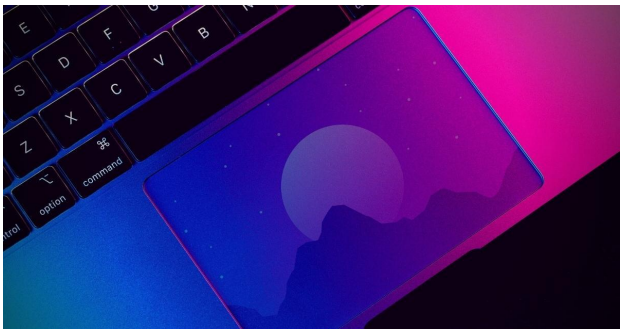
10 Annahmen über macOS-Sicherheit, die Ihre Arbeit gefährden

von Phil Stokes, sentinelone.com/blog/ • Übersetzung: KJM

Der Artikel erschien bereits im Februar 2022, aber Phil Stokes' Gedanken über die Gefährdung von Macs sind nach wie vor interessant und wichtig.



Macs sind großartig, nicht wahr? Ich habe viele. Abgesehen von den beiden, die mir mein Arbeitgeber zur Verfügung stellt, habe ich selbst fünf funktionierende Macs, die von 2009 bis 2021 reichen. Zu Forschungszwecken lasse ich außerdem macOS auf einer Reihe von virtuellen Maschinen laufen. Wenn du mir ein paar Minuten Zeit gibst, kann ich dir eine Instanz jeder macOS-Version von 10.5.8 Leopard (ca. 2008!) bis hin zur neuesten Beta von macOS 12 Monterey aufspielen. Ja, ich bin ein Apple-Nerd, ein Mac-Freak, ein macOS-Enthusiast, und ich habe über ein Jahrzehnt damit verbracht, zu lernen, wie Macs und macOS funktionieren. Ich bin auch Mac-Sicherheitsforscher, und ein Katalog älterer macOS-Versionen ist Teil meines Arsenals an Werkzeugen, wenn es darum geht zu verstehen, wie Macs und Mac-Benutzer sicher gehalten werden können.

Der Großteil meiner Arbeit dreht sich heute um die Identifizierung, das Aufspüren und das Verständnis von Mac-Malware in Unternehmen, und im Laufe meiner Arbeit stoße ich unweigerlich auf mehr als nur einen fairen Anteil an infizierten Macs. Die Benutzer dieser Macs sind meist überrascht, wenn sie erfahren, dass ihr Mac mit bösartiger Adware oder Malware infiziert ist.

Nur wenige wissen, wie die Malware auf ihr Gerät gelangt ist. Die meisten dachten, sie bräuchten keine besonderen Sicherheitsvorkehrungen zu treffen, wenn sie einen Mac benutzen. Einige sagten, dass der Verzicht auf AV-Produkte genau der Grund war, warum sie sich für einen Mac entschieden und ihren früheren Windows-Rechner aufgegeben haben. Alle hatten keine Ahnung, wie sie die Infektion entfernen oder überprüfen konnten, ob der Mac tatsächlich gesund war, nachdem sie es versucht hatten. Oft sind IT-Teams, die für die Behebung von Problemen mit Windows-Geräten geschult und beauftragt sind, bezüglich Mac-Problemen ebenso unsicher.

In diesem Beitrag erzähle ich Ihnen, was ich diesen und vielen anderen Benutzern über die Sicherheit von macOS erzählt habe. Ich werde mit einigen weit verbreiteten Mythen über die sichere Verwendung und Verwaltung von Macs aufräumen und erklären, wie Sie sicherstellen können, dass Ihre Mitarbeiter nicht die nächsten unglücklichen Mac-Benutzer sind, die auf gefährliche Weise im Internet nach einer Lösung für ein Problem suchen, von dem sie kaum wussten, dass sie es haben.

1. Ich muss mein System nicht aktualisieren

Viele Menschen glauben, dass ältere Versionen von macOS genauso sicher sind wie die neuesten Versionen. Zwar erhalten macOS Monterey, Big Sur und Catalina derzeit noch kritische Sicherheitsupdates, aber alles, was älter ist, ist mit Sicherheit mit Sicherheitslücken behaftet.

Ein größeres Problem sind jedoch Geräte, die zwar die neuesten Updates erhalten, aber nicht mit den alltäglichen Aktualisierungen Schritt halten. Aus der Sicherheitsperspektive sind Punkt-Updates (z. B. von Monterey 12.1 auf 12.2 usw.) viel wichtiger als Betriebssystem-Upgrades, zumindest solange Sie nicht mehr als N-2 (mehr als zwei Haupt-Upgrades hinter dem aktuellen Betriebssystem) sind. Wenn Sie noch mit Catalina oder Big Sur arbeiten, sind die einzigen sicheren Versionen dieser Betriebssysteme die neuesten: 10.15.7 + das Sicherheitsupdate vom 26. Januar bzw. 11.6.3. Zum Zeitpunkt der Erstellung dieses Artikels ist Monterey auf 12.2.

