das Recht auf Löschung, und in bestimmten Konstellationen sogar ein privates Klagerecht.“ Mangels US-Bundesdatenschutzgesetz gebe es für Unternehmen jedoch keine allgemeinen Leitlinien oder Faustformeln, wann sie „auf der sicheren Seite sind“. Es komme stets auf die konkrete Fallkonstellation und das entsprechende einzelstaatliche Recht an, sagt Sebisch.

Neues Bundesdatenschutzrecht

Ein Vorschlag, das zu ändern, liegt derzeit in den beiden Kammern des US-Kongresses: der American Data Privacy and Protection Act (ADPPA). Er wurde von Vertretern der Republikaner und Demokraten initiiert und schließlich von einflussreichen Mitgliedern des Repräsentantenhauses und des Senats eingebracht. Aus Sicht von Sebisch ist ein solch parteiübergreifender Vorschlag sehr beachtlich, weil Demokraten und Republikaner in puncto Datenschutzrecht zuvor nicht auf einen Nenner gekommen seien.

Der ADPPA könnte ein Bundesdatenschutzrecht schaffen, das in einigen Teilen dem EU-Recht ähnelt. Er betrachtet nicht nur unmittelbar personenbezogene Daten als regulierbar, sondern auch solche Daten, die einen Personenbezug herstellen können, wenn man sie mit weiteren Angaben koppelt. Dazu zählen auch sogenannte Identifier, denen sich Personen eindeutig zuordnen lassen.

Zudem schreibt er vor, das Erheben, Verarbeiten und

Weitergeben von Daten auf das Nötige zu beschränken und fordert damit eine ähnliche Datensparsamkeit wie die DSGVO. Laut ADPPA dürfen Daten nur noch erhoben werden, wenn dies „vernünftigerweise notwendig und verhältnismäßig“ ist. Darunter fallen Daten für Produktion und Dienstleistungen, Kundenkommunikation, Rechnungswesen und IT-Sicherheit.

An einigen Stellen geht der ADPPA-Vorschlag sogar über den Text der DSGVO hinaus: etwa beim Verbot irreführender Oberflächengestaltungen, die Betroffene zu ungewollten Einwilligungen verleiten. Hier folgt der ADPPA dem neuen Digital Services Act (DSA) der EU und formuliert darüber hinaus restriktive Regelungen zur algorithmischen Verarbeitung biometrischer Daten. „Er hat mehr Momentum als jede Vorgängerinitiative“, erläutert Tyson Barker, der für die Deutsche Gesellschaft für Auswärtige Politik (DGAP) in Berlin die transatlantische Technologiepolitik beobachtet. „Der Vorschlag beschränkt Sammelklagen, verdrängt stärkere Einzelstaatengesetze, macht bei den Betroffenenrechten viele Anleihen bei der DSGVO und integriert Elemente des DSA, etwa zu datenbasierter Werbung“, zählt Barker auf.

Derzeit hält er es jedoch für unwahrscheinlich, dass der ADPPA in dieser Form verabschiedet werde, weil ihn die wichtigste Person nicht unterstützt: Maria Cantwell, die demokratische Vorsitzende im Wirtschaftsausschuss des Senats. An Cantwell führt laut Barker kein Weg vorbei. Sie fordert wesentlich weiter gehende Regelungen zum Schutz der Privatsphäre, als sie der ADPPA derzeit vorsieht. Auf jeden Fall will sie eines verhindern: dass ein schwaches Bundesgesetz stärkere Regelungen in einzelnen Bundesstaaten aushebelt.

US-Senatorin Maria Cantwell möchte verhindern, dass ein zu laxes bundesweites Datenschutzgesetz künftig rigidere Vorgaben in einzelnen Bundesstaaten blockiert. *Bild: Maria Cantwell / U. S. Senate*

Bundesrecht und Landesrecht

Der Streit um den ADPPA und Cantwells Auffassung ähnelt der Subsidiaritätsdebatte in Europa: Was soll auf der obersten Ebene rechtlich geregelt werden, was sollen untere Ebenen beschließen? Die vollständige Vereinheitlichung auf Bundesebene zu Lasten der Gesetzgebung der Mitgliedstaaten wird in den USA als „preemption“ bezeichnet. Dies ist im ADPPA zumindest für bestehende Gesetze nicht vorgesehen. Er führt eine lange Liste von strengeren Gesetzen auf Bundes- und Einzelstaatsebene auf, die ausdrücklich nicht ausgehebelt werden sollen – etwa der Biometric Privacy Act aus Illinois. Cantwell befürchtet jedoch, dass der ADPPA künftige strengere Datenschutzregelungen in einzelnen Bundesstaaten ausschließt und somit landesweit einen zu laxen Datenschutz zementiert.

Der ADPPA regelt laut Sebisch auch den Zusammenhang zwischen behördlichen und privatrechtlichen Klagen. So sollen geschädigte Personen vier Jahre nach Inkrafttreten des Gesetzes private Klagen vor dem Bundesgericht einreichen

dürfen. Bei Datenschutzverletzungen von Unternehmen könnten sie Schadenersatz, Unterlassung, Prozesskosten und Anwaltsgebühren geltend machen, erläutert Sebisch.

Bevor sie eine Klage einreichen, müssten Betroffene dem ADPPA-Entwurf zufolge aber die Federal Trade Commission (FTC) und den Generalstaatsanwalt ihres Bundesstaates informieren. Eröffnet eine der beiden Institutionen ein Verfahren, wären Sammelklagen für dessen Dauer erst einmal ausgeschlossen. Die FTC könnte die Regelungen ähnlich wie die Datenschutzaufsichtsbehörden in Europa von sich aus durchsetzen. In diesen Tagen diskutiert der Ausschuss für Energie und Wirtschaft des US-Repräsentantenhauses sehr intensiv über den ADPPA-Entwurf. Damit er schließlich Gesetz wird, müssen seine Befürworter aber noch Maria Cantwell überzeugen. Jan Sebisch von der GTAI erwartet deshalb noch einige Änderungen, bevor der ADPPA das erste in den gesamten USA gültige Datenschutzgesetz überhaupt werden kann.

Mit dem ADPPA würden sich die USA der europäischen Vorstellung von Datenschutz deutlich annähern. Das wäre für transatlantische Datenübertragungen eine Verbesserung – dürfte aber noch lange nicht den Ansprüchen europäischer Datenschützer genügen. Dennoch begrüßt der Landesdatenschutzbeauftragte von Baden-Württemberg, Stefan Brink, die Initiative für das Gesetz: „Die Strahlkraft der Datenschutzgrundverordnung reicht ganz offensichtlich bis in die USA“, freut sich Brink angesichts vieler konzeptioneller Übernahmen im US-Vorschlag. „Inwiefern ein US-Datenschutzrecht die Beratung und Prüfung von Datenverarbeitungen mit Übermittlung in die USA verändert, hängt jedoch von der genauen Ausgestaltung des Gesetzes ab.“

Geheimdienste bleiben unberührt

Bei aller Euphorie enthält der ADPPA noch einige Lücken. Denn er soll grundsätzlich nur die Rechte von Personen mit einer US-Aufenthaltserlaubnis schützen. Darunter fallen auch viele

in den USA lebende Ausländer. Doch selbst US-Bürger, die im Ausland leben, könnten sich dem Entwurf nach nicht auf ihn berufen, betont Calli Schroeder von der US-Bürgerrechtsorganisation EPIC. Zugleich wären Ansprüche aus den Vorschriften nicht von Personen außerhalb der USA einklagbar – also auch nicht von Europäern.

Einen Aspekt klammert der ADPPA zudem vollständig aus, da er als Verbraucherschutznorm konzipiert ist: den Datenzugriff von US-Behörden, darunter Strafverfolgern und Geheimdiensten wie der NSA. Genau hier liegt seit dem Urteil des EuGH zum Privacy Shield 2020 aber ein großer Stolperstein. Infolge der Snowden-Affäre prüfte der EuGH, unter welchen Umständen US-Behörden auf personenbezogene Daten zugreifen dürfen, die in den USA oder aber von US-Unternehmen außerhalb der USA gespeichert sind. In seinem Urteil bemängelte der EuGH sowohl die umfangreichen Zugriffsmöglichkeiten der US-Geheimdienste als auch das Fehlen von Rechtsmitteln, die EU-Bürger dagegen einlegen können. Dieses Urteil fordert das politische Washington gleich auf mehreren Ebenen heraus.

Auf der einen Seite ist es aus Sicht vieler US-amerikanischer Politiker ein Unding, dass ein europäisches Gericht amerikanischen Behörden und Gesetzgebern Vorschriften machen möchte. Auf der anderen Seite steht die enorme wirtschaftliche Bedeutung, die der EU-Markt für die meisten US-Tech-Konzerne hat. Und ein Szenario, in dem US-Firmen vom Datenstrom aus Europa abgeschnitten werden, ist mit der kommenden Entscheidung der irischen Datenschutzaufsichtsbehörde DPC nur noch Monate statt Jahre entfernt.

US-Präsident Joe Biden hat den Datenaustausch mit Europa zur Chefsache erklärt. Er möchte die EU mit Präsidialverfügungen zufriedenstellen. *Bild: Evan Vucci/AP/dpa*

TADPF soll Datenverkehr sichern

Damit EU-US-Datentransfers in Zukunft rechtssicher sind, soll daher eine neue Vereinbarung zwischen den USA und der EU her. Damit sie nicht ebenfalls vor dem Europäischen Gerichtshof scheitert, soll sie Daten von EU-Bürgern besser schützen als Safe Harbor und Privacy Shield.

US-Präsident Joe Biden erklärte dies zur Chefsache und kündigte bei seinem Besuch in Brüssel im Frühjahr einen neuen transatlantischen Datenschutzrahmen an: Die US-Regierung bietet der EU-Kommission ein Transatlantic Data Privacy Framework (TADPF) an. Die Vorarbeiten dafür laufen seit Anfang vorigen Jahres. Doch bis Redaktionsschluss fehlte das wohl wichtigste Element: der Rechtstext, mit dem die US-Regierung den Einwänden des EuGH künftig begegnen will.

Bislang gibt es nur mündliche Ankündigungen von Präsident Biden. So wollen die USA künftig weniger Daten über EU-Bürger

sammeln und ihre Behörden strenger prüfen. EU-Bürger sollen sich zudem rechtlich gegen eine Erfassung durch US-Geheimdienste wehren können – vor einer dafür zuständigen Gerichtsinstanz.

Solange die Präsidialverfügungen aber nicht vorhanden sind, kann die EU-Kommission mit dem in der DSGVO vorgesehenen Prozess für eine Angemessenheitsentscheidung nicht beginnen. Offen ist zudem, ob die EU-Kommission eine solche Entscheidung auf Basis von US-Präsidialverfügungen überhaupt treffen kann. Denn ein künftiger Präsident könnte eine Executive Order jederzeit mit einem Federstrich ändern.

Landesdatenschützer Stefan Brink wünscht sich deshalb einen anderen Weg: „Ein – parlamentarischer – Rechtsakt würde mehr Beständigkeit und damit auch Rechtssicherheit versprechen." Seine Behörde hätte bei der Angemessenheitsentscheidung der EU-Kommission zwar ein Recht zur Mitsprache, allerdings nicht zum Veto.

Klagen mit Ansage

„Europas Sorgen im Fall einer Wiederkehr Trumps könnten Überlegungen nötig machen, wie der Kongress die Präsidialverfügungen in Gesetzen kodifizieren könnte", sagt Tyson Barker von der DGAP. 2024 muss der US-Kongress den Abschnitt 702 des für die Überwachungsbefugnisse der Behörden wichtigsten Gesetzes, dem Foreign Intelligence Surveillance Act (FISA), erneut beschließen. „Das könnte eine Gelegenheit sein, das Gesetz so anzupassen, dass es die Inhalte der Präsidialverfügungen widerspiegelt", erklärt Barker.

Es bewegt sich also etwas beim Datenschutz in den USA, wenn auch aus europäischer Sicht zu wenig. Bei der Ankündigung des TADPF meinte Datenschutzvorkämpfer Max Schrems, er wolle die Vereinbarung prüfen. Er geht davon aus, dass nach einer eventuellen Angemessenheitsentscheidung der EU-Kommission zum TADPF Klagen beim EuGH eingereicht werden. Falls nicht von ihm

selbst, dann von anderen Datenschutzaktivisten. (*hag@ct.de*)

Datenschutzaktivist Max Schrems hat mit seinen Klagen bereits Safe Harbor und Privacy Shield gekippt. Die Geschichte könnte sich mit dem TADPF wiederholen. *Bild: Hans Punz/APA/dpa*

1. Literatur
2. Holger Bleich, FAQ: Das Ende des Privacy Shields, c’t 21/2020, S. 178

EU – Umgang mit Daten

Europäisches Trommelfeuer

Wie die EU den Umgang mit Daten revolutionieren will

Europa soll zum Vorbild für die digitale Gesellschaft werden. Dazu zündet die EU ein wahres Feuerwerk an Gesetzen. Sie sollen die Dominanz der US-Unternehmen brechen und europäischen Firmen einen besseren Zugang zu Daten verschaffen. Die geplanten Regulierungen stellen sogar die DSGVO in den Schatten, wie unsere Übersicht zeigt, und werden die Gesellschaft wohl nachhaltig verändern.

Von Joerg Heidrich

kompakt

- Ab Mitte 2023 reguliert der Digital Markets Act europaweit die Geschäftspraktiken von Onlineplattformen, ab 2024 greift der Digital Services Act.
- Der Data Governance Act und der Data Act sollen vor allem den Umgang mit nicht personenbezogenen Daten regeln, die nicht unter die DSGVO fallen.
- Firmen sollen ihre Daten künftig mit Treuhändern teilen, ein AI Act verbietet KI-Systeme in besonders risikoreichen Einsatzgebieten.

Mit viel Pathos kündigte die EU-Kommission Anfang 2020 in einer Art Manifest ihre neue Datenstrategie an. Die EU könne zu einem Vorbild für eine Gesellschaft werden, die „dank Daten in der Lage ist, in der Wirtschaft wie im öffentlichen Sektor bessere Entscheidungen zu treffen“. Um eine weltweit führende Rolle in der Datenwirtschaft zu übernehmen, müsse man unverzüglich handeln und die vielfältigen Probleme regulatorisch angehen, die von der Konnektivität über die Datenverarbeitung und -speicherung bis hin zur Cybersicherheit reichen.

Hierfür sei es nötig, die Voraussetzungen für den Umgang mit

Daten zu verbessern und für die Gesellschaft „Pools mit hochwertigen Daten“ aufzubauen. Diese sollen nicht nur die Produktivität von Firmen steigern und deren Wettbewerbsfähigkeit verbessern, sondern auch den Bereichen Gesundheit, Umwelt und öffentliche Dienste zugutekommen. Zugleich will man die digitale Wirtschaft fördern, damit sie mit Firmen aus den USA und China mithalten kann.

Um diese ambitionierten Ziele zu erreichen, hat die Kommission seit der Ankündigung ein ganzes Bündel aus Gesetzen auf den Weg gebracht. Juristen erwarten gar ein neues Rechtsgebiet, das Datenrecht. Im Fokus der Diskussion steht etwa ein halbes Dutzend dieser Vorhaben. Sie haben das Potenzial, die Gesellschaft nachhaltig zu verändern.

Digital Services Act

Dies gilt insbesondere für den Digital Markets Act (DMA) und den Digital Services Act (DSA). „Acts“ sind Verordnungen, die – wie beispielsweise die DSGVO – unmittelbar als europäisches Recht gelten. Im Gegensatz zu Richtlinien müssen Gesetzgeber in den einzelnen europäischen Ländern sie nicht erst in nationales Recht umsetzen.

EU-Binnenmarktkommissar Thierry Breton kündigte mit den neuen EU-Verordnungen „das Ende des Wilden Westens" im Internet an. *Bild: Virginia Mayo/Pool AP/dpa*

Der DSA tritt ab 2024 in Kraft und wendet sich insbesondere an Anbieter von Onlinediensten und sozialen Medien. Er verpflichtet diese, in kurzer Zeit gegen rechtswidrige Inhalte vorzugehen. Besonders strenge Anforderungen gibt es für jene großen Onlineplattformen und Suchmaschinen, die im Monat von mehr als 45 Millionen Menschen genutzt werden. Aufgrund ihrer Reichweite sollen deren Anbieter „systemische Risiken" eindämmen, die sich etwa aus der Verbreitung rechtswidriger Inhalte ergeben. Dazu zählen Desinformation oder Wahlmanipulation, Cybergewalt gegen Frauen sowie jugendgefährdende Inhalte. Die EU-Kommission sieht darin einen wichtigen Schritt „zur Verteidigung europäischer Werte wie Demokratie und Rechtsstaatlichkeit" im virtuellen Raum. Der DSA wird damit zum EU-weiten Nachfolger des deutschen Netzwerkdurchsetzungsgesetzes (NetzDG), welches bereits jetzt Social-Media-Angebote reguliert.

In die Pflicht nimmt der DSA auch Onlinemarktplätze. Sie haben dafür zu sorgen, dass über ihre Plattformen keine gefährlichen

oder illegalen Produkte wie Markenfälschungen angeboten werden. Das Gesetz sieht dazu neue Mechanismen vor, die es Usern ermöglichen, illegale Inhalte zu melden. Die Plattformen müssen zudem mit „vertrauenswürdigen Hinweisgebern“ zusammenarbeiten, die ihnen helfen sollen, verbotene Inhalte zu ermitteln und zu entfernen.

Der DSA regelt ferner bestimmte Formen der Werbung. Hier war sogar ein grundsätzliches Verbot von Werbetracking in der Diskussion, der Ansatz konnte sich jedoch nicht durchsetzen. Das Gesetz enthält allerdings ein Verbot irreführender Werbepraktiken, zum Beispiel gezielt auf Kinder ausgerichtete Werbung oder solche, die auf sensiblen Daten wie Religionszugehörigkeit, sexueller Ausrichtung oder politischer Meinung basiert. Dies wird die werbetreibende Industrie vor große Herausforderungen stellen.

Nach den neuen Vorschriften sind auch sogenannte Dark Patterns verboten. Onlineplattformen dürfen Nutzer nicht mehr täuschen oder manipulieren beziehungsweise „ihre Fähigkeit, freie und fundierte Entscheidungen zu treffen“ beeinträchtigen oder behindern.

Digital Markets Act

Der DMA kommt etwas früher und gilt bereits ab der zweiten Jahreshälfte 2023. Seine Vorschriften ergänzen das Wettbewerbsrecht und sollen die Macht der marktbeherrschenden Digitalkonzerne einschränken. Auf deren Plattformen, den sogenannten Gatekeepern, soll es zukünftig durch gesetzliche Regulierung fairer zugehen.

Welche Unternehmen unter diese Einstufung fallen, legt die Kommission explizit fest. Erfasst werden mit hoher Sicherheit Unternehmen wie Airbnb, Alphabet, Apple, Amazon, Meta und Microsoft. Dass es sich dabei um amerikanische Konzerne handelt, ist kein Zufall. Die gesamte Digitalstrategie der EU beruht darauf, es amerikanischen Unternehmen schwerer zu

machen und so die digitale Wirtschaft im europäischen Raum zu stärken. Aber auch die Verbraucher sollen geschützt werden, indem Firmen ihre Nutzerdaten nicht mehr über Plattformgrenzen hinweg zusammenführen dürfen.

Den Gatekeepern ist es zukünftig untersagt, ihre eigenen Dienste oder Produkte höher zu gewichten als die von anderen geschäftlichen Nutzern ihrer Plattform. Dies dürfte etwa Amazon oder Alphabet treffen, denen Kritiker häufig vorhalten, eigene Angebote gegenüber Dritten zu bevorzugen.

Weitere Regelungen sollen sogenannte Lock-In-Effekte verhindern. Die als Gatekeeper eingestuften Plattformen müssen ihre Angebote kompatibel zu denen von Wettbewerbern gestalten. In der Vergangenheit musste etwa Microsoft bereits hohe Strafen zahlen, weil es unter Windows seinen Edge-Browser gegenüber anderen Browser bevorzugt hatte.

Verstößt ein Gatekeeper gegen die Vorschriften des DMA, so kann dies für ihn sehr teuer werden. Die neue Vorschrift sieht Geldstrafen vor, die bis zu 10 Prozent Gesamtumsatzes betragen, die das Unternehmen im vorhergehenden Geschäftsjahr weltweit erzielt hat. Bei wiederholten Verstößen können die Strafen sogar bis zu 20 Prozent des Umsatzes betragen. Im Fall von Amazon wären das aktuell bis zu 94 Milliarden US-Dollar.

