# Was ist ein Snapshot, und wie funktioniert er?

von Howard Oakley, eclecticlight.co • Übersetzung KJM

Angepriesen als eine der größten neuen Funktionen in APFS, gibt es in macOS nichts Verwirrenderes als den Snapshot. Selbst wenn man das Konzept versteht, ist man mit der Arithmetik ihrer Größe meist überfordert. Lassen Sie mich versuchen, es zu erklären.

Jeder physische Speicher bzw. jede Festplatte ist in eine oder mehrere Partitionen unterteilt, wobei der kontinuierliche Speicherplatz von einem Dateisystem wie HFS+ oder APFS verwaltet wird. Als altes Dateisystem verwendet HFS+ jede Partition als ein einzelnes Volume, aber APFS behandelt seine Partitionen als Container für ein oder mehrere Volumes, von denen sich jedes den Speicherplatz in diesem Container teilt. Das ermöglicht es APFS-Volumes, ihre Größe zu ändern, wenn sie die Dateien enthalten müssen, die sie speichern.

Jedes APFS-Volume besteht aus Dateisystem-Metadaten, in denen die Verzeichnisse und andere Informationen gespeichert sind, die es verwendet, sowie aus allen Daten, die seinen Inhalt ausmachen. Innerhalb des Containers gibt es einen Satz von Dateisystem-Metadaten für jeden Datenträger, und die Inhaltsdaten werden dann mit denen aller anderen Datenträger innerhalb des Containers gemischt.

## Erstellen eines Snapshots

Wie der Name schon sagt, ist ein Snapshot eine Erfassung eines Volumes zu einem bestimmten Zeitpunkt. Die Erstellung eines Snapshots ist sehr schnell und einfach: Für einen Moment werden die Metadaten des Dateisystems des Volumes eingefroren und dupliziert, um eine identische Kopie zu erstellen, die als Snapshot gespeichert wird. Auf langsameren Macs mit großen APFS-Volumes können Sie das Erstellen eines Schnappschusses manchmal als kurzzeitiges Einfrieren bemerken, aber da die Dateisystem-Metadaten im Verhältnis zu den Dateidaten klein sind, werden Sie dies auf schnelleren Macs nicht einmal bemerken.

Der Zweck eines Schnappschusses besteht darin, dass Sie das Volume in einen früheren Zustand zurückversetzen können, wie er durch die Dateisystem-Metadaten im Schnappschuss definiert ist. Um dies zu ermöglichen, verwaltet das Dateisystem ab dem Moment, in dem der Schnappschuss erstellt wird, Änderungen an den Dateidaten anders, da es alle geänderten Daten beibehalten muss, da Sie sonst nicht in der Lage wären, das Volume auf den Zustand des Schnappschusses zurückzusetzen. Wenn Sie nach der Erstellung eines Snapshots eine Datei löschen, kann das Dateisystem den von diesen Daten belegten Speicherplatz nicht löschen und wiederverwenden, sondern muss ihn so lange beibehalten, bis der Snapshot gelöscht wird. Und genau das macht Schnappschüsse so kompliziert, sowohl als Konzept als auch in der Arithmetik ihrer Größe.

## Snapshot-Größe

Um dies anhand eines sehr einfachen Beispiels zu veranschaulichen, nehmen wir an, Ihr APFS-Volume hat 100 GB gespeichert, wenn Sie einen Schnappschuss von diesem Volume erstellen. Dann löschen Sie eine Datei, die 10 GB belegt hat. Ohne den Schnappschuss hätte Ihr Datenträger dann 10 GB mehr freien Speicherplatz, und es wären 90 GB an Dateien auf dem Datenträger vorhanden. Aufgrund des Snapshots sind diese 10 GB jedoch nicht frei, da der Snapshot ohne sie nicht in der Lage wäre, das Volume in den Zustand zurückzuversetzen, in dem es sich zum Zeitpunkt der Erstellung des Snapshots befand. Erst wenn der Snapshot gelöscht wird, werden diese 10 GB zur Wiederverwendung freigegeben.

Dasselbe geschieht, wenn sich Dateien ändern, nur dass hier die Mengen kleiner sind, da das Dateisystem geänderte Speicherblöcke und nicht ganze Dateien aufbewahrt. Kehren wir zu den 100 GB Daten zurück, nur dass diesmal nicht eine große Datei gelöscht wird, sondern nur 1 GB ihrer Daten geändert wird. Der Snapshot behält dann die ursprünglichen 1 GB bei, so dass 101 GB an Daten auf dem Datenträger verbleiben, deren freier Speicherplatz nur um dieses 1 GB abgenommen hat.

Wie groß ist nun dieser Snapshot? Es gibt zwei Antworten, je nachdem, ob Sie den Speicherplatz wissen wollen, der belegt wird, wenn Sie zu diesem Snapshot zurückkehren, in diesem Fall 100 GB, oder die Menge an Speicherplatz, die frei würde, wenn der Snapshot gelöscht würde. Im ersten Fall wären das 10 GB (nachdem die 10 GB große Datei gelöscht wurde), im zweiten Fall 1 GB (wenn seit dem Schnappschuss nur 1 GB geändert wurde).