Der Grund dafür, dass Punkt-Updates weitaus wichtiger sind, liegt darin, dass sie im Gegensatz zu größeren Betriebssystem-Upgrades, die aus Marketinggründen zeitlich festgelegt werden und in der Regel neue (und manchmal fehlerhafte!) Funktionen hinzufügen, in der Regel auf die Behebung von Fehlern und Sicherheitslücken ausgerichtet sind, einschließlich Schwachstellen, von denen bekannt ist, dass sie in freier Wildbahn aktiv ausgenutzt werden. In der jüngsten Aktualisierung 12.2 hat Apple beispielsweise die Sicherheitslücke CVE-2022-22587 geschlossen, von der es heißt, dass es „Kenntnis von einem Bericht hat, wonach dieses Problem aktiv ausgenutzt worden sein könnte". Mit dieser Aktualisierung wurden auch zwölf andere CVEs behoben, darunter:

- CVE-2022-22586 - AMD-Kernel: Eine bösartige Anwendung kann möglicherweise beliebigen Code mit den Rechten des Kernels ausführen
- CVE-2022-22584 - ColorSync: Die Verarbeitung einer in bösartiger Weise erstellten Datei kann zur Ausführung von beliebigem Code führen
- CVE-2022-22591 - Intel-Grafiktreiber: Eine bösartige Anwendung kann möglicherweise beliebigen Code mit Kernel-Privilegien ausführen

Kürzlich betrat ich einen Apple Reseller Store und stellte mit einiger Überraschung fest, dass neben dem Mac, auf dem die Kassensoftware lief, andere Mitarbeiter ein MacBook Pro aus dem Jahr 2012 verwendeten. Woher ich das wusste? Weil das letzte Jahr, in dem Apple ein MacBook mit internem CD-Laufwerk hergestellt hat, 2012 war, und ich konnte den verräterischen Schlitz an der Seite des Geräts sehen, als ich darauf wartete, meinen Einkauf zu tätigen.

Es ist ein Beweis für die Langlebigkeit der Apple Hardware, dass ein Unternehmen im Jahr 2022 immer noch ein Gerät aus dem Jahr 2012 für produktive Aufgaben verwenden kann, aber es ist auch ein potenzielles Problem. Das MBP aus der Mitte des Jahres 2012 wurde mit OS X 10.8 Mountain Lion veröffentlicht! Die neueste Version von macOS, die auf einem MacBook Pro aus der Mitte des Jahres 2012 laufen könnte, ist Big Sur. Ich hoffe sehr, dass sie auf die 11.6.3 Version von letzter Woche aktualisiert haben!

Apple veröffentlicht keine punktuellen Updates nach einem Zeitplan wie Microsofts „Patch Tuesday“. Sie bringen sie heraus, wenn etwas Dringendes zu beheben ist, und das ist in der Regel eine Sicherheitslücke. Die Grundlage jeder Computersicherheit ist es, mit Software-Updates auf dem Laufenden zu bleiben. Sorgen Sie dafür, dass Ihre Benutzer auf dem neuesten Stand sind!

2. Mac-Malware ist rar

Die Menge an Malware, die auf Windows-Rechner abzielt, ist wirklich atemberaubend. Kein Wunder, dass sich jedes Jahr eine nicht unerhebliche Zahl von Computerkäufern für einen Mac entscheidet, um den ständigen Sicherheitsproblemen von Windows zu entgehen. Die Menge an Malware, die auf Macs abzielt, ist zwar nur ein kleiner Prozentsatz davon, aber ein kleiner Prozentsatz einer großen Zahl kann immer noch eine große Zahl sein. Im Vergleich zu Windows ist Mac-Malware viel seltener, aber noch lange nicht "selten".

Im vergangenen Jahr sind 10 neue zielgerichtete macOS-Malware-Familien aufgetaucht, und auch die Verbreitung von Adware-Plattformen wie Shlayer, Bundlore, Surfbuyer, Pirrit, WizardUpdate und Adload hat weiter zugenommen.

Im Jahr 2021 sagte Craig Federighi — Apples VP of Software Engineering — dass er „einige Familienmitglieder habe, die Malware auf ihren Macs hatten“. In einem Kommentar, der viele Mac-Benutzer, aber absolut keine Sicherheitsforscher überraschte, merkte Federighi weiter an, dass „Apple jede Woche ein paar Malware-Stücke selbst oder mit Hilfe von Dritten identifiziert“ und dass Apple „ein endloses Spiel von Whack-a-Mole“ kämpfe und jetzt ein „wesentlich größeres Malware-Problem“ habe als in der Vergangenheit.

Hören Sie auf Craig. Lustigerweise weiß er, wovon er spricht! Nehmen Sie die Bedrohung durch macOS-Malware ernst.

3. Adware ist nicht gefährlich

Für diejenigen, die diese Ansicht vertreten, lautet meine erste Reaktion: Definieren Sie „gefährlich“.

Adware ist ein Code, der auf Ihrem Computer läuft, oft ohne Ihr Wissen oder Ihre Zustimmung, der Fingerabdrücke von Ihrem Gerät nimmt und personenbezogene Daten über Sie sammelt, diese an unbekannte Dritte weitergibt und Persistenzagenten installiert, die sich nur schwer entfernen lassen und — wie der Name schon sagt — unerwünschte Werbung anzeigen, während Sie surfen, indem sie Ihre Suchanfragen kapern.