Die dänische EU-Kommissarin für Wettbewerb, Margrethe Vestager, gilt als treibende Kraft hinter dem Digital Markets Act, der wettbewerbswidrige Praktiken der großen US-Konzerne eindämmen soll. *Bild: Oliver Berg/dpa*

Umstrittene Interoperabilität

Die geplante Regulierung von Messenger-Diensten trifft bei kleineren Anbietern eher auf Ablehnung. Künftig müssen sich Platzhirsche wie WhatsApp und iMessage dafür öffnen, auch Nachrichten von Wettbewerbern zu empfangen. Kleinere Anbieter wie Signal oder Threema sperren sich jedoch gegen das Vorhaben. Die Firmen sehen nämlich durch die Pläne der EU die vertrauliche und sichere Kommunikation über ihre Apps bedroht. So fürchtet der Betreiber von Signal, dass die Zusammenarbeit mit den dominanten Messengern letztlich die Privatsphäre des eigenen Angebots verschlechtert. Die Mitbewerber hätten dann Zugriff auf Metadaten und könnten diese für ihre Zwecke nutzen. Daher haben beide Anbieter bereits angekündigt, auf eine Zusammenschaltung mit WhatsApp & Co. zu verzichten.

Laut Digital Markets Act müssen Gatekeeper wie WhatsApp sich für Konkurrenten öffnen, wenn diese das fordern. Anbieter wie Threema und Signal wollen davon jedoch keinen Gebrauch machen. *Bild: Threema*

Trainingsdaten für KI

Während der DMA und der DSA primär Plattformen und größere Onlinedienste regulieren, betrifft der zweite wichtige Teil der EU-Strategie den Umgang mit Daten. Für personenbezogene Daten gilt die Datenschutz-Grundverordnung (DSGVO) bereits seit 2018. Allerdings gibt es eine Vielzahl von Daten, die nicht unter die DSGVO fallen, insbesondere solche, die von Maschinen stammen und für das Training neuronaler Netze genutzt werden. Hier setzen zwei weitere Gesetzesvorhaben der EU an: der Data Governance Act (DGA) und der Data Act (DA).

Den DGA verabschiedeten die EU-Gremien bereits im Mai 2022. Er soll im September 2023 in Kraft treten. Ziel des Gesetzes ist es, dem öffentlichen Sektor den Zugang zu Daten zu erleichtern und ein „vertrauenswürdiges Umfeld“ für die Forschung sowie für innovative Dienste und neue Produkte zu schaffen.

Der DGA geht bei der Weitergabe von Daten an den öffentlichen Sektor sehr weit. Der Regelung liegt der Gedanke zugrunde, dass auch geschützte Daten der Gesellschaft zugutekommen sollen, wenn sie beispielsweise durch öffentliche Förderung generiert oder gesammelt wurden. Firmen sollen beispielsweise Geschäftsgeheimnisse, personenbezogene Daten und durch Rechte des geistigen Eigentums geschützte Werke übertragen. Dies gilt allerdings nur für Daten, die sich bereits „im Besitz öffentlicher Stellen“ befinden. Dort vorhandene Daten können etwa für Forschungszwecke im öffentlichen Interesse weiterverarbeitet werden.

Faire Datenbroker

Der DGA soll darüber hinaus ein neues und potenziell revolutionäres Geschäftsmodell etablieren: Es sollen Datenvermittlungsdienste entstehen, die eine sichere Umgebung bieten, in der Unternehmen oder Einzelpersonen Daten austauschen. Unternehmen sollen ihre Daten teilen können, ohne Missbrauch oder einen Wettbewerbsnachteil befürchten zu müssen.

Die Vermittlungsdienste bieten nur eine Plattform an und sind ansonsten neutrale Akteure. Die von ihnen vorgehaltenen Daten dürfen sie nicht zu eigenen Zwecken nutzen. Erstaunlicherweise müssen sie aber keinen Sitz innerhalb der EU haben, sondern dürfen sich auch außerhalb der EU niederlassen.

Auf Basis der neuen Regulierung sollen Dienste entstehen, die einen Handel mit persönlichen Daten ermöglichen. Der Gesetzgeber sieht solche Datainteremediären als Schlüssel für eine neu entstehende Datenwirtschaft. Genannt werden als Beispiel Daten-Wallets, also Apps, mit deren Hilfe der Einzelne in die Nutzung seiner Daten einwilligt und dadurch auch Geld verdienen oder sonstige Vorteile erlangen kann.

Daten für alle

Der dritte Bereich des Data Governance Acts bildet das Konzept des Datenaltruismus ab. Die EU will es Privatpersonen und Unternehmen erleichtern, der Gesellschaft Informationen für Ziele im allgemeinen Interesse zur Verfügung zu stellen. Hierzu zählen beispielsweise Daten für Forschungszwecke im Bereich der Medizin, des Klimawandels oder um öffentliche Dienstleistungen zu verbessern.

Allerdings ist es gar nicht so einfach, eine datenaltruistische Organisation zu werden. Die Stellen müssen neben hohen Anforderungen an ihre technische Ausstattung und Transparenz auch umfangreiche Berichtspflichten erfüllen, sobald sie in ein Verzeichnis aufgenommen wurden.

Den wohl radikalsten Ansatz hinsichtlich des Umgangs mit Daten verfolgt die Europäische Kommission derzeit mit dem Data Act (DA). Dieser befindet sich allerdings noch in einer recht frühen Phase des Gesetzgebungsverfahrens und wird nicht vor 2024 in Kraft treten. Der Grundgedanke des Data Act liegt darin, bislang weitgehend ungenutzte Potenziale von Daten auszuschöpfen und dadurch die europäische Wirtschaft zu fördern.

Zu diesem Zweck verpflichtet der DA Unternehmen dazu, ihre eigenen Daten zugänglich zu machen und Dritten zur Verfügung zu stellen. Dabei geht es in erster Linie nicht um personenbezogene Informationen, sondern um Maschinendaten, insbesondere aus Industrieanlagen, medizinischen Geräten, IoT- oder Smart-Home-Prozessen. Gerade kleine und mittlere Unternehmen (KMU) können auf solche Daten bislang nicht zugreifen oder sie zusammenführen, wodurch ihnen erhebliche Wettbewerbsnachteile bei der Entwicklung innovativer Geschäftsfelder entstehen.

Daten vergesellschaften

Der Data Act regelt zahlreiche, noch nicht abschließend diskutierte Voraussetzungen, unter denen Unternehmen verpflichtet werden können, ihre Informationen zu teilen. Zugleich soll er festlegen, wer unter welchen Umständen auf diese Daten zugreifen darf. Das können auch öffentliche Stellen sein, sofern sie ein erhebliches Interesse nachweisen, etwa im Rahmen der Bekämpfung einer Pandemie. Der DA soll so eine Art „freien Datenmarkt“ für nicht-personenbezogene Nutzungsdaten schaffen, auf dem diese gehandelt und weitergeben werden. Unter bestimmten Voraussetzungen sollen auch Vergütungen fließen.

Die Unternehmen, bei denen die begehrten Daten entstehen und in deren Rechte eingegriffen werden soll, reagieren nicht gerade begeistert auf den Vorstoß der EU-Kommission. So kritisiert beispielsweise der Bundesverband der Deutschen Industrie (BDI) in einer Stellungnahme bereits den Ansatz der Regulierung im DA. Man zweifele an der „Notwendigkeit eines solchen breit gelagerten Eingriffs in die Grundprinzipien der Datenwirtschaft in noch jungen Märkten”.

Die Kommission hält den Eingriff jedoch für notwendig, damit die europäische Wirtschaft mithilfe eines solchen Datenbinnenmarkts wettbewerbsfähig gegen eine sich rasant entwickelnde internationale Konkurrenz bleibt. Wie weit der Data Act jedoch in seiner finalen Form gehen wird, ist angesichts des langen Weges durch die Mühlen der europäischen Gesetzgebung noch offen.

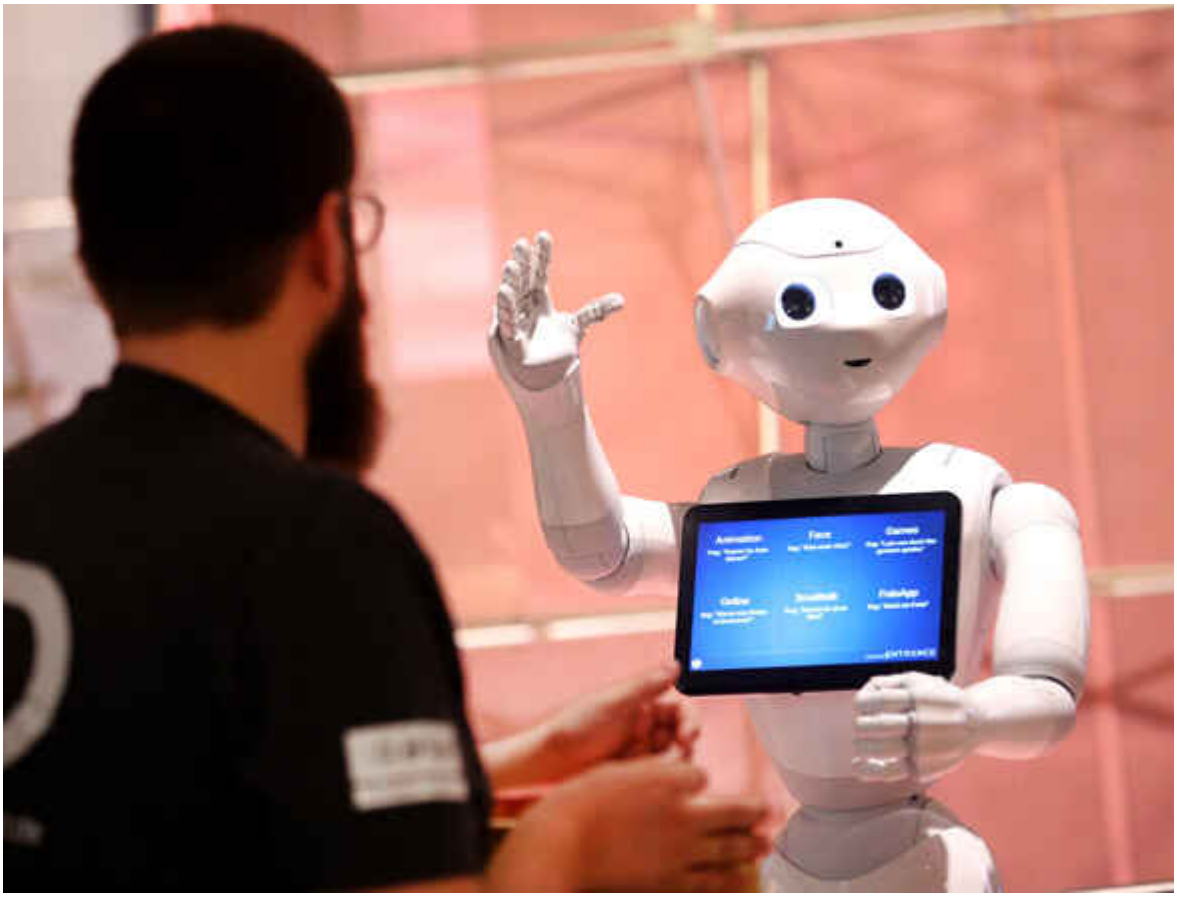
KI im Zaum halten

Erwähnenswert ist in diesem Zusammenhang auch der Artifical Intelligence Act, der ebenfalls noch in einer sehr frühen Phase der Gesetzgebung hängt und nicht vor 2024 zu erwarten ist. Der AI Act soll einen europaweit einheitlichen rechtlichen Rahmen schaffen, in dem Unternehmen und

Institutionen sichere und vertrauenswürdige Systeme mit künstlicher Intelligenz entwickeln und einsetzen.

Im Kern der vorliegenden Fassung steht dabei ein Stufensystem, das die KI-Anwendungen in verschiedene Risikoklassen mit daraus resultierenden Vorgaben einteilt. In die strengste Kategorie des „Inakzeptablen Risikos“ fallen vier Praktiken, die der Gesetzgeber als klare Bedrohung bewertet und grundsätzlich verbietet.

Hierzu gehören Social Scoring, also die „Klassifizierung der Vertrauenswürdigkeit natürlicher Personen auf der Grundlage ihres sozialen Verhaltens“ ebenso wie das sogenannte Nudging, die unterschwellige Beeinflussung einer Person außerhalb des Bewusstseins. Ebenfalls verbieten wollen die Initiatoren das „Ausnutzen der Schwäche oder Schutzbedürftigkeit einer bestimmten Gruppe von Personen aufgrund ihres Alters oder ihrer Behinderung“. Zumindest teilweise wollen sie außerdem untersagen, biometrische Echtzeit-Fernidentifizierungssysteme in öffentlich zugänglichen Räumen zur Strafverfolgung zu nutzen. Erstaunlicherweise nicht in dieser Gruppe finden sich naheliegende Bedrohungen durch autonome Waffensysteme, die ihre Ziele mithilfe von künstlicher Intelligenz auswählen.



Der AI Act teilt KI-Systeme in Risikostufen ein und verbietet künftig beispielsweise deren Einsatz beim Social Scoring. *Bild: Roland Weihrauch/dpa*

Anwendungen, die als potenziell bedrohlich eingestuft werden, fallen in die Kategorie „Hohes Risiko“. Nutzt jemand Algorithmen für derartige Bereiche, so muss er zahlreiche Voraussetzungen erfüllen und die Sicherheit der Anwendung nachweisen. Hierzu zählt etwa, natürliche Personen biometrisch zu identifizieren und zu kategorisieren, ferner die Strafverfolgung, die Rechtspflege sowie die Verwaltung und der Betrieb kritischer Infrastrukturen.

Für Angebote im Bereich des „begrenzten Risikos“ gelten vor allem Transparenzverpflichtungen. Hierunter fallen zum Beispiel Chatbots, die dann als solche gekennzeichnet werden müssen. Nutzer sollen informierte Entscheidungen treffen können, ob sie diese Angebote nutzen wollen. Nicht reguliert werden KI-gestützte Prozesse mit „minimalem Risiko“ wie KI-gestützte Videospiele oder Spamfilter, da von ihnen nur eine geringe Gefahr für die Sicherheit und Rechte der Nutzer

ausgehe.

Der AI Act sieht in seinem derzeitigen Stadium weiterhin vor, dass die von einer KI getroffenen Entscheidungen „transparent und fair“ sein müssen. Das könnte in einigen Bereichen, in denen etwa Deep Neural Networks zum Zuge kommen, sehr schwierig werden, weil die trainierten Netzwerke zum Teil Tausende Variablen einbeziehen. Aber auch bei diesem Entwurf kann es noch zu erheblichen Änderungen im Rahmen des Gesetzgebungsverfahrens kommen.

Fazit

Die Grundgedanken der ambitionierten Datenstrategie der EU-Kommission sind nachvollziehbar und im Grundsatz auch sinnvoll. Die Liste von geplanten oder bereits umgesetzten Gesetzen ist sogar noch weitaus länger als hier dargestellt.

Es ist allerdings fraglich, ob man ein hochgradig disruptives und dynamisches Umfeld tatsächlich einer so weitgehenden staatlichen Regulierung unterwerfen und diese mit den Rechten von Bürgern und Unternehmen in Einklang bringen kann. Ungeklärt ist beispielsweise das Verhältnis der DSGVO zu den vielen neuen Acts, denen ein allzu rigider Datenschutz in vielen Bereichen im Weg stehen wird. Schließlich ist es ja ein Ziel der Regulierungen, die internationale Wettbewerbsfähigkeit der europäischen Wirtschaft zu verbessern, indem man ihr den Zugang zu Daten erleichtert. Zudem überschneiden sich viele der neuen Grundverordnungen in zahlreichen Punkten. Zu befürchten ist daher, dass ein regulatorisches Dickicht entsteht, welches auf Jahre zu einer großen Rechtsunsicherheit führt. *(hag@ct.de)*

Die wichtigsten EU-Gesetzesinitiativen	
Name	Wichtigste Regelungen
Digital Markets Act (DMA)	– reguliert den Wettbewerb und insbesondere große Unternehmen – verpflichtet Gatekeeper zu fairem Wettbewerb – fordert Interoperabilität zwischen Anbietern (Messenger)
Digital Services Act (DSA)	– verlangt sicheren digitalen Raum ohne rechtswidrige Inhalte – fordert von Onlinemarktplätzen eine Überwachung der Angebote – verbietet bestimmte Werbepraktiken, etwa gezielte Ansprache von Kindern
Data Governance Act (DGA)	– reguliert Verfügbarkeit von Daten für den öffentlichen Sektor – schafft Basis für Datenvermittlungsdienste und Datenaltruismus
Data Act (DA)	– fördert die Wirtschaft durch stärkere Datennutzung – regelt Voraussetzungen, unter denen Firmen ihre Daten teilen müssen – strebt einen freien Datenmarkt für nicht-personenbezogene Daten an
Artificial Intelligence Act (AIA)	– reguliert den Rahmen und die Entwicklung künstlicher Intelligenz – teilt KI-Anwendungen in Risikoklassen mit bestimmten Beschränkungen ein

Datenstrategie der EU-Kommission: ct.de/ynr9

Handytickets für iOS erzeugen

Taschenticketautomat

Apple Wallet: Handytickets für iOS erzeugen

Fluggesellschaften bieten sie an, die Bahn und Konzertveranstalter: digitale Tickets, die man nicht ausdrucken muss und einfach auf dem Mobiltelefon mitnimmt. Apple hat sich dafür die App namens Wallet und ein Dateiformat mit raffinierten Zusatzfunktionen ausgedacht. So erzeugen Entwickler mit überschaubarem Aufwand eigene digitale Tickets, Gutscheine und Kundenkarten.

Von Jan Mahn

kompakt

- Digitale Tickets auf dem Handy sind praktisch und mehr als ein Ersatz für die Papierversion. Sie sind schnell griffbereit und informieren zum Beispiel über Planänderungen.
- Apple hat für iOS eine Ticket-App namens Wallet zusammen mit einem eigenen Datenformat entwickelt.
- Um als Entwickler Tickets zu erzeugen, braucht man theoretisch nur einen Texteditor und einen Apple-Entwickleraccount – für echte Tickets vom Fließband gibt

es Open-Source-Generatoren.

Früher, eigentlich bis vor wenigen Jahren, waren sämtliche Eintrittskarten und Reisetickets noch durchgängig vom Anbieter gedruckte Dokumente, auf einem speziellen Papier mit Glitzerstreifen, damit sie nicht jeder nachbauen konnte. Als nächste Evolutionsstufe folgten Tickets zum Selbstausdrucken. Die Echtheit bestätigt man seither nicht mehr über ein exklusives Spezialpapier, sondern über einen aufgedruckten Code, sei es ein Bar- oder ein QR-Code. Das Kontrollpersonal scannt ihn und ein mit einem Server verbundenes Lesegerät verrät, ob dieses Ticket gültig und noch nicht genutzt ist.

Anstatt den Code auszudrucken und ein zerknicktes A4-Ticket zum Konzert mitzunehmen, kann man den Code inzwischen auch direkt auf dem Mobiltelefon belassen und dessen Display beim Einscannen vorzeigen. Doch wer schon mal versucht hat, ein PDF-Ticket auf dem Handy aus der Mail-App zu fischen und so zu zoomen, dass man den QR-Code bequem scannen kann, der weiß, dass das nicht an den Komfort von Papier herankommt. Bequemer geht es mit einer Ticket-App. Apple hat sich schon 2012 die App Passbook ausgedacht und später in Wallet umbenannt. Neben Tickets liegen dort seitdem auch Apple-Pay-Kreditkarten. Die App funktioniert aus Kundensicht denkbar einfach: Man bekommt auf welchem Weg auch immer – per Mail, in einer anderen App oder auf einer Website – einen Link, um ein Ticket herunterzuladen oder direkt eine Ticket-Datei. Auf dem iOS-Gerät wird die Datei direkt in der Wallet-App geöffnet und die Karte dem Wallet hinzugefügt. Öffnet man den Link auf einem per iCloud verbundenen macOS-Computer, landet sie ebenfalls via Cloud-Magie auf dem iOS-Mobiltelefon. Und auch auf die Apple-Watch rutschen die digitalen Karten auf Wunsch. Gegen Vervielfältigung und Weitergeben sind die Pässe nicht geschützt, es können auch mehrere Konzertbesucher dasselbe Ticket auf ihr Telefon laden – so wie man auch ein PDF-Ticket

mehrfach ausdrucken kann. Beim Einlass muss der Bar- oder QR-Code also immer mit einer Datenbank abgeglichen werden.

Die Einladung zu einer fiktiven Grillfeier mit Freunden steckt als digitales Ticket in der Apple-Wallet-App: Für Freunde mit Android-Telefonen muss man entweder ein eigenes Ticket ausstellen oder ihnen eine alternative App empfehlen.
Beim Einlass zum Konzert findet der Besucher all seine gültigen Tickets fein säuberlich sortiert in dieser App und der QR- oder Barcode ist immer an den Bildschirm angepasst. Doch damit nicht genug: Der Ticketanbieter kann das Ticket auch so präparieren, dass es zum Beispiel eine Stunde vorm Konzert beim Benutzer aufpoppt und er es nicht einmal mehr raussuchen muss. Und wenn die Show ausfällt oder sich der Flug verspätet, kann der Veranstalter alle Kunden mit Wallet-Ticket per Push-Benachrichtigung informieren, ohne dass diese eine separate App bräuchten. Als Alternative zu QR-Codes können

sich die digitalen Tickets bei der Kontrolle auch per Near Field Communication (NFC) ausweisen.