Die Unterschiede zwischen diesen verschiedenen Größenangaben sind so groß, dass immer klar sein sollte, was angegeben wird. Das Festplattendienstprogramm gibt beispielsweise immer die Größe an, die nach seiner Schätzung durch das Löschen des Schnappschusses freigesetzt würde, während der Finder Schätzungen über den Speicherplatz abgeben kann, der benötigt wird, wenn Sie zu diesem Schnappschuss zurückgehen.

Da Schnappschüsse nicht Teil des aktiven Dateisystems sind, können sie als potenziell freier Speicherplatz betrachtet werden, wenn man den verbleibenden Speicherplatz in einem Container berechnet. Dies ist jedoch nicht ganz konsistent. Wenn Sie sich nicht sicher sind, wie viel Speicherplatz wirklich frei ist, verwenden Sie nicht die Zahlen des Finders, sondern die des Festplattendienstprogramms, wo Sie wirklich freien Speicherplatz, zu löschenden Speicherplatz (der auch Schnappschüsse enthalten kann) und die Summe als verfügbaren Speicherplatz sehen sollten.

Sobald ein Snapshot erstellt wurde, wird die Datenmenge, die er aufbewahren muss, mit der Zeit immer größer, da sich immer mehr Blöcke mit geänderten oder gelöschten Daten ansammeln. Aus diesem Grund müssen alle Anwendungen, die Schnappschüsse erstellen können, einschließlich Time Machine, diese Schnappschüsse rechtzeitig entfernen. Gelegentlich wird ein lokaler Time Machine-Schnappschuss verwaist und bleibt über die 24 Stunden hinaus bestehen, nach denen er eigentlich gelöscht werden sollte. Dieser Snapshot kann leicht wachsen und das Volume und seinen Container erdrücken.

### Snapshot-Deltas, Veränderbarkeit und Kopien

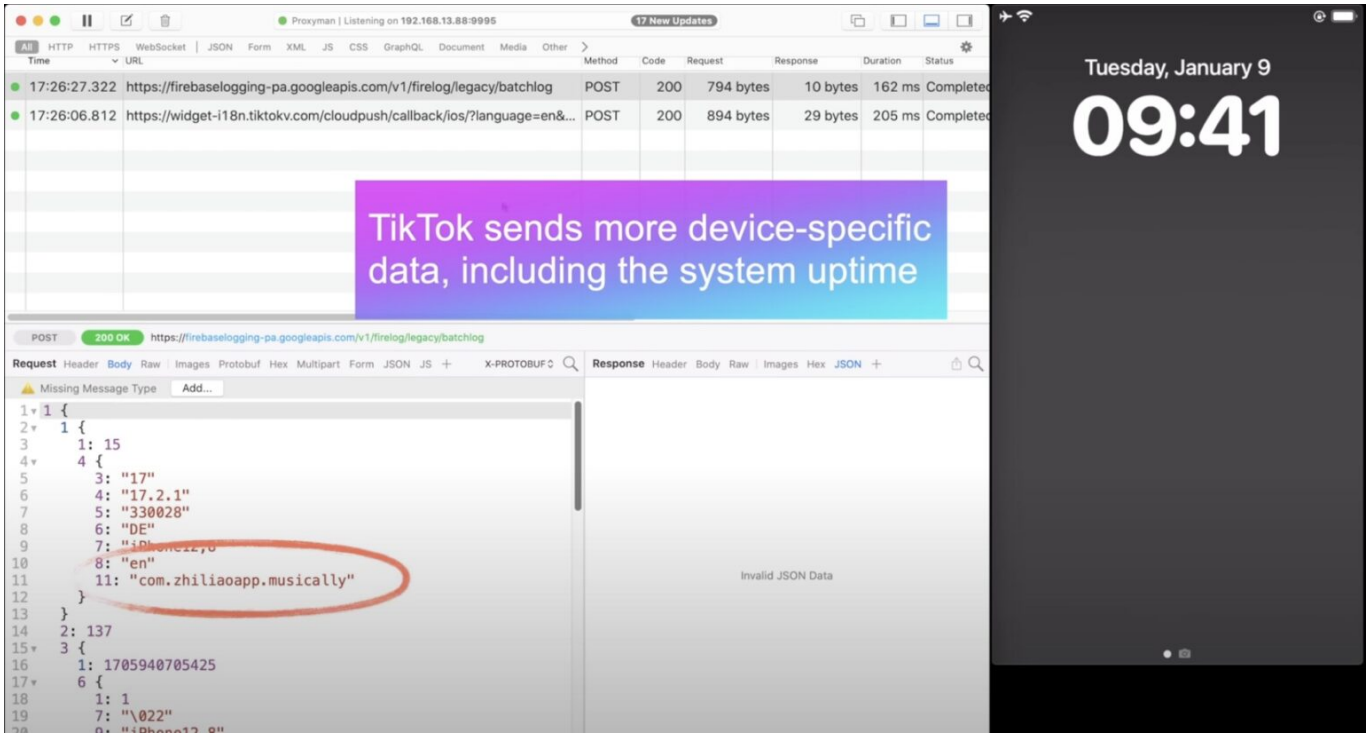
macOS speichert in seiner FSEvents-Datenbank eine Aufzeichnung der an jedem Volume vorgenommenen Änderungen, die normalerweise von Time Machine verwendet wird, um zu ermitteln, was gesichert werden muss. Da Time Machine auch Schnappschüsse für die letzten 24 Stunden erstellt und aufbewahrt, könnte es stattdessen (wie schon in High Sierra) Schnappschüsse vergleichen, um festzustellen, was sich in der Zeit zwischen diesen Schnappschüssen geändert hat, was als Schnappschuss-Delta bezeichnet wird (der griechische Buchstabe d steht für die Differenz).