Adware wie Adload und Shlayer kontaktieren in der Regel obskure URLs und laden im Hintergrund unerwünschte Software herunter, ohne den Benutzer zu informieren.

Manche Adware ähnelt Spyware, und einige Adware-Entwickler ergreifen so extreme Maßnahmen, um eine Erkennung durch Sicherheitssoftware oder eine Analyse durch Sicherheitsexperten zu vermeiden, dass sie durchaus in das Geschäft einsteigen und Malware-Autoren ein paar neue Tricks beibringen könnten. Wie lautet also Ihre Definition von „gefährlich“?

Jeder Code von Drittanbietern, der auf Ihren Rechnern ohne die ausdrückliche Genehmigung des Benutzers und/oder des Unternehmens ausgeführt wird, sollte als Gefahr für das Unternehmen betrachtet werden. Aus dieser Sicht ist Adware nur eine Art von Malware und sollte auch so behandelt werden.

4. Apple ist die Sicherheit, die Sie brauchen

Apple hat hart daran gearbeitet, sich den Ruf vom „sicheren Mac“ zu erarbeiten, aber die Kluft zwischen der Marketing-Botschaft und der Realität wird immer deutlicher sichtbar. Es ist nicht so, dass Apple die Sicherheit nicht ernst nimmt — das tut es wirklich, und wir freuen uns immer, das Apple-Produktsicherheitsteam zu unterstützen, indem wir Informationen weitergeben, wenn wir können. Das Problem ist, dass Apples Sicherheitstechnologien auf macOS leicht zu überwinden sind, und es lohnt sich, kurz zu untersuchen, warum das so ist.

Im Gegensatz zu iOS und mobilen Apple-Geräten bieten macOS und der Mac eine Umgebung, in der Gerätebesitzer ihre Computer auf alle möglichen neuartigen, interessanten und kreativen Arten anpassen und nutzen können — und wir hoffen, dass dies immer so bleiben wird. Der Anwendungsfall für eine leistungsstarke Computerplattform unterscheidet sich grundlegend von dem eines mobilen Geräts, und aus diesem Grund kann Apple nur so viel für die Sicherheit tun, dass es nicht in die Falle tappt, in die Microsoft getappt ist, nämlich zum Nachrüstungsanbieter zu werden, um die Sicherheit seines eigenen Betriebssystems zu verbessern.

Beim Mac geht Apple mit Bedacht vor. Gatekeeper, Codesigning und Notarisierung stellen zwar Zugangsbarrieren dar, aber die halten professionelle Adware- und Malware-Autoren nicht ab. Schutzprogramme auf dem Gerät wie XProtect und MRT.app helfen auch bei der Beseitigung einiger der wichtigsten entdeckten Malware- und Adware-Varianten, aber es gibt viele, die sie nicht abwehren können. XProtect ist eine altmodische Technologie zum Scannen von Dateien, die aktualisiert werden muss (was Apple unbemerkt im Hintergrund tut, mehr oder weniger einmal im Monat), nachdem neue Malware bereits einige unglückliche Opfer getroffen hat.

Entscheidend ist, dass es für Malware-Autoren einfach ist, XProtect auf ihren eigenen Rechnern zu überprüfen und zu sehen, wie die Signaturen ihre Arbeit erkennen. MRT.app ist etwas schwieriger zu untersuchen, aber unabhängig davon, wie gut Apple versucht, seine Signaturen zu verschleiern, gibt es für Malware-Autoren immer einen einfachen Test: Testen Sie Ihre Malware auf Ihrem Mac, und wenn sie entfernt oder blockiert wird, passen Sie sie so lange an, bis sie es nicht mehr wird.

Malware-Autoren haben immer direkten Zugriff auf genau die Software, die Apple zum Blockieren oder Entfernen von Malware einsetzt. Teilweise sollte die Notarisierung Apple dabei helfen, dies zu umgehen, aber die Bedrohungsakteure entdeckten bald, dass der automatisierte Malware-Dienst überlistet werden kann, und das Spiel "Whack-a-mole", wie Herr Federighi es zu Recht beschrieb, geht weiter.

Wenn Sie dazu beitragen wollen, dass Ihre Macs sicher bleiben, sorgen Sie für zusätzliche Sicherheit!

5. Ich wüsste, wenn mein Mac infiziert wäre

Eine der am meisten übersehenen Schwächen des Macs ist der Mangel an Endbenutzer-Tools, die er sowohl für Sicherheits- als auch für Verwaltungszwecke bereitstellt. Die einst nützliche Console.app ist heute nur noch eine No-Go-Zone außer für die masochistischsten Mac-Fanatiker; das Terminal bietet einige nützliche, aber obskure Befehlszeilen-Tools, um Dinge wie laufende Prozesse zu untersuchen, offene Dateien und Ports aufzulisten und bestimmte Arten von System- und Benutzerdaten zu sammeln.

Aber — und das ist ein großes Aber — keines dieser Tools bietet Benutzern oder Administratoren eine tatsächliche Möglichkeit, bösartige Änderungen zu betrachten, zu verfolgen oder zu identifizieren. Keines der nativen Tools ermöglicht es einem Benutzer zu sehen, welcher Prozess für die Änderung welcher Datei(en), die Ausführung welcher Binärdateien oder die Änderung welcher Systemdaten verantwortlich war.