Proprietär, aber transparent

Der Funktionsumfang hat Sie überzeugt und Sie wollen als Entwickler direkt loslegen, solche Tickets zu erzeugen? Dann haben wir zuerst ein paar nicht so gute Nachrichten: Das Format für die Wallet-Tickets hat sich Apple im stillen Kämmerlein ausgedacht. Es gibt also keinen (Web-)Standard und Apple kümmert sich auch nicht um den Teil der Nutzerschaft, der ohne iPhone aus dem Haus geht, sondern lieber ein Android-Gerät zum Konzert mitnimmt. Wie die Tickets dennoch aufs Android-Telefon gelangen, lesen Sie auf Seite 154.

Und Android?

Auch auf dem Android-Telefon kann man die für Apples Betriebssysteme erstellten Tickets öffnen. Im Play Store gibt es die kostenlose App WalletPasses. Sie stammt von einem Entwickleraccount namens „WalletPasses Alliance“. Das klingt wie ein unabhängiger Herstellerverband, scheint aber ein Fantasiename zu sein. Außerhalb des Stores tritt ein Verband dieses Namens nirgends in Erscheinung. Auch Apple hat damit nichts zu tun. Die App funktioniert aber, kann Apples Datenformat lesen und zeigt die Passes nahezu im gleichen Layout wie die Original-App an.

Dass Apple in diesem Bereich jahrelang die Nase vorn hatte, schien auch Google zu stören. Auf der Entwicklerkonferenz Google I/O im Mai 2022 stellte das Unternehmen seine Pläne für Google Wallet vor. Nicht nur der Name erinnert an Apples App, auch das Konzept: Das Bezahlen mit Google Pay soll künftig nur eine Funktion der digitalen Brieftasche namens Google Wallet sein. Daneben sollen Kundenkarten, Tickets und Impfpässe ein digitales Zuhause bekommen. Die Entwickerdokumentation für diese neuen Funktionen ist unter der Adresse developers.google.com/wallet zu finden.

Nur weil das Format von Apple entwickelt wurde, bedeutet das zum Glück aber nicht, dass nur Apple-Software solche Tickets erzeugen kann. Und anders als bei Transaktionen über den App-Store nimmt Apple auch keine Provision für jedes ausgestellte Ticket. Stattdessen ist das Format ausführlich dokumentiert (siehe ct.de/yw3e) und jeder mit einem Texteditor und einem Zip-Werkzeug könnte Tickets erzeugen. Es gibt jedoch einen Haken: Damit die Tickets, in Apples Terminologie Pass genannt, beim Kunden funktionieren, muss man sie digital signieren. Dafür braucht man ein Apple-Entwickler-Zertifikat, das man nur bekommt, wenn man sich als Entwickler im Apple-Developer-Programm registriert. Der Account berechtigt auch dazu, Apps in den Store zu bringen und damit Geld zu verdienen. 99 US-Dollar (und mit Steuern auch 99 Euro) kostet ein solcher Account für Einzelpersonen im Jahr. Wie Sie Apple-Entwickler werden und an ein Zertifikat zum Signieren der Tickets kommen, lesen Sie auf Seite 155.

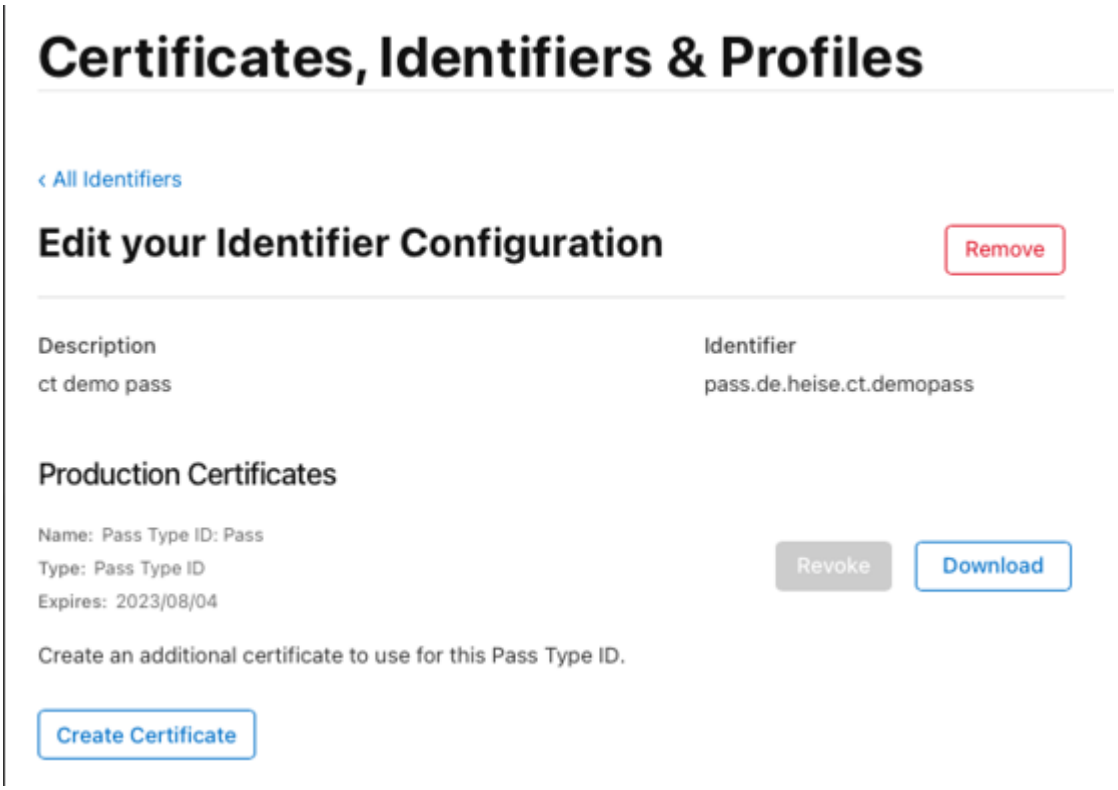
Developer-Account und Zertifikat beschaffen

Ein Apple-Developer-Account ist Voraussetzung, um Passes für die Wallet signieren zu können. Nebenbei dürfen Entwickler mit einem solchen Account auch Apps in den App Store bringen – 99 Euro kostet die Mitgliedschaft für ein Jahr. Um Mitglied zu werden, braucht man eine gewöhnliche Apple-ID, die man als normaler Nutzer zum Beispiel für die App-Stores und Apple Music nutzt. Der Login muss durch einen zweiten Faktor abgesichert sein. Los geht die Registrierung unter der Adresse developer.apple.com/enroll. Der Assistent fragt zunächst nach der Art des Accounts – im einfachsten Fall meldet man sich als Privatperson an. Firmenangehörige, die mit dem Account auch Apps unter Firmennamen verkaufen wollen, müssen den anderen Knopf betätigen. Die Fragen des Assistenten sind weitestgehend schnell beantwortet – etwas verwirrend ist die Anforderung, die eigenen Kontaktdaten zweimal einzutippen, einmal davon „Romanized“. Das ist für asiatische Entwickler gedacht, die ihre Daten einmal in ihren Schriftzeichen und noch einmal im

lateinischen Buchstabensystem eingeben sollen. Europäer füllen beide Abschnitte des Formulars einfach identisch aus.

Am Ende des Prozesses geht es ans Bezahlen per Kreditkarte, die PayPal-Option war bei uns ausgeblendet. 99 Euro und ein paar Minuten Wartezeit später bekommt man eine Mail und ist offiziell Apple-Entwickler. Unter der Adresse developer.apple.com/account findet man ab jetzt den internen Bereich.

Für jeden Typ von digitalen Tickets, aber nicht für jedes einzelne Ticket, brauchen Sie einen sogenannten Identifier, der im internen Bereich hinterlegt ist. Eine Fluggesellschaft bräuchte also für all ihre Flugtickets einen solchen Identifier. Wenn sie über die Wallet auch Essensgutscheine verteilen wollte, müsste sie einen neuen anlegen – und zu jedem Identifier braucht man ein von Apple signiertes Zertifikat. Damit kann man stets beliebig viele Tickets signieren.



Ein Identifier und ein passendes Zertifikat sind die Voraussetzung, um gültige Tickets für die Wallet zu erzeugen. Anlegen kann man sie im Developer-Portal mit einem

kostenpflichtigen Account.
Klicken Sie zum Anlegen eines Identifiers im Entwicklerportal auf „Certificates, Identifiers & Profiles“ und dort unter Identifiers auf das blaue Plus. Sie brauchen ein Objekt vom Typ „Pass Type IDs“. Anschließend geben Sie dem Identifier eine Beschreibung wie „Mein Demoticket“ und denken sich eine eindeutige Bezeichnung in Form einer umgekehrten Domain aus, wir haben zum Test pass.de.heise.ct.demopass gewählt. Das Formular ergänzt den ersten Block pass. automatisch, die Domain müssen Sie auch nicht besitzen – es geht nur darum, einen eindeutigen String zu generieren, den niemand sonst hat. Hat man den Assistenten durchgeklickt, liegt der Identifier bereit und kann mit einem Zertifikat verknüpft werden.

Klicken Sie den Eintrag in der Liste an und wählen dann „Create Certificate“. Der Assistent erwartet von Ihnen einen Namen (nur für Ihre eigene Sortierung) und den Upload eines CSR, eines „Certificate Signing Request“. Das ist eine Datei, die man auf dem lokalen Computer zusammen mit einem geheimen Schlüssel erzeugt. Der Schlüssel bleibt immer auf dem eigenen Gerät, der CSR ist eine schriftliche Bitte, den öffentlichen Schlüssel zu signieren. Als Antwort auf den CSR bekommen Sie von Apple einen signierten öffentlichen Schlüssel zurück.

Am schnellsten kommen Mac-Nutzer an einen passenden CSR (wen wundert es). Sie öffnen das Systemprogramm Schlüsselbundverwaltung und wählen oben links in der Menüleiste
„Schlüsselbundverwaltung/Zertifikatsassistent/Zertifikat einer Zertifizierungsinstanz anfordern …“. Der Assistent hat nicht viele Fragen. Man gibt eine E-Mail-Adresse (wird nicht im Zertifikat eingebaut und ist nicht sichtbar) und einen Namen (Freitext, zum Beispiel „Wallet-Tickets“) ein. Das dritte Feld für die Mailadresse der Zertifizierungsstelle bleibt leer. Anschließend „Auf der Festplatte sichern“ anwählen, den Haken „Eigene Schlüsselpaarinformationen festlegen“ aktivieren und den Assistenten abschließen. Der CSR liegt dann im Dokumente-

Ordner. Der private Schlüssel heißt Wallet-Tickets, liegt im Schlüsselbund und kann dort später exportiert werden, wenn man ihn braucht.

Unter Linux (und unter Windows im WSL) ist es ebenfalls möglich, an einen CSR zu kommen, wenn auch nicht von Apple dokumentiert. Führen Sie einfach folgenden Befehl aus:

```
openssl req -nodes -newkey rsa:2048 -keyout apple_pass.key -
out CertificateSigningRequest.certSigningRequest
```

Die meisten Fragen des Assistenten können Sie überspringen, nur den Ländercode (DE) und die E-Mail-Adresse sollten Sie setzen. Auch bei diesem Verfahren landen die Daten nicht im Zertifikat und werden nicht angezeigt. OpenSSL erzeugt den CSR und den Schlüssel in der Datei apple_pass.key.

Unabhängig vom Betriebssystem schnappen Sie sich am Ende die erzeugte Datei mit dem sperrigen Namen CertificateSigningRequest.certSigningRequest und laden Sie, zurück im Developer-Portal, im Feld für den CSR hoch. Postwendend erhalten Sie eine Datei namens pass.cer mit Ihrem Zertifikat zurück.

Datenstrukturkunde

Ein Pass ist technisch nur eine Zip-Datei mit ein paar verpflichtenden Inhalten. Nach dem Verpacken mit einem Zip-Programm muss man die Dateiendung .zip lediglich durch .pkpass ersetzen und kann sie anschließend verschicken. Um zu verstehen, wie die Tickets funktionieren, erfahren Sie zunächst, welche Dateien im Ordner liegen müssen – im Anschluss erhalten Sie Tipps, wie Sie das Generieren in bestehende Prozesse einbauen können. Denn obwohl man die Pässe theoretisch per Hand zusammenbauen bauen könnte, Spaß macht das nicht.

Alle Dateien, die zu einem Pass verpackt werden sollen, müssen in einem Ordner liegen. In diesen Ordner gehört verpflichtend

eine Datei namens pass.json. Die enthält im JSON-Format alle Texte und Einstellungen. Zunächst sind da ein paar Pflichtfelder:

```
{
 "passTypeIdentifier":
          "pass.de.heise.ct.demopass",
 "serialNumber": "1234567890",
 "formatVersion": 1,
 "organizationName": "c’t magazin"
 "description": "Einladung",
 "teamIdentifier": "<Ihre ID>",
 [...]
}
```

Der passTypeIdentifier ist die Zeichenkette, die Sie zuvor im Developer-Bereich angelegt haben. Die Seriennummer (serialNumber) müssen Sie als Aussteller generieren und sich darum kümmern, dass sie für alle Pässe mit einem Identifier eindeutig ist – mit einer Datenbank im Hintergrund, die Ihre Tickets verwaltet, sollte das kein Problem sein. Vorgaben zum Format gibt es nicht, viele von uns untersuchte Tickets großer Aussteller enthielten in diesem Feld UUIDs [1].

Die formatVersion ist schnell erklärt, dafür ist aktuell nur der Wert 1 zulässig. Die description soll laut Dokumentation keine Inhalte des Tickets (wie den Namen des Inhabers) enthalten. Es handelt sich um eine Beschreibung, die beispielsweise von den Assistenzwerkzeugen sehbehinderter Nutzer vorgelesen werden kann. Den teamIdentifier müssen Sie aus der Developer-Plattform kopieren. Sie finden ihn, indem Sie unter developer.apple.com/account links auf Membership klicken. Es handelt sich um eine zehnstellige Zeichenkette aus Großbuchstaben und Zahlen.

Es folgen auf der obersten Ebene des JSON-Objekts viele freiwillige Angaben, die man auch weglassen kann. Diese bestimmen unter anderen, wie das digitale Dokument aussehen soll. Ans eigene Farbschema passt man das Ticket mit

backgroundColor, foregroundColor und labelColor an. Die Werte müssen wie in CSS als RGB-Farbe angegeben sein, andere Schreibweisen (wie die hexadezimale) sind nicht erlaubt. Ein Eintrag für ein leuchtendes Orange als Hintergrund sieht zum Beispiel wie folgt aus:

```
"backgroundColor": "rgb(255,125,0)"
```

Außerdem kann man auf der obersten Ebene festlegen, wann das Dokument relevant ist, also beim Nutzer automatisch auf dem Sperrbildschirm auftauchen soll. Bei einem Konzertticket könnte das kurz vor dem Einlass sein. Wenn es eine eindeutige Zeit gibt, ist das der einfachste Weg, das Ticket automatisch in den Vordergrund zu rücken. Das Datumsformat muss dem W3C-Standard für Datum und Uhrzeit entsprechen, am einfachsten gibt man die Zeit in UTC an (signalisiert durch das Z am Ende):

```
"relevantDate":"2022-08-10T10:00Z"
```

Was für Eintrittskarten gut funktioniert, ist bei anderen Dokumenten gar nicht so nützlich. In einem Wallet-Pass kann zum Beispiel auch eine Kundenkarte stecken. Für solche hat sich Apple ein besonderes Mittel zur Kundenbindung ausgedacht – für datenschutzbewusste Europäer mag die aber übergriffig wirken, weshalb man sie sparsam einsetzen sollte. Im Pass kann man Geokoordinaten sowie eine Distanz hinterlegen. Nähert sich der Kunde einem Bereich um einen Laden, taucht der Pass mit einem Hinweistext auf. Dabei erhalten Sie als Aussteller keine Benachrichtigung und die Verarbeitung geschieht lokal auf dem Telefon – aber das weiß der datenschutzbewusste Kunde nicht und könnte sich verfolgt fühlen. Technisch funktioniert das wie folgt:

```
"locations": [
 {
 "latitude": 52.3859153,
 "longitude": 9.80959388,
 "relevantText": "Kommen Sie herein!"
```

```
 }
],
"maxDistance": 100
```

Unter locations können Sie bis zu zehn Orte mit ihren Koordinaten hinterlegen, die maxDistance ist der Abstand in Metern. Unterschreitet das Telefon diesen Abstand, erscheint der Pass mit dem unter relevantText angegebenen Werbetext. Haben Sie zu viele Geschäfte, um sie alle unter locations einzutragen, gibt es eine Alternative: Sie können auch Bluetooth-Beacons in den Läden aufhängen und die digitalen Tickets darauf reagieren lassen – die Dokumentation (siehe ct.de/yw3e) verrät, welche Datenfelder dafür vorgesehen sind. Wer es mit solchen Kundenbindungsmaßahmen übertreibt, muss damit rechnen, dass die Kunden die virtuelle Kundenkarte schnell wieder aus der Wallet-App werfen.

Das Rauswerfen funktioniert aber nicht nur manuell, wenn der Nutzer vom Pass genervt ist, sondern auch automatisch, wenn ein Ticket nicht mehr aktuell ist. Gerade Veranstaltungs- und Reisetickets möchte man am Tag darauf nicht mehr in der App sehen (oder höchstens in einer Art Papierkorb). Mit einem expirationDate (im W3C-Datumsformat wie auch das relevantDate) nehmen Sie den Kunden das Aufräumen ab.

Karten für alle Gelegenheiten

Nach diesen verpflichtenden und freiwilligen Angaben müssen Sie sich entscheiden, um welchen Typ digitales Dokument es sich handelt und diesen in der Datei pass.json eintragen (mehr dazu später). Zur Auswahl stehen:

- eventTicket: Eintrittskarte zu einer Veranstaltung
- boardingPass: Ticket für Flüge, Bus- oder Bahnreisen
- coupon: Gutschein oder Rabattcoupon
- storeCard: Kunden- oder Mitgliedskarte
- generic: sonstige digitale Karten

Für Verkehrsunternehmen, Veranstaltungsorganisatoren,

Ladenbetreiber und Fitnessstudios gibt es somit passende Designvorlagen, für alle anderen Dokumente ist generic gedacht. Mit der Wahl eines Typs entscheidet man sich für ein Layout, im Prinzip funktionieren aber alle Typen identisch und unterscheiden sich bei den Funktionen nur in Nuancen. Als Ersteller darf man vier Bereiche mit Texten füllen – in der Infografik auf Seite 156 haben wir die Abschnitte markiert und beschriftet. Im Bereich oben rechts (headerFields) kann man bei einer Veranstaltung zum Beispiel das Datum gut sichtbar hinterlegen. Die Wallet-App simuliert ja eine Brieftasche und stapelt mehrere Tickets hintereinander. Diese Kopfzeile ist immer lesbar und wird nicht von anderen Karten verdeckt.

Die zentralen Informationen, die groß und fett geschrieben werden sollen, liegen in primaryFields und erstrecken sich oben quer über das Ticket. Die nächste Ebene (kleiner dargestellt und mit mehreren Einträgen nebeneinander) heißt secondaryFields, noch kleiner werden auxiliaryFields dargestellt. Die virtuelle Variante der Ticketrückseite heißt bei Apple backFields und ist gedacht für Geschäftsbedingungen und anderes Kleingedrucktes. Angezeigt werden die Daten nur, wenn der Nutzer die drei Punkte oben rechts auf einem Ticket antippt.

Apple hat sich dagegen entschieden, Datenmodelle für allerlei Gelegenheiten mit starren Feldern zu spezifizieren (etwa Datum, Sitzplatz, Start, Ziel, Reisender, Gate, Bahnsteig). Stattdessen kann man in den Bereichen alle Angaben in Schlüssel-Werte-Paaren frei definieren und statt eines Konzerttickets auch eine digitale Kantinenkarte bauen.

Zunächst legt man den gewählten Typ im JSON-Dokument auf der obersten Ebene als Objekt an, darunter Objekte für die Felder, die man nutzen möchte (primaryFields, secondaryFields …). Sie sind allesamt optional. In den Feldern platziert man seine Inhalte jeweils mit einem Schlüssel (key), einer Beschriftung (label) und dem Wert (value). Das Label steht dann im fertigen Pass über oder unter dem Wert.