Eine wichtige Eigenschaft von APFS-Snapshots ist, dass sie nicht mehr geändert werden können, sobald sie erstellt wurden. Es gibt zwar keinen grundsätzlichen Grund, warum es nicht möglich sein sollte, Schnappschüsse zu bearbeiten, aber es ist sicherlich kompliziert, und die Unveränderbarkeit von Schnappschüssen ist eines der Merkmale von APFS. Dies stellt sicher, dass Sie, wenn Sie zu einem Snapshot zurückkehren oder Dateien von einem Snapshot wiederherstellen wollen, alles bekommen, was Sie erwarten. Schnappschüsse bilden somit eine zuverlässige Aufzeichnung des vergangenen Dateisystemzustands.

Normalerweise können Sie einen Snapshot nicht auf ein anderes Volume verschieben oder kopieren. Obwohl Snapshots im Container und nicht im Volume gespeichert werden, ist das Kopieren eines Snapshots aufgrund der damit verbundenen Dateidaten nicht mit dem Kopieren eines Ordners vergleichbar. Soweit wir wissen, kopiert Time Machine bei der Sicherung auf ein APFS-Volume effektiv einen Snapshot, allerdings auf eine komplizierte Art und Weise, indem es alle geänderten Daten kopiert und den Snapshot auf dem Sicherungsvolume synthetisiert. Dies kann verwirrend sein, da Time Machine auch lokale Schnappschüsse auf jedem Volume erstellt, das es sichert. Für jedes Backup werden also zwei Snapshots erstellt: ein normaler, lokaler Snapshot auf demselben Volume und ein Snapshot auf dem Backup-Speicher, der aus dem Dateisystem und den Daten, die während des Backups kopiert wurden, synthetisiert wird.

### Zusammenfassung

- Ein Snapshot besteht aus einer Kopie der Metadaten des Dateisystems zum Zeitpunkt der Erstellung des Snapshots, aus Blöcken, die alle seither geänderten Daten auf dem Datenträger enthalten, und aus den zu diesem Zeitpunkt unveränderten Daten auf dem Datenträger.
- Geänderte Dateidaten in einem Snapshot werden erst freigegeben, wenn der Snapshot gelöscht wird.
- Snapshots können nicht geändert werden, obwohl die Dateidaten für sie mit der Zeit wachsen.
- Time Machine erstellt lokale Schnappschüsse auf jedem Volume, das gesichert wird, und erstellt Sicherungen auf dem Backup-Speicher in Form von Schnappschüssen.




# Manche iPhone-Apps spionieren mittels Push-Benachrichtigungen

Quelle: osxdaily.com • Übersetzung: KJM

Apple ist bekannt dafür, dass es sich um ein datenschutzfreundliches Unternehmen handelt, das zahlreiche Sicherheits- und Datenschutzfunktionen in das iPhone und das iPad einbaut, um Dinge wie die Standortverfolgung und die Verfolgung von Apps zu kontrollieren, aber einige namhafte App-Entwickler lassen sich kreative Wege einfallen, um Details über Ihr Gerät auszuspähen. Eine dieser raffinierten Methoden zum Ausspionieren von Geräten nutzt das Push-Benachrichtigungssystem, um Systeminformationen über Ihr iPhone zu sammeln.

Laut den Sicherheitsforschern von Mysk können Apps eine Push-Benachrichtigung an den Benutzer senden, die dann einen Code auf dem Gerät des Benutzers auslöst, der Analyse- und Geräteinformationen an entfernte Server sendet, und diese Daten können möglicherweise dazu verwendet werden, Fingerabdrücke von einem bestimmten Gerät und/oder Benutzer zu erstellen. Mysk erklärt:

„Viele Apps nutzen diese Funktion [Benachrichtigungen], um detaillierte Geräteinformationen zu senden, während sie unauffällig im Hintergrund laufen. Dazu gehören: Systembetriebszeit, Gebietsschema, Tastatursprache, verfügbarer Speicher, Akkustatus, Gerätemodell, Bildschirmhelligkeit, um nur einige zu nennen. Solche Signale werden häufig für die Erstellung von Fingerprints und die Verfolgung von Nutzern in verschiedenen Apps unterschiedlicher Entwickler verwendet. Fingerabdrücke sind unter iOS und iPadOS streng verboten."