Deep-Dive IR- und Digital-Forensik-Untersuchungen können manchmal bestimmte historische Ereignisketten wiederherstellen, aber das erfordert Fachwissen, Zeit und Geld.

Kurz gesagt, die Frage, die kein Mac-Benutzer wirklich beantworten kann, ohne eine Software eines Drittanbieters hinzuzufügen, lautet: Wie kann ich wissen, ob mein Mac durch eine Backdoor wie SysJoker oder Spyware wie DazzleSpy oder XcodeSpy infiziert wurde?

Für Unternehmen ist die einzig sinnvolle Wahl eine Sicherheitslösung, die einen tiefen Einblick sowie erweiterten Schutz und Erkennung bietet.

6. Meine Daten sind auf meinem Mac sicher

Der Datenschutz hat in den letzten Jahren zunehmend an Bedeutung gewonnen und wird immer stärker ins Visier genommen, da fast jeder von uns einige oder alle seiner sensiblen Daten auf seine Geräte verlagert hat.

Im Einklang mit diesem Trend hat Apple eine Reihe von Änderungen an macOS vorgenommen, um zu versuchen, personenbezogene Daten und andere Daten auf unseren Macs zu schützen, aber die Ergebnisse waren alles andere als glänzend. Zunächst einmal werden alle Datenschutzmaßnahmen von Apple von jeder Anwendung umgangen, die vollen Festplattenzugriff (Full Disk Access, FDA) anfordert und vom Benutzer gewährt wird. Apple geht standardmäßig davon aus, dass die Benutzer diese Erlaubnis nicht erteilen, ohne die Risiken zu kennen, aber diese Annahme hat einen fatalen Fehler. Viele gängige Anwendungen benötigen diese Erlaubnis, um ordnungsgemäß zu funktionieren, und die Benutzer sind mehr daran interessiert, dass die Anwendungen funktionieren, als sich bei den Entwicklern eingehend darüber zu erkundigen, wie diese Erlaubnis verwendet wird oder missbraucht werden könnte.

Eine Anwendung, die unabhängig von den Einstellungen des Benutzers vollen Festplattenzugriff hat, ist Apples eigener Finder. Dies ermöglicht eine heimtückische Hintertür über eine Automatisierung, die nur einen Zustimmungsklick (statt einer Passwortautorisierung) erfordert, um an den Benutzern vorbeizukommen.

Außerdem verlangen die Administratoren in vielen Unternehmen, dass das Terminal vollen Festplattenzugriff hat. Leider gibt es hier keine Granularität, d. h. wenn ein Benutzer FDA für das Terminal gewährt, ist es nun für alle Benutzer (und alle Prozesse) verfügbar.

Wie bereits erwähnt, handelt es sich hierbei nicht um einen Unfall oder einen Fehler, sondern um ein Design, aber Fehler in demselben Framework (auch bekannt als TCC), das für den Schutz der Benutzerdaten verantwortlich ist, sind so häufig geworden, dass sie fast uninteressant sind!

Vergewissern Sie sich, dass Sie genau wissen, was vom Betriebssystem geschützt wird und was nicht und unter welchen Bedingungen.

7. Kriminelle interessieren sich nicht für Mac-User

Es ist ein weit verbreiteter Mythos in der Computersicherheit, dass die meisten Malware-Autoren nicht an Mac-Benutzern interessiert sind, weil „der Markt zu klein“ ist, um ihre Zeit wert zu sein. Schließlich, so wird angenommen, erfordert die Entwicklung, Verbreitung und Verwaltung von Malware-Infektionen eine beträchtliche Investition in Ressourcen, und für diesen Aufwand wollen die Kriminellen einen guten ROI. Daher, so die Annahme, machen sie sich nicht die Mühe, Macs ins Visier zu nehmen, sondern halten sich an die leichtere Beute der Windows-Benutzer.

Hier gibt es eine Menge Trugschlüsse aufzudecken. Erstens: Der Markt ist zu klein? Dieses Denken ist etwa 15 Jahre veraltet, genauer gesagt vor der Markteinführung des iPhones 2007. Macs waren vielleicht einmal ein Nischenprodukt für bestimmte „Kreative“ und ein paar lautstarke Enthusiasten, aber ihr Marktanteil ist in den letzten zehn Jahren stetig gestiegen.

Zunächst war dies auf die Integration des Ökosystems von iOS und macOS (bzw. OS X, wie es damals hieß) zurückzuführen, aber seit langem sind Macs aufgrund ihrer Langlebigkeit, Stabilität und — im Vergleich zu Windows — Sicherheit auch für sich genommen beliebt. Entwickler aller Couleur lieben sie, Führungskräfte lieben sie, und im letzten Quartal meldete Apple, dass allein die Mac-Verkäufe einen Umsatz von über 10 Milliarden Dollar ausmachten. Das ist für jeden Malware-Autor ein ziemlich großer Markt, den es anzugreifen gilt — fragen Sie einfach die Entwickler von XLoader, XCSSET und OSAMiner.