Bei einem Veranstaltungsticket für eine fiktive Grillfeier mit Freunden kann das zum Beispiel folgendermaßen aussehen:

```
"eventTicket": {
 "headerFields": [
  {
   "key": "seat",
   "label": "SITZPLATZ",
   "value": "Bierbank 1"
  }
 ],
 "primaryFields": [
  {
   "key": "event",
   "label": "VERANSTALTUNG",
   "value": "Grillfeier mit Freunden"
  }
```

```
 ],
 "secondaryFields": [
  {
   "key": "location",
   "label": "ORT",
   "value": "Garten"
  }
 ],
 "auxiliaryFields": [
 {
   "key": "food",
   "label": "MITBRINGEN",
   "value": "Nudelsalat"
  }
 ],
 "backFields": [
  {
   "key": "terms",
   "label": "Bedingungen",
   "value": "Bitte bis 17:00 absagen"
  }
 ]
}
```

Bei der Vergabe der Schlüsselnamen ist man frei, sie müssen nur einmalig sein. Falls Sie zufällig in die Verlegenheit kommen sollten, Tickets für ein Reiseunternehmen zu programmieren, gibt es noch eine Besonderheit. Sobald Sie das Objekt boardingPass angelegt haben, müssen Sie darin verpflichtend einen transitType angeben. Im Ticket erscheint dann zwischen den beiden primären Informationen in primaryFields ein passendes Icon. Ein Ausschnitt aus einem Flugticket kann zum Beispiel wie folgt aussehen:

```
"boardingPass": {
  "transitType": "PKTransitTypeAir",
  "primaryFields": [
   {
    "key": "from",
    "label": "VON",
    "value": "HAJ"
```

```
   },
   {
    "key": "to",
    "label": "NACH",
    "value": "LYR"
   }
  ]
}
```

Die Buchstaben PK stehen für PassKit, so heißt das Framework für die Tickets und auch für den Zugriff auf Apple Pay. Neben TypeAir gibt es noch TypeBoat, TypeBus, TypeGeneric und TypeTrain.

Codes und Bilder

Sind all diese Werte ausgefüllt, gibt es noch zwei weitere optionale Aufgaben. Auf der einen Seite sind das die Bilddateien für Logos. Dabei kann (muss aber nicht) sich ein Grafiker genauso austoben wie bei den Favicons für Websites und noch Varianten für unterschiedlich große Bildschirme erzeugen (mit @2x am Ende des Dateinamens). Die Arbeit fällt pro Unternehmen nur einmal an. In der Tabelle auf Seite 158 sehen Sie, welche Bildchen Sie anlegen und in den Ordner neben die pass.json legen können. Alle Bildchen sind optional.

Letzte Baustelle ist der Code, mit dem Sie die Echtheit des Dokuments prüfen. Das kann ein Barcode sein, ein QR-Code oder auch die NFC-Schnittstelle des Mobiltelefons. Für letztere Technik ist zusätzlicher Zertifikatsaufwand nötig, dazu sei auf die Dokumentation verwiesen (siehe ct.de/yw3e). Bar- und QR-Codes dagegen sind schnell eingebunden und gehören auf die oberste Ebene im JSON-Objekt. Sie sind wie die meisten Felder optional:

```
barcodes": [
 {
  "altText": "123 Mustermann",
  "format": "PKBarcodeFormat",
  "messageEncoding": "iso-8859-1",
```

```
  "message": "123MUSTERMANN"
 }
]
```

Die Wahl des Formats hängt vor allem von Ihrer bestehenden Leser-Infrastruktur ab. In einen QR-Code passen die meisten Daten, neben PKBarcodeFormatQR sind auch FormatPDF417 und FormatAztec vorgesehen. Apple verweist darauf, dass man heutzutage unter dem Schlüsel barcodes eine Liste mit potenziell mehreren Einträgen anlegen soll. Ab iOS 9.0 wird diese Schreibweise verwendet. Früher legte man einen einzelnen Barcode unter barcode ab. Das ist seit dem Start von iOS 9.0 offiziell abgekündigt und wäre nur noch für iOS 8 und noch ältere Systeme nötig. Bei unseren Tests fanden wir etwa bei einem Ticket der Lufthansa aus dem Jahr 2022 ausschließlich den alten Eintrag barcode im Singular.

Bilddateien für Logos und Hintergründe		
Dateiname	Zweck	Format[1]
background.png	Großflächiges Hintergrundbild	180 × 220
footer.png	Kleiner Streifen über dem Barcode	286 × 15

Bilddateien für Logos und Hintergründe		
Dateiname	Zweck	Format[1]
icon.png	Quadratisches Logo, wenn das Ticket auf dem Home-Screen angezeigt wird	29 × 29
logo.png	Logo des Unternehmens, wird oben links neben dem headerFields angezeigt	160 × 50 (oder schmaler)
strip.png	Zusätzlicher Hintergrund für den Bereich primaryFields	375 × 123
thumbnail.png	Zusätzliches Logo, wird bei Veranstaltungstickets auf der Vorderseite rechts dargestellt	90 × 90
[1] In Pixeln. Zusätzlich kann man alle Bilder für hochauflösende Bildschirme noch in hochskalierten Varianten anlegen und die Dateinamen mit @2x.png kennzeichnen.		

Zur Prüfung

Die Datei pass.json und die Bildchen liegen im Ordner, damit ist das Ticket fast fertig zum Verpacken. Eine letzte verpflichtende Datei fehlt aber noch. Sie heißt manifest.json und dient der Signaturprüfung. Dafür enthält sie ein Inhaltsvezeichnis aller Dateien im Ordner im JSON-Format. Stark gekürzt sieht sie zum Beispiel so aus:

```
{
  "pass.json": "74342dc0649fc1 [...]",
  "icon.png":  "e0f0bcd503f611 [...]",
  "logo.png":  "66a0989dcf0c5c [...]",
  [...]
}
```

Jede Datei, die zum Pass gehört, bekommt hier einen Eintrag mit ihrem Dateinamen und dem SHA1-Hash ihres Inhalts. Die Idee dahinter: Beim Verpacken erzeugt der Ersteller mithilfe seines Apple-Zertifikats für diese Manifest-Datei eine Signatur im Format „PKCS #7 Detached“, das zum Beispiel auch bei E-Mails mit S/MIME zum Einsatz kommt. Die erzeugte Signatur legt er mit dem Dateinamen signature mit in den Ordner. Beim Laden vollzieht die Wallet-App auf dem Telefon diese Schritte zum Test einmal nach und bildet ebenfalls alle Hash-Werte aller Dateien. Hätte zwischendurch jemand eine der Dateien auch nur um ein Bit manipuliert, wäre schlagartig ihr SHA1-Hash ungültig, dadurch die Manifest-Datei und schließlich auch die Signatur.

Auch Reisetickets und Kundenkarten finden in der Wallet-App

ihren Platz.
Den gesamten Signaturprozess darf man aber nicht überbewerten – er stellt letztlich nur sicher, dass ein registrierter Entwickler, der den passTypeIdentifier bei Apple angelegt hat, das Ticket mit seinem Schlüssel signiert hat. Am Einlass beim Konzert oder am Flughafen sagt das aber überhaupt nichts aus, den Identifier sieht das Kontrollpersonal nicht einmal und die Authentifizierung erfolgt lediglich über den QR- oder Barcode. Jeder mit Apple-Account kann Wallet-Pässe basteln und signieren, die wie Bahn- oder Lufthansa-Tickets aussehen. Herausfinden kann man den wahren passTypeIdentifier nur, wenn man den Pass in Ruhe auf einem PC untersucht.

Daraus folgt auch ein ganz legaler Praxistipp für Entwickler, die eigene Pässe bauen und sich inspirieren lassen wollen: Sie sollten einen Pass eines bekannten Anbieters auf dem Telefon öffnen, oben rechts auf die drei Punkte klicken und ihn sich per AirDrop oder Mail an den PC schicken. Dort ändert man einfach die Dateiendung .pkpass in .zip und entpackt das Archiv. Auf diese Weise lässt sich erfahren, wie die großen Anbieter ihre Pässe bauen.

Vom Fließband

Mit diesen Erklärungen und etwas Recherche in bestehenden Tickets sind Sie in der Lage, eigene Tickets und Karten für viele Gelegenheiten zu gestalten. Erklärungen zu allen Funktionen, die Apple sonst noch in den Passes versteckt hat, finden Sie in der Dokumentation über ct.de/yw3e. Nützlich für einige Szenarien, wenn auch nicht mal eben eingerichtet, sind die Themen Mehrsprachigkeit und Updates über einen Server – wie Sie letztere Funktion zum Laufen bringen, würde den Umfang dieses Artikels deutlich sprengen. Bevor Sie sich an solche Herausforderungen machen, sollten Sie Ihren ersten gültigen und signierten Pass erzeugen.

Wir empfehlen dringend, den Signaturprozess mit der Manifest-Datei nicht per Hand durchzuspielen. Die Debugging-

Möglichkeiten sind auf den ersten Blick begrenzt. Entweder ein Ticket ist gültig oder das Telefon weigert sich mit einer nichtssagenden Fehlermeldung. Wer ohnehin schon im Apple-Universum entwickelt, kommt mit dem iOS-Simulator von XCode immerhin an detailliertere Fehlermeldungen im System-Log.

Machen Sie sich das Leben einfacher und suchen Sie nach einer Apple-Wallet-Bibliothek in der Programmiersprache Ihres Vertrauens und erzeugen Pässe lieber programmatisch. Die Bibliotheken funktionieren alle ähnlich: Sie erwarten den privaten Schlüssel und das Zertifikat. Im Programmcode hinterlegt man statische Werte, die bei allen Tickets identisch sind, als Vorlage. Die dynamischen Inhalte (ID, Reisedatum, Name des Reisenden …) werden dann zur Laufzeit eingebacken. Heraus fällt eine verpackte und signierte pkpass-Datei.

Über ct.de/yw3e finden Sie eine Sammlung mit Bibliotheken für verschiedene Programmiersprachen. Für private Experimente kann man anhand der Dokumentationen und mit Kenntnis der jeweiligen Sprache schnell einen Prototypen zusammenstricken. Im Unternehmenseinsatz ist das Generieren solcher Tickets ein Musterbeispiel für den Einsatz eines Microservices – zum Beispiel in Form eines kleinen Containers, der intern ein HTTP-API anbietet und von einem anderen System (das Buchungen verarbeitet) die variablen Ticket-Daten als JSON-Daten annimmt. Zurück liefert der Microservice einen fertigen Pass. Wenn Sie sich für eine solche Umsetzung interessieren, werfen Sie mal einen Blick auf unser Repository zum Artikel – da haben wir einen solchen Microservice als Docker-Container zusammengebaut. Übergeben müssen Sie dem Container nur Ihr Zertifikat und Ihren privaten Schlüssel.

Fazit

Mit seiner Wallet-App und dem eigenen Dateiformat hat Apple ein echtes Alltagsproblem gut und recht flexiblel gelöst. Leider gilt dasselbe wie bei Apps in der Mobilgeräte-Welt:

Möchte man die Android-Nutzer nicht ausschließen, muss man wohl oder übel verschiedene Pässe erzeugen. Apple und Google gehen in diesem Bereich getrennte Wege, statt Standards zu vereinbaren.

Hat man die Hürde mit Entwickler-Account und Zertifikat überwunden, ist der Rest der Arbeit einfaches JSON-Handwerk. Beim Datenformat gilt dankenswerterweise: Vieles kann, wenig muss. Um ein Grundgerüst zu einem Pass zu verschnüren, sollte man dann zu einer Softwarebibliothek in der Sprache des Vertrauens greifen. So steht eigenen digitalen Tickets nichts mehr im Weg. *(jam@ct.de)*

1. Literatur
2. Jan Mahn, Zufall schlägt das System, Ein Plädoyer für UUIDs in Datenbanken, c't 6/2022, S. 138

Dokumentation und Beispiel-Container: ct.de/yw3e

Texte auszeichnen mit Markdown

Überschrift

Mit Markdown schnell und einfach Texte auszeichnen

Ob Blog-Einträge, Kommentare in Foren oder Bugtracker auf Entwicklungsplattformen – immer mehr Software unterstützt Markdown zum Auszeichnen von Texten. Nach unserer Einführung

wissen Sie nicht nur, warum der Überschrift ein # voransteht, sondern auch, wie Sie Textpassagen kursiv stellen, Aufzählungen und Tabellen eintippen und vieles mehr.

Von Sylvester Tremmel

kompakt

- GitHub, Reddit, Trello – zahllose Systeme verstehen Markdown; unsere Einführung erklärt die weit verbreitete Auszeichnungssprache.
- Markdown zu schreiben geht schnell und fällt leicht; wer die Sprache beherrscht, nutzt sie oft auch für die eigenen Texte und Notizen.
- Auch in kollaborativen Projekten wird dadurch niemand ausgeschlossen, lesbar sind Markdown-Texte ohne Kenntnis der Sprache und in jedem beliebigen Texteditor.

Mit Markdown ergänzt man reinen Text leicht um Formatierungsinformationen, die eine visuell schöne Darstellung erlauben. Der Clou: Markdown-Texte sind nicht nur bequem zu schreiben, sondern auch im Quelltext gut lesbar. Dadurch benötigt man keine Textverarbeitung wie Microsoft Word oder LibreOffice Writer. Jeder beliebige Texteditor eignet sich, um Markdown zu verfassen und zu lesen. Die schöne Darstellung durch passende Software ist ein Bonus fürs Endergebnis, keine Voraussetzung beim Arbeiten an den Texten.

Weil Markdown so praktisch ist, kennen mittlerweile alle möglichen Systeme die Sprache: zahlreiche Notiz-Apps wie etwa „Drafts“ [1] oder „Obsidian“ [2]; komplexe Systeme zum Schreiben von Texten wie „Notion“ [3] oder „HedgeDoc“ [4] und Nischenanwendungen wie die Rezeptdatenbank „Tandoor Recipes“ [5]. Große Serveranwendungen wie GitHub oder GitLab und viele Systeme für Internetforen erlauben ebenfalls, die eigenen Beiträge und Nachrichten mit Markdown auszuzeichnen. Und in seinem ursprünglichen Zweck – dem Schreiben von Texten zur Publikation im Internet – glänzt Markdown ebenfalls: Zahllose

Blogging-Systeme, Website-Editoren [6] und Dokumentations-Generatoren unterstützen die Sprache.

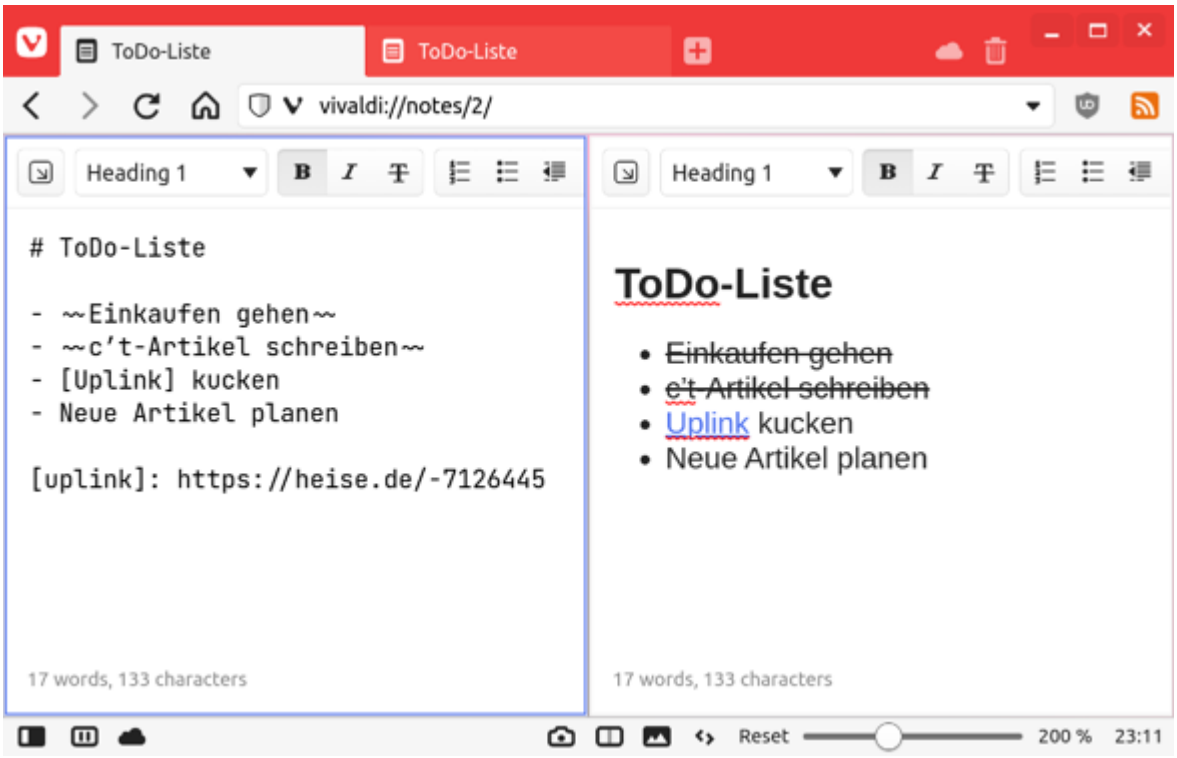
Die weite Verbreitung hat leider den Nebeneffekt, dass diverse Varianten der Sprache existieren (siehe Kasten). Die grundlegenden Features funktionieren aber überall gleich (oder zumindest sehr ähnlich) und was diese Einführung zeigt, sollte in den meisten Markdown-Implementierungen problemlos funktionieren. Der Text orientiert sich grob an CommonMark, weist aber auch darauf hin, wenn es andernorts nette Erweiterungen gibt oder etwas nicht ganz gleich funktioniert.

Pandoc's GitHub-flavoured CommonMark?

Nicht überall, wo „Markdown" draufsteht, ist das gleiche Markdown drin. Die ursprüngliche Version der Sprache wurde von John Gruber und Aaron Swartz aus der Taufe gehoben, um damit Artikel fürs Web zu schreiben. Mittlerweile findet Markdown allerdings in allen möglichen Systemen Verwendung und die immer neuen Einsatzzwecke luden zu allerlei Erweiterungen der Sprache ein. Hinzu kam, dass Grubers Dokumentation der Markdown-Syntax (alle Links unter ct.de/y5hr) an einigen Stellen nicht ganz eindeutig ist oder von seiner Referenzimplementierung abwich.

Manche der entstandenen Varianten sind kaum dokumentierte Ad-hoc-Ideen von den Autoren der jeweiligen Software, andere – wie etwa „GitHub Flavored Markdown" oder „Pandoc's Markdown" – sind weit verbreitete und sauber spezifizierte Erweiterungen der Sprache. Den Wildwuchs wieder einhegen soll „CommonMark", eine erweiterte und präzisierte Markdown-Spezifikation. Das funktioniert nicht ganz: Die CommonMark-Spezifikation sollte möglichst kompatibel zu bereits existierenden Praktiken sein und geriet daher teilweise recht komplex. Infolgedessen weichen verschiedene Markdown-Implementierungen in Details von CommonMark und auch voneinander ab. Außerdem gibt es weiterhin viele Features, die über CommonMark hinausgehen und von System zu System unterschiedlich funktionieren.

Ungeachtet dieser Einschränkungen ist CommonMark viel wert, weil es eine relativ verlässliche Basis darstellt: Wer die dort spezifizierten Features kennt und nicht auf abstruse Weise miteinander kombiniert, der hat mit jeder vernünftigen Markdown-Implementierung Freude. Und wenn ab und an eine Kleinigkeit auf dem jeweiligen System nicht funktioniert, weiß der erfahrene Markdown-Autor, das Problem zu umschiffen. Je nach Anwendungsfall und Bedarf kann man dann immer noch nachschlagen, welche über CommonMark hinausgehenden Möglichkeiten die jeweilige Software bietet.



Markdown kann man an den verschiedensten Stellen nutzen, hier verschönert es den Inhalt der Notizen-Funktion im Browser Vivaldi.

Jeder Text ist Markdown

Markdown zu schreiben fällt grundsätzlich leicht, weil jeder Text Markdown ist – ungültige Syntax gibt es nicht. Wenn ein Markdown-Textabschnitt nicht anderweitig interpretiert werden kann, dann ist er eben genau das: ein Textabschnitt, genauer gesagt ein Absatz:

Ein Absatz in Markdown

Und noch einer, der sich über
zwei Zeilen erstreckt.

Einfache Zeilenumbrüche behandelt Markdown wie Leerzeichen, sodass man den Quelltext auch manuell umbrechen kann – wie beim zweiten Absatz in diesem Beispiel –, ohne dass diese Umbrüche die Ausgabe beeinflussen. Um einen neuen Absatz zu beginnen – der auch in der Ausgabe als neuer Absatz gerendert wird –, muss man eine Leerzeile einfügen – was auch im Texteditor deutlicher ist.

Um einen Zeilenumbruch auch in der Ausgabe zu produzieren, reicht es, im Markdown-Text die vorhergehende Zeile mit einem Backslash oder mehr als einem Leerzeichen zu beenden:

Ein Absatz mit einem\
Zeilenumbruch und␣␣
noch einem.