Offenbar ist diese Art von gruseligem Push-Benachrichtigungsverhalten auch dann möglich, wenn die App nicht aktiv ausgeführt wird.

Glücklicherweise gibt es eine einfache Möglichkeit, das potenzielle Schnüffeln zu stoppen, und zwar indem man die Benachrichtigungen für die Apps, die an dieser Aktivität beteiligt sind, einfach deaktiviert.

### Wie man das heimliche Ausspähen von Push-Benachrichtigungen auf dem iPhone verhindert

Die Lösung, um dieses potenzielle Schnüffelverhalten zu verhindern, ist ziemlich einfach: Deaktivieren Sie die Push-Benachrichtigungen für die betreffenden Apps.

1. Rufen Sie auf dem iPhone oder iPad die App "Einstellungen" auf.
2. Scrollen Sie nach unten zu "Benachrichtigungen".
3. Suchen Sie die Apps, für die Sie die Benachrichtigungen deaktivieren möchten (z. B. TikTok, Facebook, Threads usw.)
4. Schalten Sie die Einstellung für "Benachrichtigungen zulassen" auf AUS, um alle Benachrichtigungen für diese App zu deaktivieren.
5. Wiederholen Sie den Vorgang mit anderen Apps, für die Sie dieses potenzielle Verhalten unterbinden möchten.

Ein weiterer Vorteil der Deaktivierung von Push-Benachrichtigungen für viele dieser Anwendungen besteht darin, dass Sie viel weniger von ihnen gestört werden. Müssen Sie wirklich jedes Mal eine Push-Benachrichtigung erhalten, wenn jemand Ihre Inhalte in den sozialen Medien „mag“? Das müssen Sie selbst entscheiden, aber wenn Sie Ihre Konzentration (und offensichtlich auch Ihre Privatsphäre) bewahren wollen, dann wahrscheinlich nicht!

In Anbetracht der Tatsache, dass das Abnehmen von Fingerabdrücken auf Geräten von Apple verboten ist, ist es wahrscheinlich, dass eine zukünftige Version von iOS/iPadOS gegen dieses Verhalten vorgehen und ihm ein Ende setzen wird, oder vielleicht wird Apple dies speziell bei den großen Social Media-Unternehmen, die dies tun, einschränken. Wenn Sie sich diesem potenziellen „Device Creeping“ und den damit verbundenen Folgen nicht aussetzen wollen, deaktivieren Sie einfach die Benachrichtigungen für diese Apps.

Das folgende Video demonstriert das Verhalten in Aktion mit einigen bekannten Social-Media-Apps wie TikTok und Facebook:


Eine Demonstration dieser Aktivität und dieses Verhaltens wurde vom Mysk-Team auf Twitter/X gepostet, wobei der Tweet unten eingebettet ist:


Vielen Dank an CultOfMac für den Hinweis auf diese Studie des Mysk-Teams, die nicht nur uns, sondern jetzt auch Sie aufhorchen lässt.

Verwenden Sie Push-Benachrichtigungen von Social-Media-Apps oder von Apps im Allgemeinen? Was halten Sie von dieser Art von Verhalten? Ich persönlich beschränke die Benachrichtigungen auf einige wenige vertrauenswürdige Apps von Apple, wie Nachrichten, Telefon, Kalender und Erinnerungen, aber das mache ich schon seit langem, um Ablenkungen zu vermeiden. Ich bin auch ein Verfechter des Datenschutzes. Daher ist es für mich ein Bonus zu wissen, dass das Ausschalten von Benachrichtigungen für soziale Medien nicht nur meine Konzentration fördert, sondern auch heimliches Schnüffelverhalten verhindern kann.

# Sichere Wege, sensible Informationen über das Internet weiterzugeben

von Adam Engst, tidbits.com • Übersetzung: KJM

**IBAN**
**DE66XXXXXXXXXXXXX7180**

Irgendwann wurde der Großteil unserer Kommunikation von analog auf digital umgestellt: Briefe und Telefonanrufe wurden zu E-Mails, SMS, Kalendereinträgen und Anrufen per Handy, Internet oder Video. Bei den analogen Methoden gingen wir davon aus, dass unsere Geheimnisse weitgehend sicher bleiben würden. Es war sowohl schwierig als auch illegal (außer für Regierungen), eine Telefonleitung abzuhören oder einen Brief mit Dampf zu öffnen. Wir konnten davon ausgehen, dass unsere private Kommunikation fast immer privat bleiben würde.