Zweitens ist Mac-Malware nicht besonders schwer zu erstellen. Wenn Sie eine beliebige Mac-Anwendung erstellen können, ist es ein ziemlich triviales Unterfangen, sie dazu zu bringen, etwas Bösartiges zu tun (eine bedauerliche Tatsache, die es für bestimmte Arten von Sicherheitslösungen, die sich auf die Identifizierung von Malware anhand von Dateimerkmalen und nicht anhand des Verhaltens verlassen, schwierig macht, macOS-Malware zu erkennen). Hinzu kommt, dass macOS-Malware zunehmend plattformübergreifend ist - Malware-Autoren zielen mit demselben Quellcode, der in Sprachen wie Java, Go und Kotlin geschrieben ist, auf mehrere Plattformen ab - und das Argument "hohe Investitionen ohne Ertrag" ist nicht wirklich stichhaltig.

Sicherlich zählt Adware zu den häufigsten und profitabelsten Bedrohungen auf Macs, aber die sind nicht so weit gekommen, weil sie nur von einem "versierten Benutzer" gestoppt werden konnten.

8. Nationalstaaten haben es nicht auf Mac-Benutzer abgesehen

Wenn die Kriminellen, die auf das schnelle Geld aus sind, an Bord sind, was ist dann mit den APTs *(Advanced Persistent Threats: „fortgeschrittene andauernde Bedrohungen“)* Wie bereits erwähnt, kaufen Entwickler und Führungskräfte gerne Macs — sie sind leistungsfähig und schick —, und sie haben den Ruf, sicher zu sein (auch wenn wir feststellen, dass es inzwischen Chromebooks sind, die jetzt das Meme „die bekommen keine Viren“ genießen).

APTs hatten es schon immer auf Macs abgesehen, genauso wie auf alle anderen Geräte, die von „Personen von Interesse“ verwendet werden. Im vergangenen Jahr gab es nicht nur gezielte Angriffe auf politische Aktivisten, sondern auch sehr wahrscheinlich einen Spionageangriff auf ein US-Unternehmen.

Im letzten Monat haben wir außerdem erfahren, dass die meisten Mac-Malware-Programme zwar ein gewisses Maß an Social Engineering erfordern, es aber auch „wilde“ Exploits gibt, die einen Mac-Benutzer infizieren können, wenn er einfach die falsche Website besucht. Sowohl macOS.Macma als auch OSX.DazzleSpy wurden durch die Ausnutzung von Sicherheitslücken verbreitet, um Code mit Privilegien in einem Watering-Hole-Angriff abzulegen und auszuführen. Und wie bereits erwähnt, war CVE-2022-22587, das vor einigen Wochen gepatcht wurde, ein aktiv ausgenutzter Zero-Day, der böswilligen Angreifern die Ausführung von beliebigem Code mit Kernel-Rechten ermöglichte. Zu diesem Zeitpunkt wissen wir nicht, wer oder was die Ziele waren.

Möchten Sie gezielte Malware stoppen? Investieren Sie in eine EDR *(Endpoint Detection Response)*, die Agenten anbietet, die nativ auf Mac-Architekturen, sowohl Intel als auch auf arm64 (auch bekannt als Apple Silicon), laufen.

9. Aus dem App Store geladene Apps sind sicher

Apps aus dem Mac App Store genießen wie die aus dem iOS App Store einen privilegierten Platz in Apples Ökosystem. Solche Apps laufen in Sandbox-Umgebungen auf dem Gerät des Benutzers, werden von Apple geprüft und von ausgewiesenen Entwicklern vertrieben. Die große Mehrheit ist in der Tat sicher, das steht außer Frage. Aber es gibt dennoch Fragen zu einer kleinen Minderheit.

Die meisten App Store-Anwendungen sind sicher, aber die Herkunft des Downloads ist keine Garantie dafür, dass Sie keine Malware erhalten. Entwickler legitimer App Store-Apps haben festgestellt, dass betrügerische Apps im App Store legitime Apps kopieren und mit gefälschten Bewertungen und Rezensionen versehen sind, die wiederum massenhaft von anderen Kriminellen gekauft wurden. Es wird geschätzt, dass solche Apps die Nutzer um 2 Millionen Dollar oder mehr pro Jahr betrügen könnten.

Wenn die in Apple eingebauten Schutzmechanismen Betrug und Malware nicht erkennen und blockieren können, sind Nutzer ohne andere Schutzmechanismen ziemlich schutzlos.

10. Die besten Sicherheits-Apps gibt es im App Store

Wenn Sie auf der Suche nach einer zusätzlichen Sicherheitslösung für Ihren Mac sind, sollten Sie *nicht* im App Store suchen. Das hat nichts mit unserem vorherigen Punkt über die Fragwürdigkeit einiger App Store-Apps zu tun, sondern vielmehr mit der Art der im App Store zugelassenen Apps.

Wie wir bereits sagten, müssen Apps im App Store mit einer Sandbox versehen sein — das ist eine der Zugangsbedingungen von Apple —, aber eine gute Sicherheits-App kann schon per Definition nicht in einer Sandbox-Umgebung funktionieren. Eine Sandbox ist eine Art Container, der eine App von anderen Apps und anderen Daten auf einem Gerät isoliert. Sie ist eine von mehreren Techniken, die eingesetzt werden können, um bestimmte Arten von Anwendungen sicherer zu machen.