Um einen neuen Textabschnitt einzuleiten, schreibt man drei Sternchen (***), Bindestriche (---) oder Unterstriche (___). Markdown interpretiert dergleichen als „thematischen Bruch“, den die meisten Systeme als horizontale Linie rendern. Wer mag, darf auch mehr Zeichen setzen oder sie mit Leerzeichen auflockern:

****

- - - -

Zweierlei Überschriften

Um eine Textzeile als Überschrift zu markieren, stellt man ihr ein oder mehrere Doppelkreuze (#) und ein Leerzeichen voran. Die Anzahl der Doppelkreuze (maximal sechs) gibt die Ebene der Überschrift an:

Überschrift

Unterüberschrift

Überschriften dürfen auch mit Doppelkreuzen enden, was manche Autoren schöner finden:

```
### Unterunterüberschrift ###
```

Markdown ist das egal, es ignoriert Doppelkreuze am Ende einfach und achtet auch nicht darauf, ob ihre Anzahl zur Zahl der öffnenden Zeichen passt.

Übrigens hilft ein Backslash, wenn Markdown ein Zeichen interpretiert, das einfach Textinhalt sein soll:

```
\# Normaler Text, beginnt mit #

# Überschrift, endet mit \#
```

Daneben kennt Markdown noch eine zweite, sehr augenfällige Syntax für Überschriften:

```
Überschrift
==========

Unterüberschrift
----------------
```

Solche Überschriften nennt man Setext-Überschriften, nach einem Textauszeichnungssystem von 1991, aus dem die Syntax übernommen wurde. Setext-Überschriften sehen zwar im Texteditor schön aus, sind aber eher mühsam zu tippen. Markdown begnügt sich zwar auch mit nur einem einzelnen Gleichheitszeichen oder Bindestrich (oder jeder anderen Anzahl), allerdings geht dann schnell die bessere Optik verloren. In jedem Fall kann man mit dieser Syntax nur zwei Überschrift-Ebenen auszeichnen.

Syntax für Faule

Bei einem anderen Feature lehnt sich die Markdown-Syntax ebenfalls an Bekanntes an: Zitate leitet man – wie in E-Mails – mit Größer-als-Zeichen ein. Auch das Verschachteln funktioniert:

```
> Zitat, das sich über
> mehrere Zeilen
> erstreckt.
>
>> Unter-Zitat mit
>> zwei Zeilen und einer
>>
>> # Überschrift
```

Die Leerzeilen vor dem (Unter-)Zitat und der Überschrift dürfen laut CommonMark-Standard entfallen, aber manch andere Markdown-Implementierung besteht darauf. Grundsätzlich hilft es bei unerwarteten Ergebnissen oft, Elemente mit Leerzeilen zu trennen.

Wer seinen Text manuell umbricht, muss allerdings nicht jeder Zeile einzeln ein > voranstellen. „Markdown erlaubt Dir faul zu sein“, steht schon in der originalen Dokumentation von John Gruber. Bei Zeilen, die nur den aktuellen Absatz fortsetzen, darf man auf die Markierung verzichten. Das folgende Codebeispiel hat daher die gleiche Bedeutung wie das vorhergehende:

```
> Zitat, das sich über
mehrere Zeilen
erstreckt.
>
>> Unter-Zitat mit
zwei Zeilen und einer
>>
>> # Überschrift
```

Ebenfalls kaum gewöhnungsbedürftig – und ebenfalls mit einer eingebauten Abkürzung für Faule – ist die Art und Weise, wie Markdown Listen auszeichnet. Man stellt dem Text für einen Listeneintrag schlicht einen Listenmarker voran. Die Sprache erlaubt dafür Sternchen, Bindestriche oder Plus-Zeichen für unnummerierte Listen und Zahlen mit Punkten für nummerierte Listen:

```
* Listenpunkt
* noch ein Listenpunkt
* und ein weiterer

1. Eins
2. Zwei
3. Drei
```

Statt dem Punkt nach einer Zahl darf man auch eine Klammer setzen (1), 2), …). Übrigens beachtet Markdown nur die erste Zahl einer nummerierten Liste. Man kann also auch drei Punkte mit 3., 10. und 07. nummerieren und erhält als Ausgabe eine Liste, die 3., 4., 5. hochzählt. Das hilft, wenn Listenpunkte immer wieder an neue Positionen wandern: Man nummeriert einfach jeden Punkt mit 1. und Markdown kümmert sich darum, dass am Ende eine ordentliche Aufzählung herauskommt.

Andere Zählvarianten kennt CommonMark nicht, aber viele Markdown-Implementierungen erlauben auch römische Zahlen (i., ii., …), Buchstaben (A), B), …) oder vollständige Umklammerungen ((a), (b), …). Was funktioniert, kann man einfach von Fall zu Fall ausprobieren.

Eine ebenfalls häufig verfügbare Ergänzung zu CommonMark sind Aufgabenlisten. Dafür folgen auf den Listenmarker zwei eckige Klammern, die ein Kästchen andeuten. Erledigte Einträge erhalten ein X in ihrem Kästchen:

```
- [ ] Aufgabe 1
- [x] Aufgabe 2
- [ ] Aufgabe 3
```

Bei der Ausgabe werden dann statt der Klammern ordentliche Kästchen und Häkchen angezeigt.

Wenn ein Listeneintrag mehrere Zeilen umfassen soll, dann rückt man die Folgezeilen einfach passend ein. Über Einrückungen werden Listen auch verschachtelt:

```
+ Listenpunkt und
+ ein langer Listenpunkt,
```

```
  der über mehrere
  Zeilen geht
+ Noch ein Punkt
  1. Ein Unterpunkt
  2. und noch einer
     > mit einem Zitat

     im Listenpunkt
```

Wie erwähnt ist die Leerzeile vor dem Zitat laut Standard optional, wird aber von so manchem System verlangt. Die Leerzeile danach ist in jedem Fall nötig, weil Markdown sonst eine „faule“ Zitatfortsetzung erkennt.

Die genauen Regeln für die Tiefe von Einrückungen sind aus mehreren Gründen sehr kompliziert. Auf der sicheren Seite bleibt, wer Einrückungen so wählt, dass alle Marker einer Liste untereinander liegen und auch der Text jeder Zeile auf Linie beginnt – also so, wie es oben beim zweiten Listenpunkt und zweiten Unterpunkt der Fall ist.

Wie erwähnt ist auch bei Listenpunkten Faulheit gestattet und man kann die Einrückung komplett weglassen. Das funktioniert aber nicht für Überschriften und dergleichen, sondern nur, wenn eine Zeile schlichten Text aus der Zeile darüber fortsetzt:

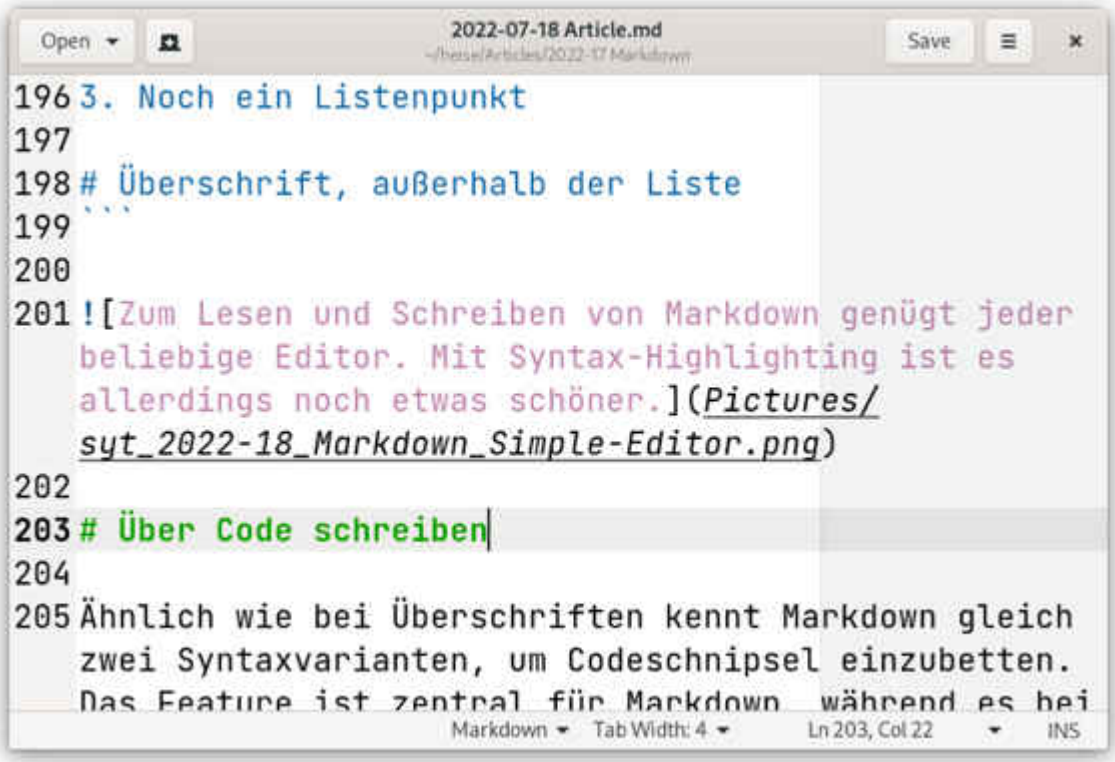
```
1. Ein langer Listenpunkt,
über zwei Zeilen.

2. Ein Listenpunkt mit

   # integrierter Überschrift

3. Noch ein Listenpunkt

# Überschrift, außerhalb der Liste
```



Zum Lesen und Schreiben von Markdown genügt jeder beliebige Editor. Mit Syntax-Highlighting ist es allerdings noch etwas schöner.

Über Code schreiben

Ähnlich wie bei Überschriften kennt Markdown gleich zwei Syntaxvarianten, um Codeschnipsel einzubetten. Das Feature ist zentral für Markdown, während es bei anderen Textverarbeitungen und Auszeichnungssprachen eher ein Nischendasein fristet. Die Sprache kommt häufig in der Softwareentwicklung zum Einsatz und Programmierer müssen eben allenthalben Code dokumentieren, kommentieren oder publizieren.

In der ersten und simpleren Variante rückt man Codeschnipsel einfach vier Leerzeichen weit ein. Den Inhalt eines Codeblocks fasst Markdown nicht an, sodass man dort nach Herzenslust #, * und alle anderen Zeichen verwenden kann:

```
    Codezeile
    Noch eine Codezeile
```

```
    # Keine Überschrift, sondern
    # ein Kommentar im Code
```

Eingerückte Code-Blöcke sind der Grund, warum man die meisten anderen Markdown-Elemente (wie Zitate, Überschriften et cetera) zwar mit Leerzeichen einrücken darf, wenn man will, aber höchstens drei Leerzeichen weit. Rückt man ein Element vier Leerzeichen weit ein, macht Markdown daraus einen Codeblock.

Überhaupt wird es schnell unübersichtlich, wenn man eingerückte Codeblöcke mit Elementen wie Listenpunkten kombiniert, die ebenfalls Einrückungen erfordern. Man kann solche Codeblöcke durchaus in Listen verschachteln und mit anderen Listeninhalten mischen, aber beim Schreiben artet das rasch in mühsames Leerzeichen-Abzählen aus.

Hier hilft die zweite Syntax für Codeschnipsel, die Codeblöcke nicht einrückt, sondern oben und unten mit expliziten Zeichen umzäunt („fenced code blocks“). So ein Zaun besteht aus drei oder mehr Gravis (`, oft auch „Backticks“ genannt) oder Tilden (~):

````
```
Codezeile
Noch eine Codezeile

# Keine Überschrift, sondern
# ein Kommentar im Code
```
````

Der abschließende Zaun muss mindestens so lang sein wie der öffnende. In aller Regel schreibt man sie gleich lang; diese Regel dient aber dazu, Codezeilen mit zum Beispiel drei Gravis im Codeblock zu erlauben, ohne dass sie fälschlicherweise den Codeblock abschließen: Man nutzt dann einfach vier oder mehr Gravis als Zaun – oder eben Tilden.

Umzäunte Codeschnipsel haben noch einen weiteren Vorteil gegenüber ihren eingerückten Pendants: Sie ermöglichen

sogenannte Info-Strings. Das sind Metadaten zum Codeblock, die man direkt nach dem öffnenden Zaun in dieselbe Zeile schreibt. Der Inhalt dieser Metadaten hängt vom konkreten System ab, für das der Markdown-Text verfasst wird. In aller Regel ist das erste (und oft einzige) Wort der Name der Programmiersprache, die im Codeschnipsel zum Einsatz kommt. Das dient zum Beispiel dazu, ein passendes Syntax-Highlighting zu aktiveren:

```
```javascript
alert('Hello World!');
```
```

Wer statt einem ganzen Codeblock nur schnell ein paar Wörter im Fließtext als Code markieren will, kann sie einfach links und rechts in je einen oder mehrere Gravis einschließen. Tilden funktionieren dafür nicht. Wenn der markierte Code selbst eine Folge von Gravis enthält, dann nutzt man zum Umfassen schlicht eine Anzahl an Zeichen, die nicht im Code als Sequenz auftritt (und trennt sie, falls nötig, mit Leerzeichen vom Inhalt):

```
Ein Text mit `Code`,
etwas ``Code samt ` Gravis`` und
nur einem Doppelgravis: ` `` `.
```

Fett formatiert

Ganz ähnlich wie kurze Codepassagen kann man Textstellen kursivieren und fetten, indem man sie mit einfachen beziehungsweise doppelten Sternchen oder Unterstrichen umgibt:

```
*Kursive* und **fette** Wörter,
sowie __fette__ und _kursive_.
```

Kursivierung und Fettung sind dabei lediglich die üblichen Darstellungsformen, die Auszeichnungen bedeuten eigentlich „betont“ und „stark betont“, was man sogar verschachteln darf:

```
Normal, _kursiv und **fett-kursiv**_.
Auch ***fett-kursiv***.
```

Etwas kompliziert werden die Regeln, wenn die Auszeichnungen nicht an Leerzeichen enden. Um einen Teil eines Wortes zu kursivieren, eignen sich zum Beispiel nur Sternchen (Wort*teil*kursivierung). Unterstriche funktionieren hier nicht, damit Markdown nicht häufige Konstruktionen wie Dateinamen mit Unterstrichen versehentlich auszeichnet. Wenn es zu einer falschen Auszeichnung kommt, hilft wieder der Backslash:

```
Ein Name_mit_Unterstrichen und
ein Name\*mit*Sternchen.
```

CommonMark spezifiziert keine weiteren solchen Formatierungen. Allerdings gibt es wieder einige Ergänzungen, bei denen es sich lohnt, einfach auszuprobieren, ob ein System sie unterstützt: Mitunter kann man mit einfachen Tilden Text tief- (~1~) und mit Zirkumflexen hochstellen (^2^). Recht häufig markieren doppelte Tilden Text als gelöscht; er wird dann durchgestrichen angezeigt. Manche Systeme erlauben auch, Text mit doppelten Gleichheitszeichen hervorzuheben. Er bekommt dann etwa einen gelben Hintergrund:

```
Text mit einer ~~Löschung~~ und
einer ==Hervorhebung==.
```

Links und verlinkte Bilder

Links setzt man in Markdown mit einer Reihe von Syntaxvariationen, die aus Klammern bestehen. Eine Möglichkeit ist, den zu verlinkenden Text in eckige und das Linkziel in runde Klammern zu setzen:

```
Webseite des [Magazins für
Computertechnik](https://ct.de).
```

Was man als Linkziel notiert, ist Markdown egal. Häufig handelt es sich um URLs oder Dateipfade – was in der Ausgabe funktioniert, hängt vom jeweiligen System ab. Zusätzlich zum Ziel kann man auch einen Link-Titel angeben. Den schreibt man einfach, von (mindestens) einem Leerzeichen getrennt, dahinter

und fasst ihn in Anführungszeichen oder runde Klammern ein:

```
[Linktext](Linkziel "Linktitel")
```

Bei einer Ausgabe als HTML-Code dient der Linktitel als Inhalt des title-Attributes des Links.

Linkziel und -titel direkt nach dem verlinkten Text anzugeben kann unübersichtlich werden, besonders wenn man sehr viele Links oder Links mit sehr langen URLs in einen Text einbettet. Abhilfe schaffen Referenzenlinks, die nach dem verlinkten Text nur ein kurzes Label angeben. Um es von einem Linkziel zu unterscheiden, notiert man das Label in eckigen statt runden Klammern.

Irgendwo anders im Markdown-Dokument (auch davor) definiert man eine passende Linkreferenz. Die wiederholt das Label (ebenfalls in Klammern) und gibt nach einem Doppelpunkt das Linkziel und den optionalen Titel an:

```
Webseite des [Magazins für
Computertechnik][CT].

[CT]: https://ct.de "c’t-Website"
```

Wenn das Label mit dem Linktext übereinstimmt, darf man es auch weglassen und die Referenz funktioniert trotzdem; die eckigen Klammern des Labels sind dann optional. Praktischerweise ignoriert Markdown Groß- und Kleinschreibung bei der Label-Zuordnung:

```
Webseiten der [ct][] und von [heise].

[CT]: https://ct.de
[Heise]: https://heise.de
```

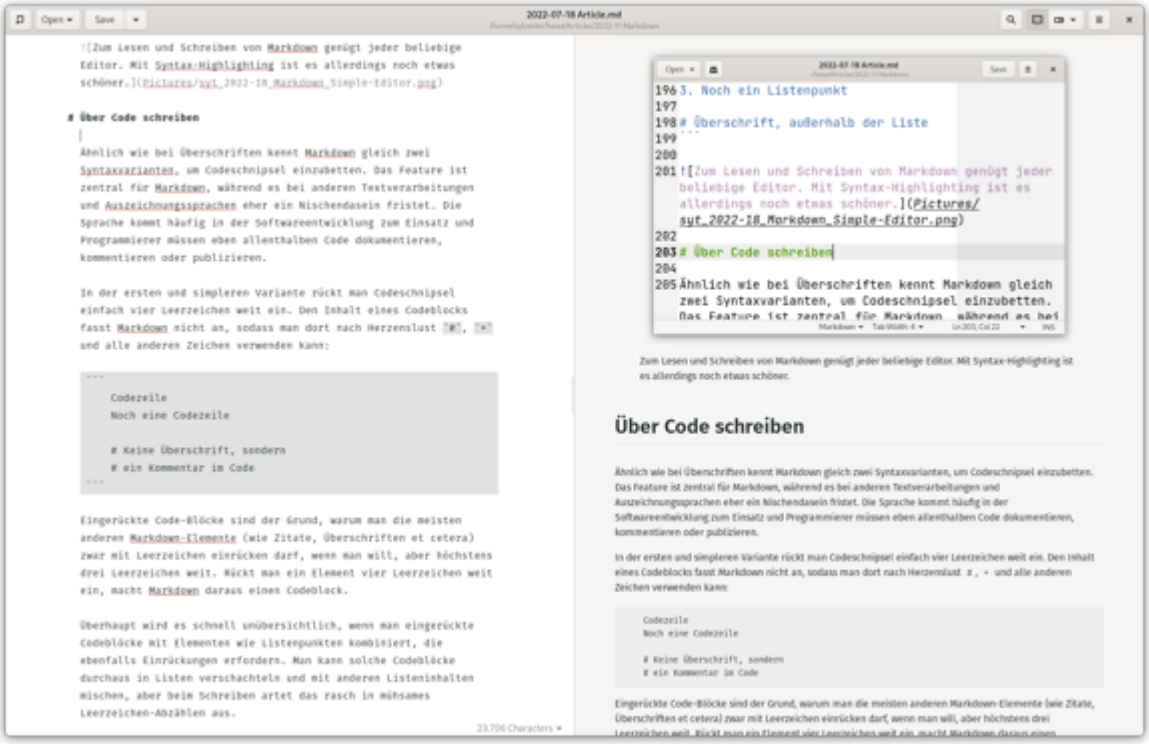
Als letzte Linkvariante gibt es noch eine Syntax für den Fall, dass Linktext und -ziel identisch sind. Um dann nicht https://ct.de schreiben zu müssen, kann man auch einfach das Linkziel in spitze Klammern setzen: <https://ct.de>. Einige Markdown-Systeme erfordern nicht

einmal das und verlinken automatisch alles, was sie als URL erkennen.

Eng verwandt mit Links sind Bilder – zumindest aus Markdown-Sicht: Eine Bilddatei kann man nicht sinnvoll in eine Textdatei einbetten und muss sie daher wie ein Linkziel referenzieren. In Markdown geschieht das über dieselbe Syntax, der man lediglich ein Ausrufezeichen voranstellt:

```
![Beschreibung](Pfad/zum/Bild-1.png)
```

Mit der Syntax von Referenzenlinks funktioniert das ebenso, nur die Variante mit spitzen Klammern gibt es nicht für Bilder. Anstelle des Linktexts steht eine Bildbeschreibung. Üblicherweise wird die als Alt-Text des Bildes ausgegeben, sollte also den Bildinhalt erklären. Allerdings weichen einige Markdown-Systeme davon ab und geben Bilder, die für sich alleine in einer Zeile stehen, anders aus. Die Beschreibung rendern diese Systeme dann als Bildunterschrift. Wieder probiert man am besten einfach aus, wie das jeweilige System diesen Fall handhabt.