Das Internet machte eine weltweite Ausbeutung möglich. Es war nicht mehr nötig, einen bestimmten Brief aus dem Poststrom zu ziehen oder sich Zugang zu einer Telefonleitung oder Vermittlungsstelle zu verschaffen. Die meisten Experten haben unterschätzt, wie ungeschützt die digitale Kommunikation lange Zeit war. Erst vor relativ kurzer Zeit, nämlich vor über zehn Jahren, begann man sich darüber klar zu werden, welche sensiblen Informationen wir unbeabsichtigt und ungeschützt versenden oder speichern, sei es auf unserer eigenen Hardware oder auf entfernten Serverlaufwerken.

Aktivisten, Journalisten, Politiker, Gewerkschaftsfunktionäre und Führungskräfte in der Wirtschaft haben die Hauptlast dieser Probleme zu tragen, da sie einem hohen Risiko ausgesetzt sind, was sie privat sagen, mit welchen Personen sie kommunizieren, wo sie sich befinden und welche finanziellen und medizinischen Daten sie haben. Selbst scheinbar banale Unterhaltungen müssen geschützt werden, da sie Aufschluss geben könnten, und diese Menschen sollten sich über ihre Kommunikationsgewohnheiten und -werkzeuge Gedanken machen.

Aber die meisten Menschen und die meisten Themen erfordern keine strenge Privatsphäre. Wir ziehen es vor, dass ein E-Mail-Thread, in dem das Abendessen von nächster Woche organisiert wird, nicht für die ganze Welt veröffentlicht wird oder sogar von jemandem gelesen wird, für den es nicht bestimmt war, egal wie banal es auch sein mag. Für die alltägliche Kommunikation bieten die vorhandenen digitalen Werkzeuge bereits ausreichend Schutz, und die Folgen einer Offenlegung dieser Daten sind gleich null.

Doch selbst diejenigen von uns, die keine hochrangigen Zielpersonen sind, müssen regelmäßig Informationen weitergeben, die unserer Psyche, unseren Beziehungen, unserer Karriere oder unseren Finanzen schaden könnten, wenn sie in die falschen Hände geraten oder öffentlich bekannt werden. Passwörter sind vielleicht das offensichtlichste Beispiel — der Sinn von Passwörtern ist, dass sie geheim sind. Wenn Sie also ein Passwort weitergeben müssen, sollten Sie sicherstellen, dass nur der vorgesehene Empfänger darauf zugreifen kann. Sobald jemand ein Passwort hat, kann er alle möglichen Informationen über Sie einsehen, extrahieren und ändern.

Der Schutz anderer Arten von Daten kann schwieriger sein, wenn sie konten- und systemübergreifend sind. Finanzielle Informationen stehen dabei ganz oben auf der Liste. Sie geben Ihre Kreditkartendaten bereitwillig an E-Commerce-Websites weiter, weil Sie wissen — oder zumindest erwarten —, dass diese sichere HTTPS-Verbindungen anbieten und die Daten mit der gebotenen Sorgfalt speichern. Aber die Übermittlung Ihrer Kreditkartendaten per E-Mail, um ein Restaurant für ein Gruppenessen zu reservieren, fühlt sich zutiefst falsch an. In den meisten Fällen ist das wahrscheinlich in Ordnung, aber Sie haben keine Ahnung, wer auf das E-Mail-Konto des Restaurants zugreifen kann oder ob die Nachricht gelöscht wird, nachdem die Daten in das Zahlungssystem des Restaurants übertragen wurden.

In anderen Szenarien geht es vielleicht um die Weitergabe von Finanzdaten wie Bankkontodaten, Unterlagen zur Steuererklärung, Rentenplanungsunterlagen usw. Man muss nicht versuchen, Vermögen zu verstecken, um sich unwohl zu fühlen, wenn Unbekannte Ihr Vermögen untersuchen, Ihre Kontonummern kennen und andere Details herausfinden. Was auch immer Sie von Hunter Biden halten, stellen Sie sich vor, wie es wäre, wenn der Inhalt Ihres Laptops extrahiert und für die ganze Welt sichtbar wäre.

Und dann sind da noch die gesundheitsbezogenen Informationen. Wir könnten uns auf einer Cocktailparty über unsere Schmerzen beklagen, hätten aber berechtigte Bedenken, Dokumente über psychische Erkrankungen oder chronische Krankheiten über unsichere Kanäle zu übermitteln. Es klingt zwar altmodisch, von Rivalen und Feinden zu sprechen, aber die Menschen stehen bei Scheidungen, bei der Arbeit und in wettbewerbsintensiven Umgebungen vor Herausforderungen, bei denen die Preisgabe privater Gesundheitsdaten schädlich sein könnte.

### Daten im Ruhezustand und bei der Übermittlung

Was sollten Sie tun, wenn Sie sensible Informationen über das Internet weitergeben müssen? Die Antwort hängt von der Art der Informationen ab, die Sie weitergeben, von den Systemen, die Ihnen zur Verfügung stehen, und von den technischen Möglichkeiten des Empfängers. Ich war neugierig, wie andere vorgehen, und habe eine Diskussion auf TidBITS Talk gestartet, die viele hilfreiche Ratschläge hervorbrachte.