Es gibt jedoch keine effektive Sicherheits-App mit Sandbox. Sogenannte „Sicherheits-Apps“, die im App Store zu finden sind, haben keinen Einblick in andere Prozesse und sind gar nicht in der Lage, Malware auf Ihrem Gerät zu blockieren oder zu entfernen (die selbst fast immer ohne Sandbox arbeitet). Im Großen und Ganzen sind sie im besten Fall nutzlos und im schlimmsten Fall betrügerisch.

Wenn Sie eine wirksame Sicherheit wünschen, benötigen Sie eine Lösung, die Ihr Gerät tatsächlich vor Bedrohungen schützt und Einblick in böswillige Aktionen bietet; mit anderen Worten: Sie brauchen etwas, das außerhalb einer Sandbox läuft.

So etwas werden Sie im App Store nicht finden.

Fazit

Macs sind großartig. Das sollten wir nicht vergessen! Aber wir können unsere Macs als großartige Arbeitsmaschinen bewundern, ohne dem naiven Glauben zu verfallen, dass sie eine Art uneinnehmbare Festung sind, die keine Hilfe braucht, um sie vor einer wachsenden Zahl von Bedrohungsakteuren zu schützen.

Die Sicherheit von Computern ist ein bewegliches Ziel, und gerade in Unternehmen erfordert dies einen engagierten Anbieter von Sicherheitslösungen, der mit den neuesten Bedrohungen Schritt halten kann. Helfen Sie Ihren Macs — und ihren Benutzern — sich selbst zu helfen, indem Sie sich der Realität der macOS-Sicherheitsbedrohungen bewusst sind und proaktiv an Ihrer Sicherheitslage arbeiten.

Wenn Sie wissen möchten, wie SentinelOne Ihre macOS-Geräte schützen kann, kontaktieren Sie uns oder fordern Sie eine kostenlose Demo an.

***Anmerkung**:*

Dieser Artikel stammt aus dem Blog einer Cybersecurity-Firma, und sein Hauptzweck ist zweifellos die Werbung für das eigene Produkt.

Aber wenn ich bedenke, welche Thesen in Computer-Foren immer noch im Brustton der Überzeugung lautstark verbreitet werden — allen voran natürlich „Macs bekommen doch keine Viren!“ —, dann ist offensichtlich noch sehr viel Aufklärung notwendig, um derlei Unsinn aus den Köpfen zu bekommen. Dieser Artikel, denke ich, hat dafür eine Reihe guter Argumente geliefert.

Welche Maßnahmen sollte man nun tatsächlich ergreifen? Man muss nicht unbedingt zu dem beworbenen Produkt greifen, das sich eher an Firmen und Behörden richtet und das ich persönlich gar nicht kenne.

Aus meiner Sicht sind z.B. folgende Apps empfehlenswert, um den eigenen Mac so gut wie möglich abzusichern:

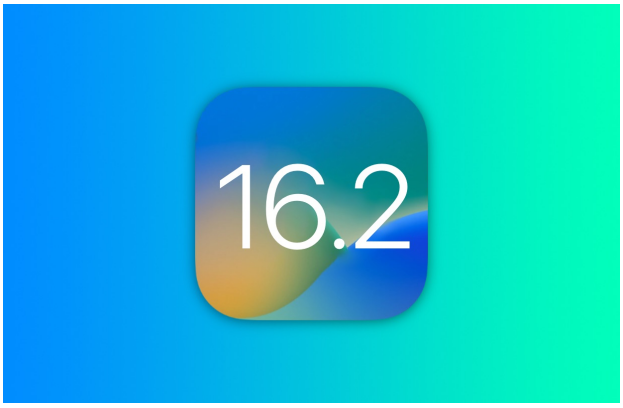
***Malwarebytes**: Kostenlose Demo funktioniert als Malware-Scanner; ein kostenpflichtiges Abo fügt Echtzeit-Hintergrundschutz hinzu.*

***ClamXAV**: Virenscanner mit Zusatz-Nutzen: Hintergrund-Komponente Sentry überwacht individuell wählbare Ordner wie z.B. Mail, Downloads, Desktop.*

***CleanMyMacX**: Von Apple empfohlenes Wartungsprogramm beinhaltet eine Echtzeit-Malware-Überwachung.*

*Apps des Mac-Sicherheitsgurus **Patrick Wardle**:*

BlockBlock**, **KnockKnock**, **LuLu**, **RansomWhere?**, **OverSight



10 neue iOS 16.2-Funktionen, die Sie sofort ausprobieren können

von Rajesh Pandey, cultofmac.com • Übersetzung: Kurt J. Meyer

Probieren Sie diese 10 neuen iOS 16.2-Funktionen so schnell wie möglich auf Ihrem iPhone aus.

iOS 16.2, das Apple am Dienstag veröffentlicht hat, bringt viele neue Funktionen, die es zu einem unverzichtbaren Update für alle iPhone-Besitzer machen. Von Sicherheitsverbesserungen und Produktivitätssteigerungen bis hin zu kosmetischen Optimierungen und anderen lustigen Dingen ist es positiv mit Upgrades beladen.

Hier sind die wichtigsten neuen iOS 16.2-Funktionen, die Sie jetzt ausprobieren sollten. (Hinweis: Viele dieser Funktionen erscheinen auch in iPadOS 16.2, das Apple heute ebenfalls veröffentlicht hat.)