Wer lange Texte in Markdown schreibt, sollte sich darauf spezialisierte Editoren ansehen. Die können – wie hier das

Programm „Apostrophe“ – zum Beispiel die layoutete Vorschau neben dem Markdown-Quelltext anzeigen.

HTML einbetten?

Das deckt die wesentlichen Aspekte von Markdown und CommonMark ab – bis auf einen. Wie eingangs erwähnt, war Markdown ursprünglich (nur) dafür gedacht, Texte für das Web zu verfassen. Der Output einer Markdown-Implementierung sollte daher HTML sein und schon im Eingabetext vorhandenes HTML konnte die Software einfach durchreichen. Das ist im Grunde immer noch der Fall; wer HTML beherrscht, kann es einfach im Markdown-Text notieren:

```
<div class="test">

*Kursiver Text*

</div>
```

Ob das Ergebnis wie erwünscht ausfällt, ist allerdings eine andere Frage. Zwar produzieren die meisten Markdown-Anwendungen tatsächlich HTML (zumindest als Zwischenschritt), aber häufig filtern sie ihre Eingabe – etwa aus Sicherheitsgründen – und man kann keine (beliebigen) HTML-Tags in das Ergebnis schleusen.

Außerdem sind die genauen Regeln zum Mischen von Markdown- und HTML-Code komplex. Im obigen Beispiel sind etwa die Leerzeilen unabdingbar. Durch sie wird die mittlere Textzeile als Markdown und nicht als HTML aufgefasst, sodass die Sternchen Wirkung entfalten – zumindest in manchen Implementierungen. Weil solche Sprachmischungen schnell implementierungsabhängige Ergebnisse produzieren, die man kaum noch durchschaut, sollte man sie eher als Notlösung betrachten: Kann man ausprobieren, wenn man mit Markdown-Syntax alleine einfach nicht ans Ziel kommt.

Tabellen

Als Beispiel für so einen Fall nennt die originale Markdown-Spezifikation Tabellen. Das ist zum Glück meistens nicht mehr korrekt, denn HTML-Tabellen sind lästig zu schreiben und schwer zu lesen. Viele Markdown-Implementierungen unterstützen eine simplere und viel übersichtlichere Syntax:

```
| Magazin | Zyklus   | Domain       |
| ------- | -------- | ------------ |
| c’t     | 14 Tage  | ct.de        |
| iX      | 4 Wochen | ix.de        |
| Mac & i | 8 Wochen | mac-and-i.de |
```

Allerdings sind Tabellen kein Teil der CommonMark-Spezifikation und es gibt zahlreiche Syntaxvariationen. Meistens darf man zum Beispiel die äußeren senkrechten Striche (|) auch weglassen. In der Regel kann man auch bestimmen, wie Tabellenspalten ausgerichtet werden sollen, indem man Doppelpunkte in die Trennlinie zwischen der Kopfzeile und dem Rest der Tabelle setzt. Beides zusammen sieht so aus (die erste Spalte wird linksbündig, die zweite zentriert und die dritte rechtsbündig ausgegeben):

```
Magazin | Zyklus   | Domain
:------ | :------: | -----------:
c’t     | 14 Tage  | ct.de
iX      | 4 Wochen | ix.de
Mac & i | 8 Wochen | mac-and-i.de
```

Außerdem bietet Markdown wieder mal eine Abkürzung für Faule: Man muss die Tabellenspalten nicht im Quelltext ausrichten, damit sie korrekt interpretiert werden. Das vereinfacht das Tippen erheblich, geht aber deutlich zulasten der Lesbarkeit:

```
Magazin | Zyklus | Domain
:- | :-: | -:
c’t | 14 Tage | ct.de
iX | 4 Wochen | ix.de
Mac & i | 8 Wochen | mac-and-i.de
```

Neben Tabellen gibt es noch viele weitere Markdown-Ergänzungen, die sich weder in CommonMark noch der originalen Spezifikation der Sprache finden. Dazu gehören zum Beispiel Fußnoten oder Textabschnitte, die – häufig am Anfang des Dokuments – Metadaten enthalten. Manche Systeme erlauben auch Emojis und sogar mathematische Formeln in LaTeX-Syntax im Markdown-Text.

Wer Bedarf an solchen Erweiterungen verspürt, konsultiert am besten die Dokumentation der Software, um die es geht. Im Regelfall ist das der schnellste Weg, um herauszufinden, was im konkreten Fall möglich ist und welche Syntaxvariante das System verlangt. Um einfach nur einen Blick über den Tellerrand zu werfen, eignet sich die Dokumentation von Pandoc (siehe ct.de/y5hr), einem System, das zahlreiche Ergänzungen in zahlreichen Syntaxvarianten versteht [7].

Fazit

Wer die Markdown-Basics beherrscht, dem steht in vielen verschiedenen Systemen eine einheitliche, praktische und schnelle Eingabemethode zur Verfügung. Zwar unterscheiden sich Implementierungen in Details, aber wenn gelegentlich etwas nicht wie erwartet funktioniert, dann hilft in der Regel ein Backslash, eine zusätzliche Leerzeile, um Elemente zu trennen, oder man vereinfacht die Dokumentstruktur etwas: Codeblöcke in Listen in Zitaten in Listen bringen nicht nur so manche Markdown-Implementierung in die Bredouille – sie sind auch einfach schwer zu verstehen.

Wie zahlreiche andere c’t-Artikel entstand auch dieser in einem Markdown-Editor. Das ging wie immer flott und einfach von der Hand und ist auch im Quelltext exzellent zu lesen – obwohl es wirklich verschärfte Bedingungen sind, mit Markdown-Syntax über Markdown-Syntax zu schreiben. *(syt@ct.de)*

1. Literatur
2. Stefan Wischner, Blitznotizen, c’t 13/2021, S. 82

3. Achim Barczok, Notiznetz, c’t 6/2021, S. 84
4. Liane M. Dubowy, Organisationstalent, Schreiben und organisieren in Notion, c’t 12/2021, S. 166
5. Andrijan Möcker, Tippgemeinschaft, HedgeDoc: Gemeinsam texten mit Markdown-Pads, c’t 13/2022, S. 164
6. Jan Mahn, Nach Art des Hauses, Rezeptdatenbank selbst hosten mit Tandoor Recipes, c’t 2/2022, S. 164
7. Anna Simon, Website-Wasservogel, Mit Pelican einfach schnelle Webseiten generieren, c’t 12/2022, S. 164
8. Jan Mahn, Formatautomat, Automatische Textumwandlung mit pandoc, c’t 7/2018, S. 168

Markdown-Spezifikationen: ct.de/y5hr

Google, Instagram, YouTube, Facebook: TikToks riesiger Erfolg treibt die Konkurrenz um

TikTokisierung

Google, Instagram, YouTube, Facebook: TikToks riesiger Erfolg treibt die Konkurrenz

um

Die Facebook-Mutter Meta und der Google-Konzern Alphabet sind gezwungen, an ihren Diensten herumzuschrauben, um an den Erfolg der Kurzvideo-Plattform TikTok anzuknüpfen. Der Nutzen mancher Neuerung ist aus Anwendersicht allerdings zweifelhaft.

Von Jo Bager

Meta hat Ende Juli die Mobil-App seines sozialen Netzwerks Facebook umgebaut. Wichtigstes neues Element ist seitdem der sogenannte Home-Tab. Damit treibt Meta eine Entwicklung auf die Spitze, die bereits in der Vergangenheit bewirkt hat, dass Nutzer in ihrem Facebook-Newsfeed immer weniger Posts von ihren „Freunden“ gesehen haben.

Wenn ein Nutzer die App öffnet, präsentiert sie ihm stattdessen noch mehr Inhalte von Accounts, denen er nicht folgt. Dazu zählen auch viele Reels – kurze, sich endlos wiederholende Videos. Damit die Inhalte im Home-Tab zu den Interessen des Nutzers passen, wertet eine KI laut Facebook „Tausende von Signalen“ aus. Wird etwa ein Reel in kurzer Zeit von vielen Menschen kommentiert, steigen seine Chancen, in vielen Home-Tabs zu erscheinen. Im Home-Tab können Nutzer zudem selbst Beiträge, Reels und Stories erstellen.

Neben dem Home-Tab hat die App mit dem Redesign auch einen neuen Feeds-Tab erhalten. Er zeigt dem Nutzer nur Posts an, die von seinen Freunden, Seiten und Gruppen stammen. In den Feeds-Tab muss man aber von Hand wechseln, die App startet immer im Home-Tab.

Man muss nicht lange scrollen in Facebooks Home-Tab, schon fühlt man sich in TikTok hineinversetzt.
Dass sich diese Beschreibung des Home-Tabs kaum von der der TikTok-App unterscheidet, ist kein Zufall. Die App der

chinesischen Kurzvideoplattform ist ein Riesenerfolg und droht, Facebook und Instagram, aber auch anderen großen Plattformen den Rang streitig zu machen.

Meta unter Druck

Zwar hat Meta mit Facebook, Instagram, Messenger und WhatsApp insgesamt mehr als drei Milliarden Nutzer – deutlich mehr als TikTok mit gut einer Milliarde. TikTok wächst aber viel schneller als Facebooks Dienste und ist vor allem bei den Nutzern in der Altersgruppe der 15- bis 25-Jährigen sehr beliebt.

Bei der Nutzerbindung verweist TikTok viele Konkurrenten bereits heute auf die Plätze. So verbringen Anwender laut den Zahlen des Marktforschungsunternehmens Sensor Tower täglich 95 Minuten in der TikTok-App. Zum Vergleich: Bei YouTube sind es nur 74, bei Instagram 51 und bei Facebook 49 Minuten.

TikToks Erfolg ist einer der Gründe, aus denen der einst erfolgsverwöhnte Meta-Konzern unter Druck steht. 36 Prozent weniger Nettogewinn musste Meta für das zweite Quartal 2022 melden. Die Nachrichtenagentur Reuters berichtet unter Berufung auf ein internes Meta-Memo, dass bestimmte Positionen unbesetzt bleiben sollen. Außerdem werde der Leistungsdruck erhöht, um Angestellte auszusortieren, die nicht in der Lage seien, „aggressivere Ziele“ zu erreichen.

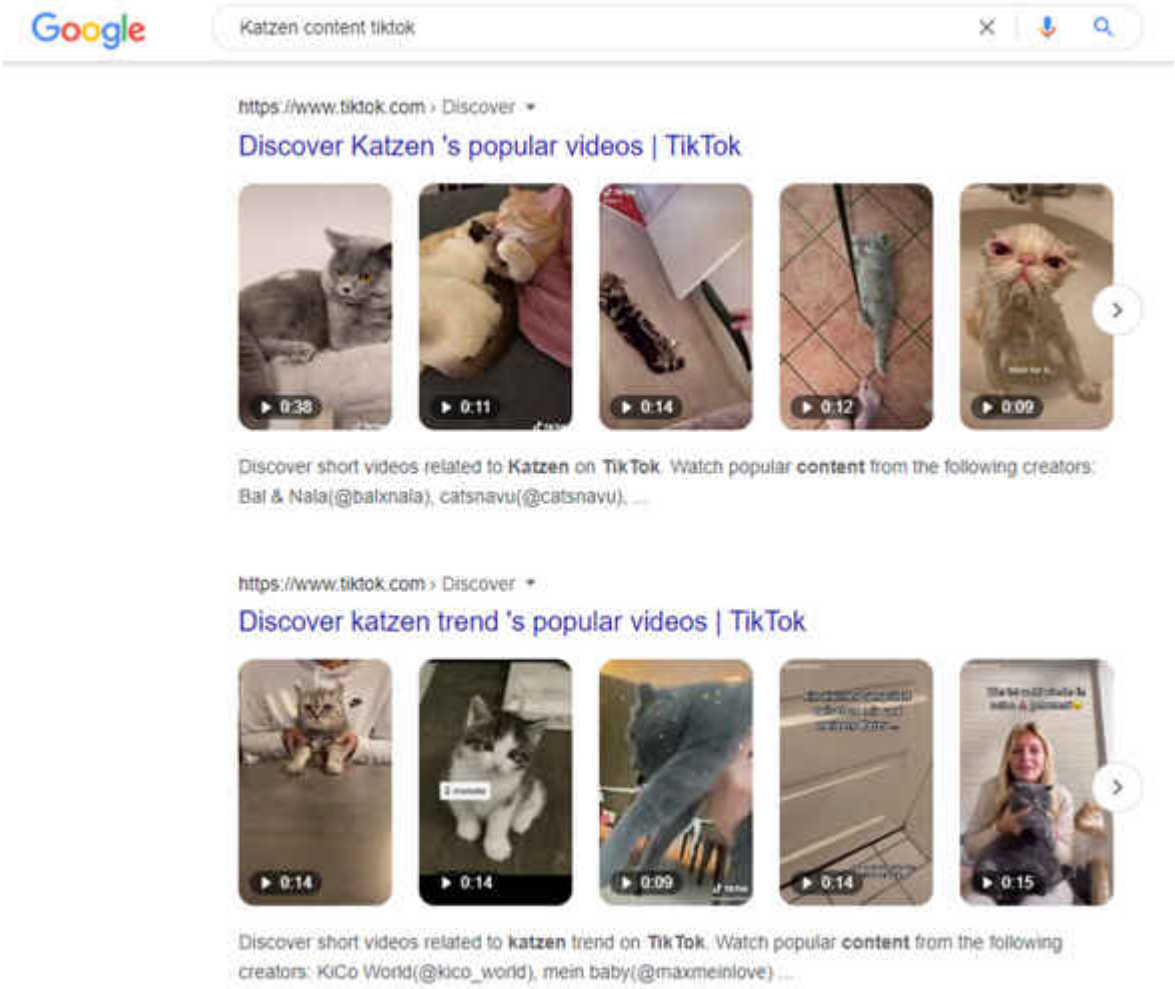
Als weitere Maßnahme baut Meta die Funktionen von TikTok in seinen Diensten nach, auch bei Instagram. Schon vor einigen Monaten hatte Instagram Kurzvideos eingeführt, Reels. Bislang fanden sich diese allerdings in einem eigenen Reiter, getrennt von den anderen Inhalten auf der Plattform. Im Juli integrierte Instagram die Kurzvideos dann in den Newsfeed. Genau wie TikTok zeigte die App außerdem ihren Nutzern vermehrt Inhalte von Konten an, denen sie gar nicht folgen.

Auch Alphabet reagiert

Meta ist nicht das einzige Unternehmen, das den Einfluss von TikTok zu spüren bekommt, sondern auch Alphabet mit seinen Diensten Google Suche, Google Maps und YouTube ist betroffen. Der Konzern hatte bereits 2021 auf TikTok reagiert und seinen Videodienst um das stark von TikTok inspirierte YouTube Shorts erweitert sowie TikTok- (und Instagram-) Inhalte in seiner Suchmaschine berücksichtigt.

Junge Menschen kommen trotzdem immer seltener auf die Idee, bei Google zu suchen. Das erklärte der Google-Manager Prabhakar Raghavan auf einer Konferenz. Wenn sie etwa nach einem Restaurant suchten, öffneten 40 Prozent der jungen Nutzer nicht Google Maps oder die Google-Suche, sondern TikTok oder Instagram. Das hätten Studien von Google ergeben, zu denen auch eine Umfrage unter 18- bis 24-Jährigen in den USA gehöre.

Laut Raghavan bevorzugen junge Menschen allgemein „visuell reichhaltigere Formen“ der Suche. Als Negativbeispiel nannte er Google Maps, dessen Aussehen auf gedruckten Karten basiere – einem Medium, mit dem junge Menschen kaum noch in Kontakt kämen.

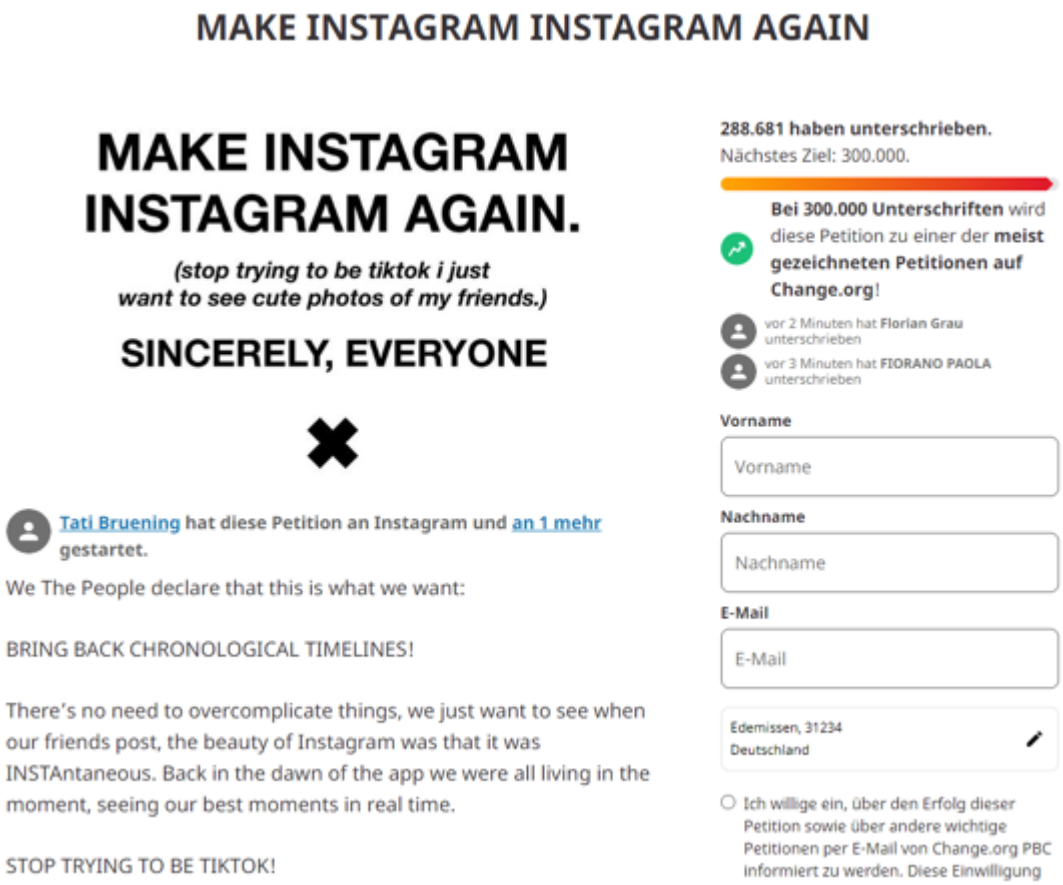


Googles Suchmaschine findet TikTok-Videos, wenn man den Begriff „tiktok“ in die Suchanfrage aufnimmt. Vor allem junge Leute suchen dennoch lieber direkt bei TikTok.

News und Musik

Sogar über das Weltgeschehen informieren junge Menschen sich inzwischen bei TikTok. Das zeigen Studien der britischen Medienaufsicht und des Reuters Institute Digital News Report 2022. Laut den Zahlen der Reuters-Studie nutzen weltweit bereits 15 Prozent der 18- bis 24-Jährigen TikTok für News.

In der Reuters-Studie reicht der Marktanteil von TikTok nicht an die anderer Onlinedienste wie Facebook, YouTube und Instagram heran. Aber auch in diesem Markt gilt: TikTok wächst am schnellsten.



Hunderttausende wollten ein Instagram zurück, das nicht versucht, so zu sein wie TikTok – mit Erfolg.

Kopier-Widerstand

TikTok ist der Online-Player der Stunde. Dem Erfolg des rasant wachsenden Dienstes können sich auch die Online-Granden nicht entziehen. Allerdings fällt ihnen außer „Nachmachen“ nicht viel ein. Facebook zum Beispiel treibt seine Anleihen beim stilprägenden Kurzvideodienst fast bis zur Selbstaufgabe.

Meta ist sich dessen offensichtlich bewusst, sonst hätte der Konzern parallel zum Home-Tab nicht auch den Feeds-Tab eingeführt, der offenbar Facebook-Traditionalisten besänftigen soll. Und damit Facebook-Nutzer originäre Videos hochladen und nicht bereits bei TikTok veröffentlichte Filmchen zweitverwerten, hat sich Meta ein Bonusmodell ausgedacht: 20 Prozent der Werbeeinnahmen winken Usern, die Videos mit Facebook-lizenzierter Hintergrundmusik hochladen. Ob die Nutzer die Neuerungen akzeptieren, muss sich aber erst noch zeigen.