Bevor ich näher auf die Möglichkeiten eingehe, sollten Sie sich überlegen, wie die von Ihnen gesendeten Informationen während der Übertragung und im Ruhezustand an der Quelle und am Zielort geschützt werden:

- **Während der Übertragung**: Um die Sicherheit bei der Übertragung zu gewährleisten und Abhören zu verhindern, sollten Sie sich auf Kommunikationskanäle konzentrieren, die zwischen Ihnen und dem Ziel verschlüsselt sind.

○ **Zwischen Ihrer Anwendung und einem Server**: Fast alle Apps, die wir für die Verbindung mit Internetdiensten verwenden, nutzen HTTPS zum Schutz der Verbindungen. Zu solchen Verbindungen gehören sowohl alle Arten von kontobasierten Ressourcen (überall dort, wo Sie eigene Dateien oder Informationen verwalten) als auch die meisten informationsbasierten Dienste (wie eine Zeitungswebsite). Ein Schloss in der Adressleiste eines Webbrowsers vor einer Domain weist auf HTTPS hin. Sie können auch in jedem Browser die Tastenkombination Command-L drücken und nach https am Anfang der URL suchen.

○ **Ende-zu-Ende-Verschlüsselung**: Noch besser ist die Ende-zu-Ende-Verschlüsselung, die sicherstellt, dass nicht einmal die Organisation, die den Dienst verwaltet, den Datenverkehr entschlüsseln kann. Die Verschlüsselungsschlüssel sind spezifisch für Sie und oft auf jedem Ihrer Geräte verschlüsselt. iMessage (Unterhaltungen mit blauen Blasen in Apples Nachrichten-App), WhatsApp (in einigen Konfigurationen) und Signal (in allen Versionen) sind Ende-zu-Ende-verschlüsselt. Die meisten oder fast alle Ihrer iCloud-Daten sind ebenfalls Ende-zu-Ende-verschlüsselt, je nachdem, ob Sie den erweiterten Datenschutz aktiviert haben (siehe "Apple's Advanced Data Protection Gives You More Keys to iCloud Data", 8. Dezember 2022). Chat-Systeme wie Slack sind verschlüsselt, aber in der Regel nicht Ende-zu-Ende-verschlüsselt, sodass Ihre Daten zwar vor Abhörern, nicht aber vor Mitarbeitern des Dienstes oder Server-Administratoren geschützt sind. SMS-Nachrichten (Konversation mit grüner Blase in Messages) sind überhaupt nicht verschlüsselt.

- **Im Ruhezustand**: Daten gelten als im Ruhezustand, wenn sie an einem Zielort gespeichert sind, z. B. auf einer SSD auf Ihrem Computer, auf den Mailservern von Ihnen und dem Empfänger oder im Datenzentrum eines Cloud-Speicherdienstes. Viele Dienste verschlüsseln Daten im Ruhezustand, obwohl ich nicht glaube, dass dies bei IMAP-E-Mails üblich ist. Wenn ein Konto kompromittiert wird, ist die Verschlüsselung im Ruhezustand jedoch weitgehend irrelevant. Es gibt zwei Möglichkeiten, mit diesem Problem umzugehen:

○ **Verschlüsselung pro Datei oder pro Nachricht**: Sie können die Daten vor dem Senden verschlüsseln, so dass sie ohne ein von Ihnen festgelegtes Kennwort nicht entschlüsselt werden können. Dies verhindert, dass jemand, der ein E-Mail-Konto oder ein Cloud-Speicher-Konto entführt, wertvolle Details aus dem Inhalt herauslesen kann. Um solche Daten zu schützen, müssen Sie das Kennwort an den Empfänger *„out of band“* senden: Verwenden Sie einen völlig anderen Kommunikationskanal, z. B. einen Telefonanruf oder einen Ende-zu-Ende-verschlüsselten Chat. Auf diese Weise kann jemand, der auf einen verschlüsselten Dateianhang in Google Mail zugreifen könnte, nicht auch auf das in Messages gesendete Kennwort zugreifen.

○ **Zeit- oder Nutzungsablauf**: Wenn Sie befürchten, dass eine Datei über einen längeren Zeitraum irgendwo gespeichert wird, unabhängig davon, wie wahrscheinlich es ist, dass sie gestohlen wird, können Sie einen Link zu den Informationen senden, der nach einer kurzen Zeit abläuft. Dadurch wird das Zeitfenster, in dem ein Verstoß stattfinden könnte, drastisch verkleinert. Einige Dienste können auch Links senden, auf die nur eine bestimmte Anzahl von Zugriffen möglich ist, so dass sie danach unbrauchbar werden.