Neue Funktionen in iOS 16.2

iOS 16.2 ist das zweite große Update seit dem 12. September, seit iOS 16 veröffentlicht wurde. Apple hat viele dieser neuen Funktionen auf dem iOS 16-Showcase in diesem Sommer während der Worldwide Developers Conference angepriesen, und sie sind gerade auf die iPhones gelangt. Andere hochkarätige Ergänzungen sprudelten in den letzten Monaten. iOS 16.2 bringt unter anderem diese wichtigsten neuen Funktionen:

- Erweiterter Datenschutz: Zusätzliche Sicherheit für iCloud-Daten.
- Apple Music Sing: Karaoke-Funktion, mit der Sie mit Ihren Lieblingstracks singen können.
- Freeform: Ein virtuelles Whiteboard für die plattformübergreifende Zusammenarbeit.
- Always-On-Display-Anpassung: Ermöglicht es iPhone 14 Pro/Max-Besitzern, ihre Bildschirme zu optimieren.
- AirDrop-Einschränkung: Beschränkt die AirDrop-Funktionalität auf maximal 10 Minuten zum Teilen mit Benutzern, die nicht in Ihrer Kontaktliste sind.
- Neue Lock Screen Widgets: Einfache Tools zur Verwaltung von Medikamenten und zur Überwachung des Schlafes.
- Sportergebnisse in Live-Aktivitäten: Schnelle Updates auf iPhone Lock Screen und Dynamic Island.
- SharePlay-Unterstützung im Game Center: Erweiterte Option für Gamer.
- Die Wetter-App fügt Nachrichten hinzu: Einige Städte erhalten regionale Updates von Apple News, wenn sie verfügbar sind.
- Aktualisierte Home-App-Architektur: Die Hausautomation erhält einen Schub.
- 5G-Unterstützung in Indien: Schnellere Mobilfunkvernetzung für einige Benutzer.

1. Erweiterter Datenschutz

Apple kommt endlich dazu, Ende-zu-Ende-Verschlüsselung für iCloud-Daten hinzuzufügen. Dieses Sicherheits-Upgrade, das als Advanced Data Protection für iCloud bezeichnet wird, verschlüsselt die folgenden iCloud-Daten:

- Geräte- und Nachrichtensicherungen
- iCloud-Laufwerk
- Anmerkungen
- Erinnerungen
- Sprachmemos
- Fotos
- Siri-Kurzbefehle
- Safari Lesezeichen
- Wallet-Pässe

Mit der neuesten Ergänzung verschlüsselt iCloud jetzt Daten in 23 verschiedenen Kategorien. Nur Daten aus Mail, Kontakten und Kalender, die in iCloud gespeichert sind, bleiben vorerst unverschlüsselt.

Apple aktiviert diese Funktion standardmäßig nicht - Sie müssen sie manuell einschalten. Hinweis: Wenn Sie es aktivieren, hat Apple keinen Zugriff auf die Verschlüsselungsschlüssel. Wenn Sie also nicht auf Ihr Konto zugreifen können, kann das Unternehmen nicht viel tun, um Ihnen zu helfen.

2. Apple Music Singen

Apple Music Sing verwandelt die Musik-Streaming-Plattform des Unternehmens in einen Karaoke-Dienst. Es zeigt die Texte des jetzt spielenden Songs in Echtzeit an und passt automatisch die Lautstärke des Originalsängers an, damit Sie die Führung übernehmen können. Eine Duett-Ansicht zeigt mehrere Sänger auf der gegenüberliegenden Seite des Bildschirms, um das Mitsingen von Multi-Sängern leicht zu machen. Apple Music Sing erfordert ein Apple Music-Abonnement und ist weltweit verfügbar.

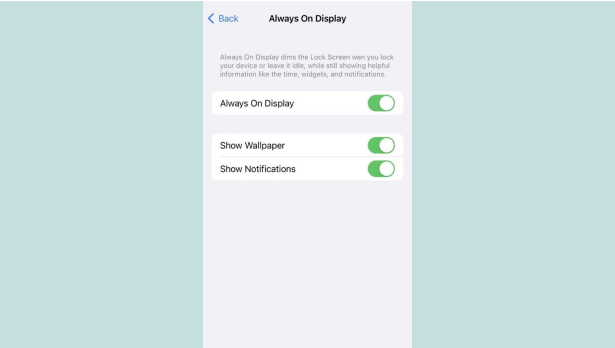
3. Freiform

Freeform ist wie ein virtuelles Whiteboard, das die Zusammenarbeit auf iPhone, iPad und Mac ermöglicht. (Foto: Apple)

Freeform wurde erstmals auf der WWDC22 vorgestellt und ist eine Collaboration-App für iPhone, iPad und Mac. Es bietet einen gemeinsamen digitalen Raum, in dem Sie mit anderen zusammenarbeiten können, ohne sich um Layouts und Seitengrößen kümmern zu müssen.

Sie können Freeform verwenden, um Notizen zu notieren, Dateien zu teilen und Fotos oder Videos einzufügen. Es gibt auch Apple Pencil-Unterstützung, so dass Sie Ihrer Kreativität wirklich freien Lauf lassen können. Apple ermöglicht das Starten einer Freeform-Sitzung über einen FaceTime-Anruf, und Sie können Live-Updates von anderen Benutzern in einem Nachrichten-Thread sehen.