Bei Instagram jedenfalls hat Meta überzogen. Insbesondere Fotokünstler sind gegen die Integration von Videos auf die Barrikaden gegangen. Sie befürchteten, dass ihre Werke in einem Video-Newsfeed nicht mehr die angemessene Beachtung finden würden und starteten die Petition „Make Instagram Instagram again“. Kurz nachdem sich die Top-Influencerin Kylie Jenner der Petition angeschlossen hatte, verkündete der Instagram-Chef Adam Mosseri eine Rücknahme der Neuerungen – vorerst. *(jo@ct.de)*

Studien zum Nachrichtenkonsum: ct.de/y75r

Widersprüchliche Ratschläge zur Google-Fonts-Einbindung

Markt + Trends | IT-Recht & Datenschutz

Widersprüchliche Ratschläge zur Google-Fonts-Einbindung

Zur aktuellen Abmahnwelle wegen der datenschutzrechtswidrigen Einbindung dynamischer Google Fonts auf Webseiten hat sich jüngst die Datenschutzbehörde aus Niedersachsen zu Wort gemeldet. Sie empfiehlt auf die dynamische Einbindung zu verzichten, die benötigten Schrifttypen (Fonts) herunterzuladen und auf dem eigenen Server zum Abruf vorzuhalten. Hierdurch wird eine Übermittlung personenbezogener Daten von Internetnutzern in die USA, etwa deren IP-Adresse, vermieden.

Google hat unterdessen ein FAQ zur Verarbeitung von Nutzerdaten im Zusammenhang mit dem Bezug von Schriftarten von

Google-Servern veröffentlicht. Der Konzern vertritt die Ansicht, dass die übermittelten Daten bei dynamischer Fonts-Einbindung ausschließlich für die Bereitstellung der Schriften verarbeitet werden. Eine Verarbeitung für Zwecke der Analyse oder Werbung erfolge nicht. Ob dies allerdings helfen könne, sich gegen Abmahnungen erfolgreich zu verteidigen, wie Google schreibt, ist unsicher. Im Januar 2022 hatte das Landgericht München I einem Kläger Schadenersatz wegen der datenschutzrechtswidrigen Google-Fonts-Einbindung zugesprochen und so die Abmahnwelle losgetreten. *Tobias Haar* (ur@ix.de)

Abmahnwelle wegen Google Fonts

Bettelbriefe

Abmahnwelle wegen Google Fonts

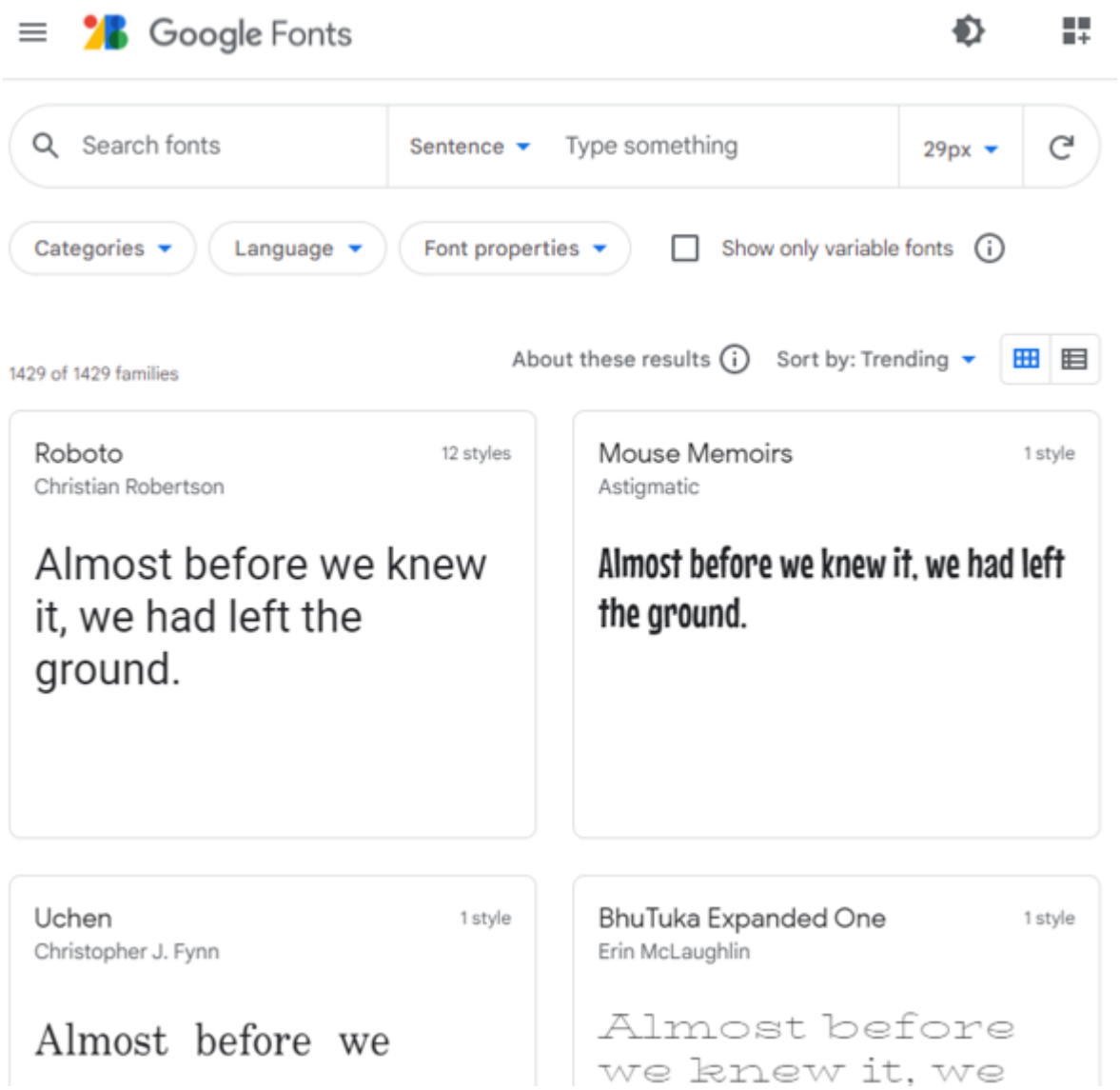
Tausende von Empfängern staunen derzeit über Forderungsschreiben, die sie im E-Mail-Postfach oder im Briefkasten vorfinden. Weil sie Googles kostenlose Fonts in ihre Websites eingebettet haben, sollen sie 100 bis knapp 500 Euro berappen. Was steckt hinter diesen Schreiben und wie wehrt man sich dagegen?

Von Joerg Heidrich

Adressaten der Schreiben sind allesamt Website-Betreiber. Die

Abmahnungen werfen ihnen einen „unzulässigen Eingriff in das allgemeine Persönlichkeitsrecht“ und einen Verstoß gegen die Datenschutz-Grundverordung (DSGVO) vor. Ihr Vergehen: Sie nutzen auf ihrer Webseite Fonts, die Google kostenlos anbietet.

Dabei handelt es sich um ein Verzeichnis von mehreren Hundert frei verwendbarer Schriftarten. Website-Betreiber können die Schriftarten herunterladen und lokal auf dem eigenen Webserver bereitstellen. Alternativ dazu können sie die Schriften auch online einbinden. Dies führt dann dazu, dass der Browser des Besuchers sie beim Aufruf einer Seite von den Servern des US-Konzerns lädt. Und das ist ein Problem.



Google Fonts hält viele kostenlose Schriftarten bereit – die aber lokal eingebunden werden sollten.

Das Landgericht (LG) München hatte im Januar 2022 die Online-Nutzung von Google Fonts mit der Begründung verboten, dass dabei unerlaubt personenbezogene Daten an Google in die USA weitergegeben werden (Az. 3 O 17493/20). Diese Entscheidung bildet die Grundlage für die versandten Abmahnungen und Forderungsschreiben.

Es handele sich bei den übermittelten dynamischen IP-Adressen um Informationen, so die Münchener Richter, die in den Schutzbereich des Datenschutzes fallen. Der Seitenbetreiber habe das Recht des Klägers auf informationelle Selbstbestimmung verletzt, indem er die dynamische IP-Adresse des Besuchers beim Aufruf der Seite an Google weiterleitete. Hierfür habe es keine Rechtsgrundlage in Form einer Einwilligung oder eines berechtigten Interesses gegeben. Dem Kläger stehe somit ein Unterlassungsanspruch zu.

Doch damit nicht genug hatte das LG München dem Besucher der Website noch einen Schadensersatzanspruch in Höhe von 100 Euro zugebilligt. Ein solcher Anspruch kann sich aus Artikel 82 der DSGVO ergeben und steht jeder Person zu, „der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist“. Hoch umstritten ist dabei die Frage, welche Intensität ein solcher Eingriff haben muss, um ein Schmerzensgeld auszulösen. In der juristischen Diskussion wird die Entscheidung aus München überwiegend als überzogen kritisiert.

„Individuelles Unwohlsein“

Die Richter sahen im vorliegenden Fall bereits durch die Übermittlung an Google einen „Kontrollverlust“ des Betroffenen und ein „individuelles Unwohlsein“. Denn Google sei bekannt dafür, Daten über seine Nutzer zu sammeln. Zudem sei es unstreitig, dass die IP-Adresse an einen Server in den USA übermittelt werde, wo kein angemessenes Datenschutzniveau gewährleistet sei.

Diese Argumentation machen sich jetzt die Schreiber der fordernden Briefe zu eigen. Man habe die Website des Empfängers besucht, dieser verwende die Online-Version der Google Fonts und solle daher wegen des dadurch verursachten individuellen Unwohlseins schnellstens 100 Euro an den Versender überweisen.

Etwas komplizierter wird es, wenn das Schreiben von einem Anwalt kommt. Offenbar haben juristische Veteranen vergangener Massenabmahnungen ein neues Tätigkeitsfeld gefunden. Sie fordern nicht nur, dass die Empfänger den Schaden ihrer Mandanten begleichen. Sie sollen zudem eine Unterlassungserklärung für die Nutzung der Google-Fonts abgeben – und die Anwaltsgebühren zahlen, meist in Höhe von 367,23 Euro.

Gerade gegen die anwaltlichen Abmahnungen gibt es allerdings eine ganze Reihe von potenziellen Einwendungen, sodass es sich dabei keinesfalls um „sichere Fälle“ für die Abmahner handelt. Es spricht bereits einiges dafür, dass die Anwaltsschreiben rechtsmissbräuchlich sind, da die angeblichen Betroffenen die Websites vorsätzlich angesteuert haben dürften. Trotzdem sollten zumindest juristische Laien in diesen Fällen vorsichtshalber einen IT-Anwalt ins Boot holen.

Weniger riskant ist dagegen die Abwehr von Aufforderungsschreiben, die nicht von einem Anwalt kommen. Denn nach derzeitigem Stand ist es eher unwahrscheinlich, dass die Mehrheit der Gerichte den Ansichten des LG München hinsichtlich der Zahlung einer Geldentschädigung folgen. Es spricht daher einiges dafür, dass man derartige Schreiben ignorieren darf. Allerdings sollte jeder Website-Betreiber auf die lokal gehostete Version von Google Fonts umsteigen. (*jo@ct.de*)

Urteil des LG München: ct.de/yjub

https://www.gesetze-bayern.de/Content/Document/Y-300-Z-GRURRS-

B-2022-N-612?hl=true

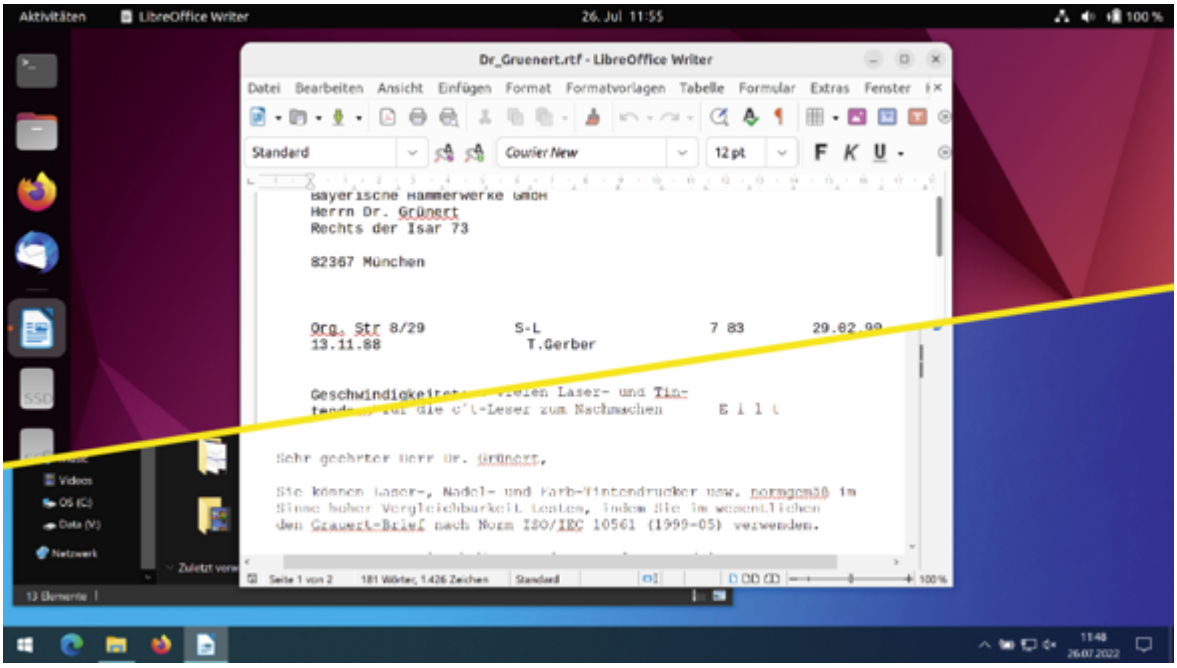
Windows und Linux zusammen

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.

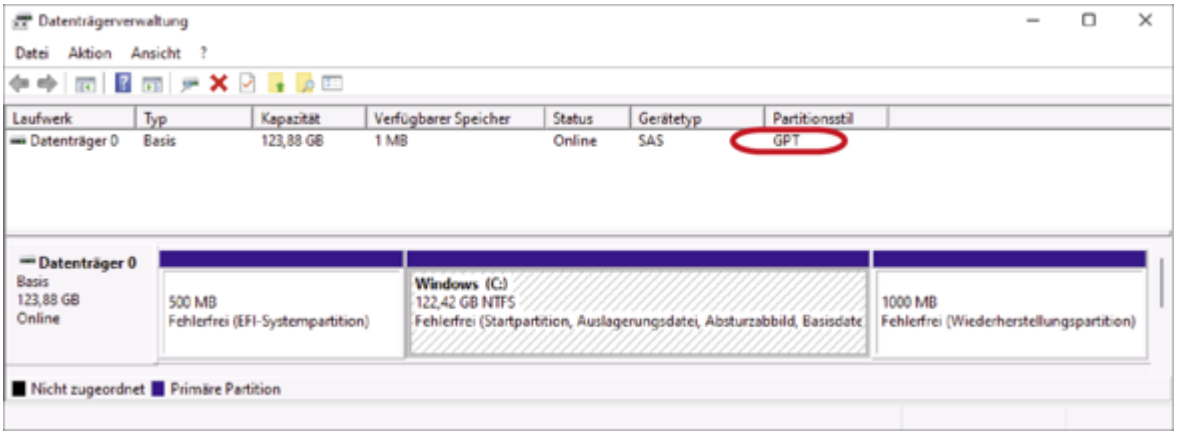
Haben Sie erst mal alle Anleitungen durchgespielt, reduziert sich die seit Jahrzehnten andauernde Diskussion um das bessere Betriebssystem für Sie auf die simple Frage, welches Betriebssystem Sie beim Einschalten des Computers starten. Und die völlig undogmatische Antwort lautet: jenes, das in diesem 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.

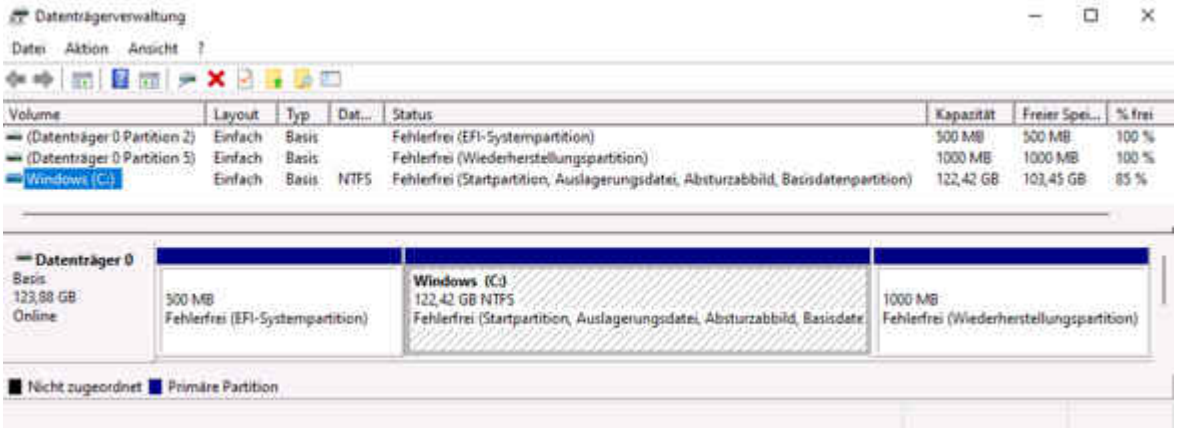
Vorbereiten

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.

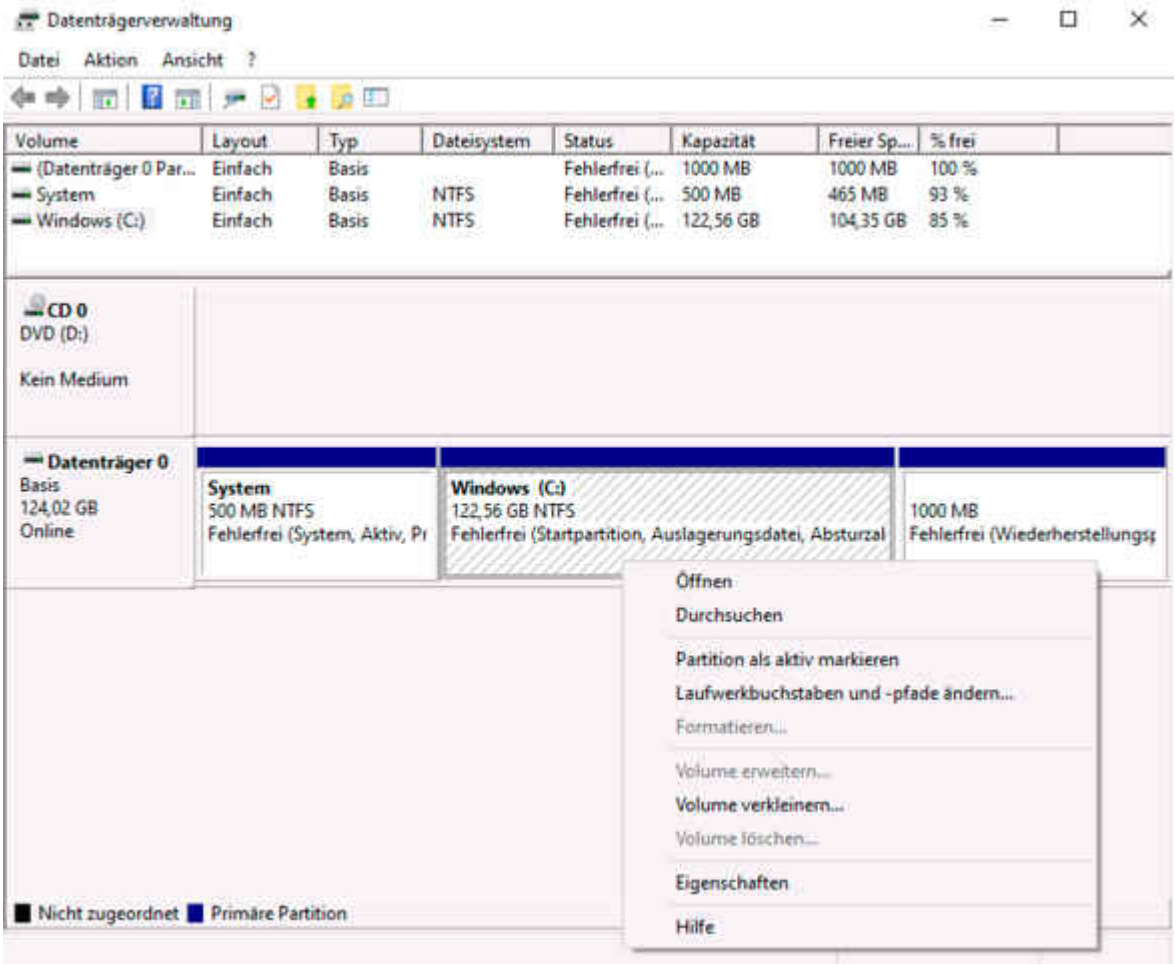
Falls der Platz immer noch nicht ausreicht: Das Titelthema von c’t 8/2018 bietet gleich fünf Artikel mit vielen weiteren Tipps [2].

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“.