### Lösungen für den sicheren Informationsaustausch

Um all dies in einer spezifischen Lösung zu vereinen, müssen Sie sich Gedanken über vier Bereiche machen:

- **Zielgruppe**: Mit wem tauschen Sie Informationen aus, und welche technischen Möglichkeiten haben diese Personen? E-Mail bietet keinen Schutz durch Verschlüsselung bei der Übertragung oder im Ruhezustand, es sei denn, Sie verlangen von Ihren Empfängern, dass sie sich für ein Sicherheitssystem entscheiden (PGP ist das gebräuchlichste) — jahrzehntelange Versuche haben noch nicht dazu geführt, dass dies auf breiter Basis geschieht. Dennoch ist die E-Mail in der Regel der einfachste Weg, um mit einem technisch unbedarften Empfänger zu kommunizieren. Nachrichten sind einfach und sicher, aber nur, wenn Sie sich ausschließlich auf iMessage verlassen können, was die Nutzung auf diejenigen beschränkt, die Apple-Geräte verwenden. WhatsApp und Signal sind ebenfalls gut geeignet, aber nur, wenn sowohl Sie als auch Ihr Empfänger sie nutzen.

- **Inhalt**: Was möchten Sie mitteilen? Die Weitergabe einer winzigen Information wie eines Passworts ist etwas anderes als der Aufwand für die Weitergabe eines Dokuments, und die Art der Weitergabe eines Dokuments kann variieren, wenn es in eine PDF-Datei umgewandelt werden kann oder in einem nativen Format wie einer Tabellenkalkulation bleiben muss.

- **Wichtigkeit**: Wie problematisch wäre es, wenn die vertraulichen Informationen, die Sie weitergeben, in die falschen Hände gerieten? Es ist ein himmelweiter Unterschied zwischen den Zugangsdaten zu Ihrem Rentenkonto und dem Passwort für ein Konto, mit dem Sie die WordPress-Website Ihres Gemeindezentrums bearbeiten können.

- **Dauerhaftigkeit**: Wie lange braucht Ihr Empfänger die Daten? Müssen sie nur einen Blick auf etwas werfen und es dann löschen? Müssen sie eine Kopie dauerhaft aufbewahren? Sie können zwar keine Dateien von den

Geräten einer anderen Person löschen, aber Sie können dafür sorgen, dass die Daten nicht im Internet bleiben.

Hier sind also meine Empfehlungen:

- **Sicherer Dienst** wie DocuSign: Wenn Sie mit einem Arzt, einem Anwalt, einem Buchhalter oder einem anderen Fachmann zusammenarbeiten, der regelmäßig vertrauliche Informationen von seinen Kunden erhalten muss, wird dieser häufig ein sicheres Portal für Nachrichten und Dateiübertragungen verwenden. Dabei kann es sich um ein benutzerdefiniertes System handeln - viele wurden als Lösungen für diese Branchen entwickelt - oder sie verlassen sich auf ein allgemein verfügbares kommerzielles Angebot wie DocuSign, um vertrauliche Dokumente hochzuladen. Bleiben Sie auf jeden Fall bei dem, was sie verlangen, es sei denn, Sie haben guten Grund zu der Annahme, dass ihre IT-Mitarbeiter technisch inkompetent sind.

- **iMessage/Signal/WhatsApp**: Wenn Sie etwas Vertrauliches austauschen möchten, ist es nicht verkehrt, iMessage oder einen gleichwertigen sicheren Dienst wie Signal oder WhatsApp zu verwenden. (Informieren Sie sich über WhatsApp, um sicherzustellen, dass Sie keine Chat-Archive preisgeben.) Dennoch verwende ich diese Dienste lieber, um Informationen auszutauschen, die für sich allein genommen nicht nützlich sind. Wenn Sie z. B. jemandem ein Kennwort senden müssen, geben Sie ihm die Anmelde-URL und den Benutzernamen zusammen mit den erforderlichen Anweisungen in einer E-Mail, aber senden Sie das Kennwort separat in Nachrichten.

- **1ty.me** oder **One-Time-Secret-Link** zur Selbstzerstörung: Wenn ich jemandem einen Benutzernamen und ein Kennwort für eine nicht kritische Website senden möchte, verwende ich oft 1ty.me oder One-Time Secret, um einen verschlüsselten Link zu erstellen, der den Text enthält. Diesen Link gebe ich dann per E-Mail weiter und fordere den Empfänger auf, ihn sofort zu öffnen. Sobald der Empfänger den verschlüsselten Link anschaut, löscht der Server die Daten, und der Link zerstört sich selbst — er ist tot und kann nicht mehr verwendet werden. Ein Angreifer könnte die Kommunikation belauschen oder auf die E-Mail zugreifen, bevor sie gelesen wurde. Wenn der Empfänger jedoch erfährt, dass der Link sich bereits selbst zerstört hat, weiß er, dass er kompromittiert wurde und kann mich alarmieren. Die Wahrscheinlichkeit ist sehr gering, dass jemand, der nicht zu den Hochrisikogruppen gehört, jemals damit konfrontiert wird. Wahrscheinlicher ist, dass das Problem von einem E-Mail-System ausgeht, das Nachrichten scannt und Links zum Schutz vor Schadsoftware verfolgt, wodurch der Link vorzeitig zerstört wird.