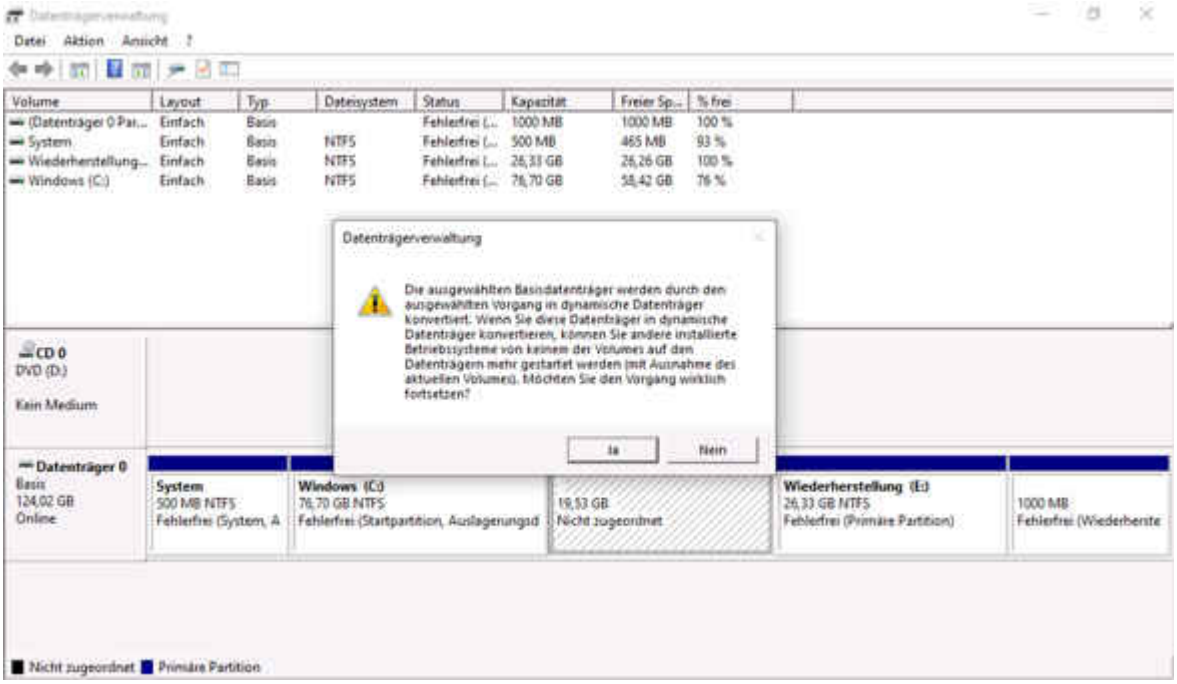
Die Datenträgerverwaltung bringt einen Assistenten zum Verkleinern der Windows-Partition mit. Der Haken ist die RE-Partition, die hier am Ende des Datenträgers liegt.
Das Programm präsentiert oben eine detaillierte Liste mit den vorhandenen Partitionen inklusive Füllstand, Art des Dateisystems, Status, 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.)



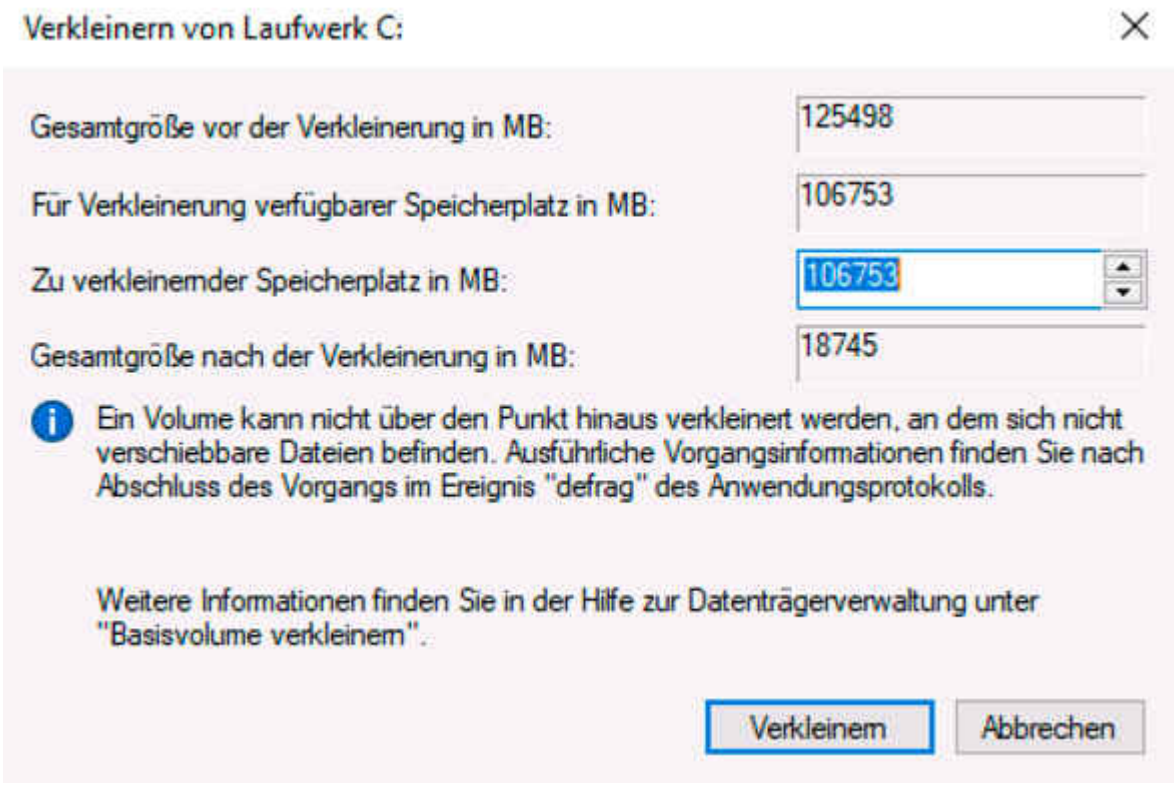
Wenn auf dem Datenträger das alte Partitionsschema MBR verwendet wird, kann das Erstellen einer weiteren Partition scheitern. Die Datenträgerverwaltung hilft dann nicht weiter.
Die Datenträgerverwaltung möchte Ihnen eine andere Krücke andrehen. Wenn Sie probieren, auf einem MBR-Datenträger eine fünfte 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.

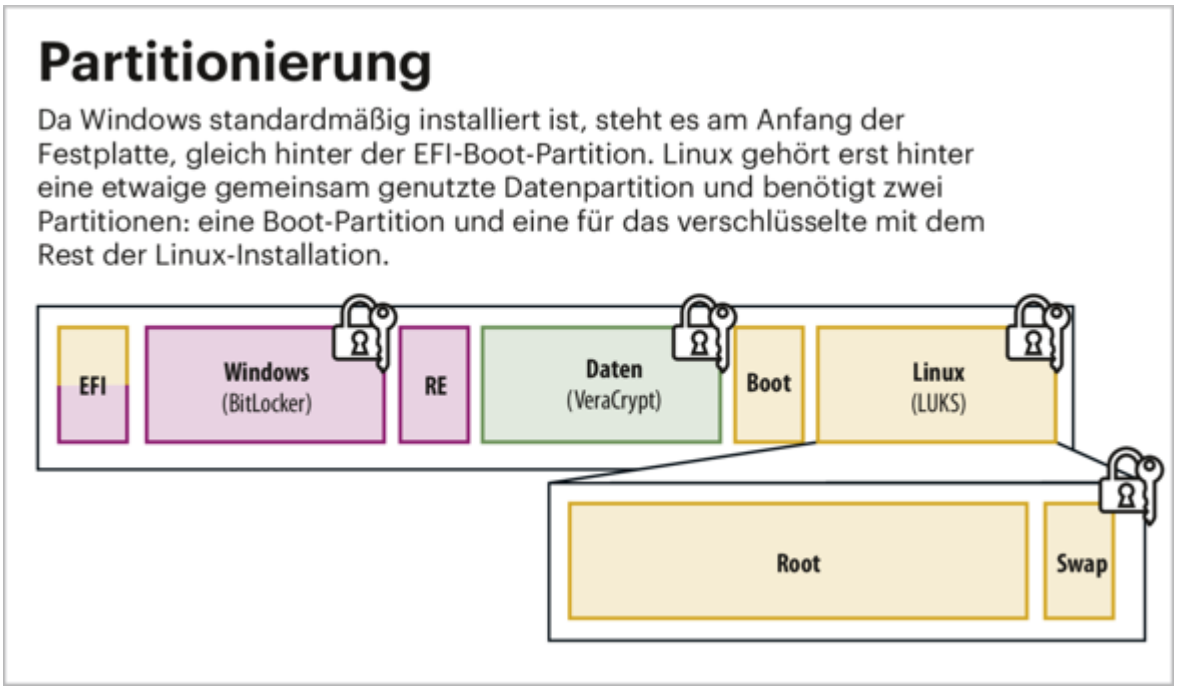
Von Mirko Dölle

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
```

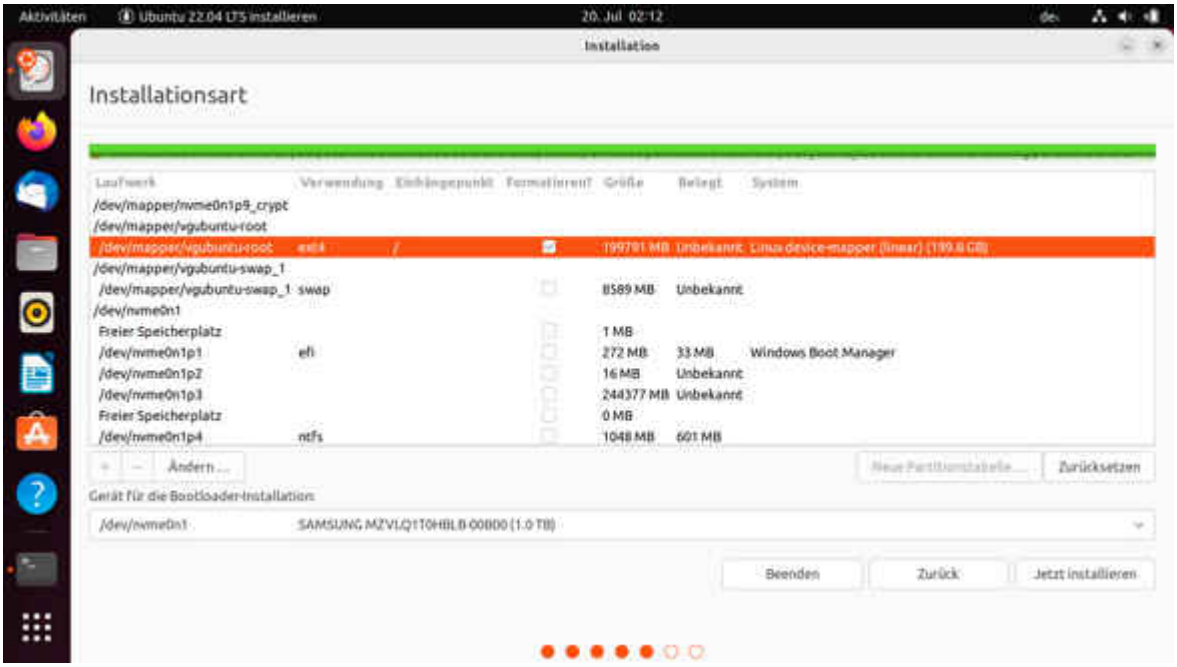
Was noch frei ist, stecken Sie in das Volume „swap_1“:

```
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

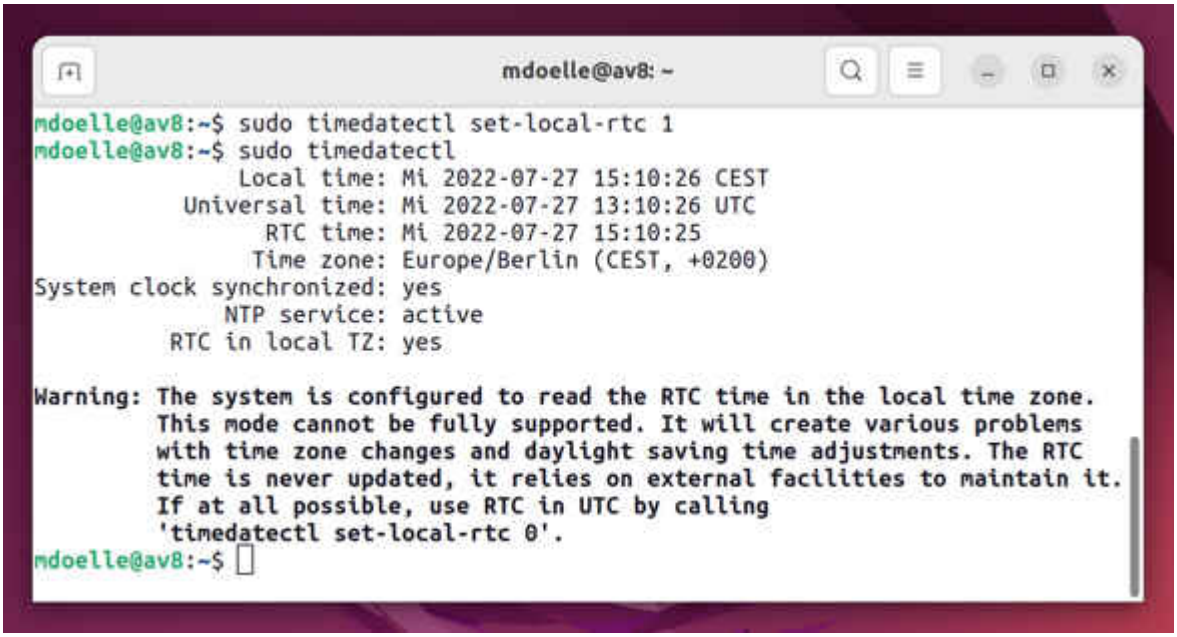
Ein ständiges Ärgernis bei Parallelinstallationen ist, dass Windows und Linux ständig die interne Uhr des Rechners verstellen: Windows speichert standardmäßig die Lokalzeit in der Hardware-Uhr, auch RTC (Real Time Clock) genannt, während Linux standardmäßig die Uhrzeit der Zeitzone UTC speichert. Letzteres 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“.

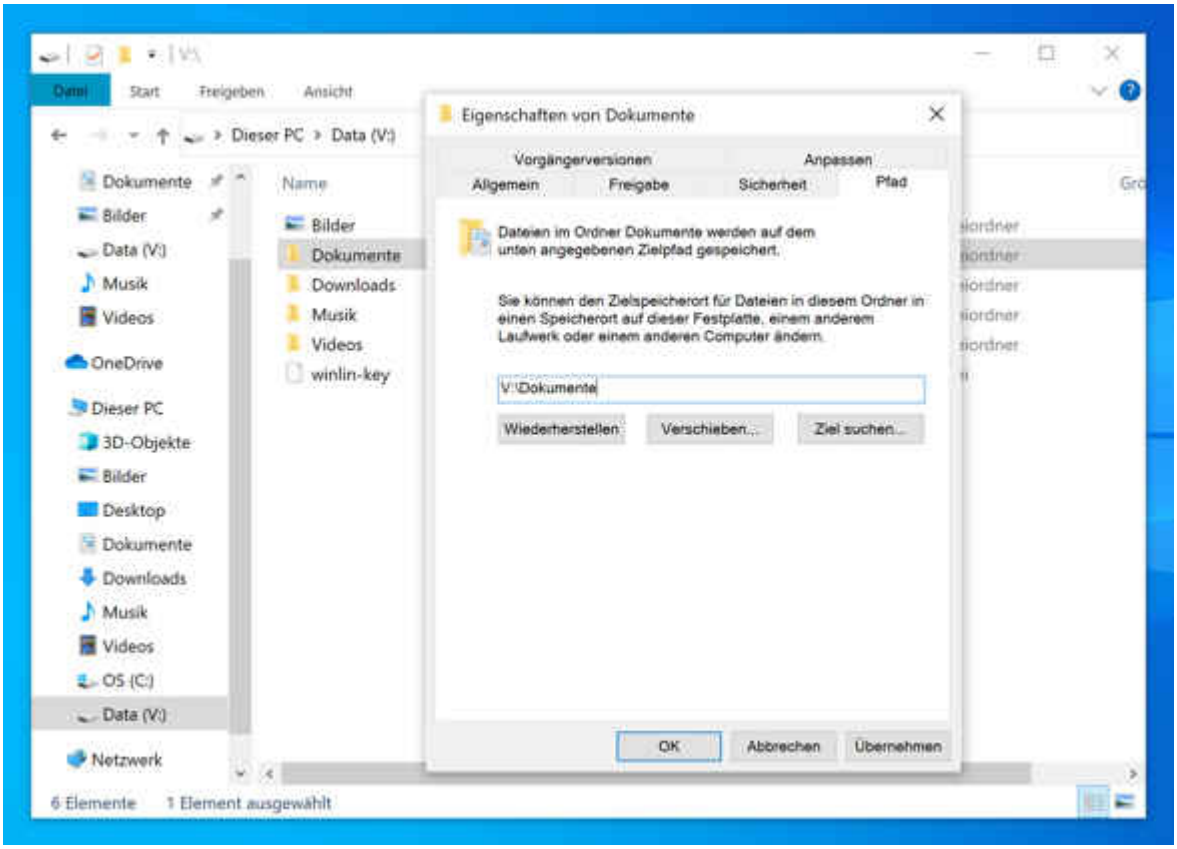
Damit VeraCrypt Sie zukünftig nicht mehr mit der Frage nach dem Passwort oder der Schlüsseldatei behelligt, importieren Sie über „Settings/Default Keyfiles…“ und dort über „Add

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:

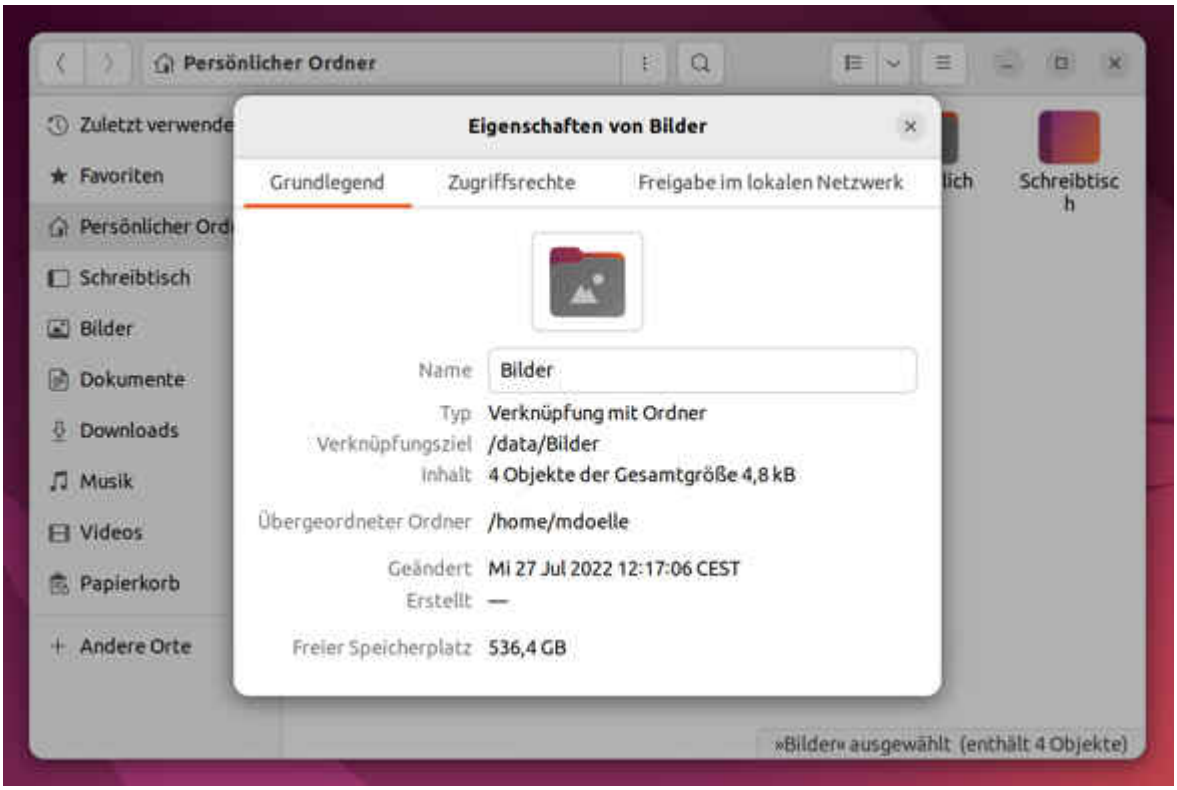
```
winlin-data  /dev/sda3  /dev/nulltcrypt-veracrypt,tcrypt-keyfile=/etc/crypto/winlin-key
```

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)*