- **1Passwort-beschränkter Link**: Wenn ich ein Passwort für ein Konto freigeben muss, das ich selbst verwende und nicht für jemand anderen erstellt wurde, verwende ich die Freigabefunktion von 1Password, um einen Link zu erhalten, wie ihn 1ty.me erstellt. Bei 1Password können Sie ein Ablaufdatum festlegen, den Link auf die Personen beschränken, deren E-Mail-Adressen Sie eingeben, und dafür sorgen, dass er sich selbst zerstört, nachdem er einmal angesehen wurde. Andere Passwort-Manager verfügen möglicherweise über ähnliche Freigabefunktionen.

- **Passwortgeschütztes PDF**: Die Freigabe eines sensiblen Dokuments, das ausgedruckt werden könnte, erfolgt am besten durch die Erstellung einer kennwortgeschützten PDF-Datei. Wählen Sie dazu in einer beliebigen Anwendung Datei > Drucken > PDF > Als PDF speichern. Klicken Sie auf die Schaltfläche Sicherheitsoptionen, klicken Sie auf „Zum Öffnen des Dokuments ein Kennwort verlangen“ und geben Sie ein Kennwort ein. Die Erstellung eines sicheren Kennworts ist wichtig, da viele Online-Dienste schwache Kennwörter aus PDFs entfernen können. Speichern Sie das Dokument und geben Sie es auf beliebige Weise weiter, aber stellen Sie sicher, dass Sie das Kennwort über einen anderen Kanal weitergeben.

- **Passwortgeschütztes Disk-Image**: Für Dateien, die sich nicht so einfach in eine PDF-Datei umwandeln lassen, oder um eine Sammlung von Dateien weiterzugeben, kann die Erstellung eines kennwortgeschützten Disk-Images für Mac-Benutzer hilfreich sein. (Benutzer anderer Plattformen können Mac-Datenträgerabbilder öffnen, aber es kann schwierig sein oder besondere Software oder Einstellungen beim Erstellen des Datenträgerabbilds erfordern). Erstellen Sie im Festplattendienstprogramm ein neues komprimiertes Disk-Image (am einfachsten ist Datei > Neues Image > Image aus Ordner), wählen Sie eine der beiden Optionen aus dem Einblendmenü Verschlüsselung (verwenden Sie 256-Bit für sensiblere Daten) und geben Sie nach Aufforderung ein sicheres Passwort ein. Auch hier sollten Sie das Passwort in einem anderen Kanal weitergeben.

- **Kennwortgeschütztes Zip-Archiv**: Ein kennwortgeschütztes Zip-Archiv dient demselben Zweck wie ein kennwortgeschütztes Disk-Image und kann von jemandem, der Windows oder eine andere Plattform verwendet, leichter entpackt werden. Wenn Sie Keka von seiner Website (nicht aus dem Mac App Store) herunterladen, können Sie kostenlos passwortgeschützte Zip-Archive erstellen; wenn Sie regelmäßig solche Archive erstellen, sollten Sie sich BetterZip ansehen. Am schnellsten geht es jedoch, wenn Sie ein kennwortgeschütztes Zip-Archiv auf Ihrem Desktop über die Befehlszeile erstellen. Gehen Sie wie folgt vor:

1. Öffnen Sie Terminal.
2. Geben Sie zip -er ~/Desktop/wunschdateiname.zip ein und drücken Sie einmal die Leertaste.
3. Ziehen Sie die Datei oder die Dateien, die Sie freigeben möchten, in das Terminal-Fenster.
4. Drücken Sie die Eingabetaste.
5. Geben Sie das gewünschte Kennwort ein und bestätigen Sie es, wenn Sie dazu aufgefordert werden. Geben Sie es sorgfältig ein; Sie können die Zeichen, die Sie eingeben, nicht sehen.

- **Cloud-Speicher-Link, der ablaufen kann**: Ich weiß nicht, wie weit diese Funktion verbreitet ist, aber einige Cloud-Speicherdienste bieten die Möglichkeit eines zeitlich begrenzten Links an. Damit können Sie eine Datei für eine andere Person freigeben und gleichzeitig sicherstellen, dass der Link nach einer bestimmten Zeit gelöscht wird, um zu verhindern, dass er bei einem Verstoß entdeckt und später verwendet wird. Dropbox unterstützt solche Links, wenn Sie ein Dropbox Professional-Konto haben. (Außerdem habe ich Linkly noch nicht verwendet, das wie ein vollwertiger Linkverkürzungsdienst aussieht, aber man könnte es theoretisch verwenden, um einen zeitlich begrenzten Link zu erstellen, der auf eine freigegebene Datei in einem Cloud-Speicherdienst verweist).

Wie Sie sehen, gibt es keine Einheitslösung, wenn es um den sicheren Austausch von Informationen über das Internet geht. Was auch immer Ihre Bedürfnisse sind, eine der oben genannten Optionen sollte ausreichen.