4. Immer auf dem Display Anpassung



iOS 16.2 fügt neue Always On Display-Anpassungsoptionen für die iPhone 14 Pro-Serie hinzu. (Foto: Rajesh)

Apples Always On Display-Implementierung in iOS 16 für die iPhone 14 Pro-Serie ist barebones, ohne dass es keine Anpassungsoptionen gibt. iOS 16.2 ändert dies, indem es Schalter bereitstellt, um das Hintergrundbild und Benachrichtigungen zu deaktivieren, wenn der Low-Power-Anzeigemodus aktiv ist.

Die Möglichkeit, das Hintergrundbild zu deaktivieren, ist eine willkommene Ergänzung, da das Always On Display dann einen schwarzen Hintergrund zeigt, was die Funktion viel subtiler macht.

5. AirDrop-Einschränkung

Apple beschränkte die Sichtbarkeit von AirDrop für die Einstellung „Jeder“ in China mit der Veröffentlichung von iOS 16.1.1 auf 10 Minuten. Diese Änderung schafft zusätzliche Reibung, wenn Dateien mit Personen geteilt werden, die sich nicht in Ihrem Telefonbuch befinden.

iOS 16.2 macht diese Optimierung global. Um AirDrop zu empfangen oder Dateien von Nicht-Kontakten zu empfangen, müssen Sie zuerst die Sichtbarkeit von AirDrop schnell über das Kontrollzentrum Ihres iPhones für alle ändern.

6. Neue Sperrbildschirm-Widgets

Neues Widget für den Sperrbildschirm für Medikamente in iOS 16.2. (Foto: Reddit)

iOS 16.2 führt neue Lock Screen Widgets für Medikamente und Schlaf ein. Die erste wird als Erinnerung dienen, um sicherzustellen, dass Sie nicht vergessen, Ihre Medikamente rechtzeitig zu haben. Was das Schlaf-Widget betrifft, so werden Ihre letzten Schlafsitzungen und Schlafphasen angezeigt.

7. Sportergebnisse in Live-Aktivitäten

Erweiterte Unterstützung für Live-Aktivitäten fügt Sportergebnisse zu iPhone-Sperrbildschirmen (und der Dynamic Island auf iPhone 14 Pro/Max-Modellen) hinzu. Die Daten, die aus der integrierten Apple TV-App abgerufen werden, ermöglichen es Sportfans, über Profi-Basketball-, Baseball- und Fußballspiele in bestimmten Regionen auf dem Laufenden zu bleiben.

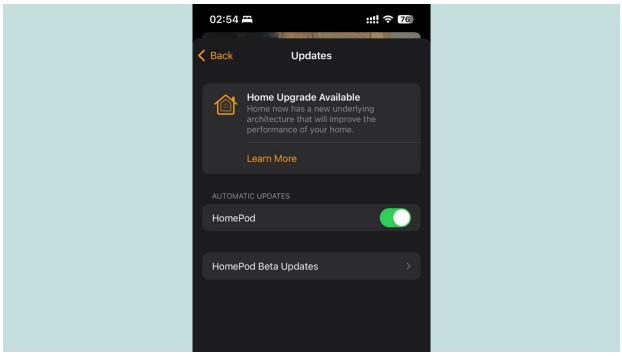
8. SharePlay-Unterstützung im Game Center

Game Center erhält SharePlay-Integration in iOS 16.2. Auf diese Weise können Sie Multiplayer-Spiele mit Ihren Freunden und Ihrer Familie während eines FaceTime-Anrufs spielen.

9. Wetter-App fügt Nachrichten hinzu

Apples Aktien-Wetter-App wird lokale und regionale Nachrichten von Apple News erhalten - zumindest in einigen Städten. (Hinweis: Die Geschichten erscheinen nur, wenn relevante Inhalte für eine bestimmte Region verfügbar sind.)

10. Aktualisierte Home-App-Architektur



iOS 16.2 aktualisiert die Architektur der Home-App. (Foto: Rajesh)

Apple verbessert weiterhin die Smart-Home-Unterstützung in iOS 16. Mit iOS 16.1 erhielt die Home-App Unterstützung für Matter, den neuen Smart-Home-Standard, der von Apple, Google und anderen Technologiegiganten unterstützt wird.

In iOS 16.2 hat das Unternehmen die zugrunde liegende Architektur der Home-App überarbeitet, um eine bessere Leistung, Effizienz und Zuverlässigkeit zu bieten. Dies sollte dazu beitragen, dass die Home-App eine bessere Erfahrung bei der Steuerung Ihrer Smart-Home-Geräte bietet.

Bonus: 5G-Unterstützung in Indien

iOS 16.2 ermöglicht 5G-Unterstützung im Airtel- und Jio-Netzwerk in Indien auf dem iPhone 12 und neueren Modellen. 5G-Netze sind gerade in Indien live gegangen. Dies ist eine willkommene Ergänzung, zumal die iPhone-Verkäufe im Land starten.

iOS 16.3 kommt 2023

Viele andere kleinere neue Funktionen und Änderungen in iOS 16.2 werden die Erfahrung bei der Verwendung Ihres iPhone weiter verbessern. Es ist auch das letzte große iOS-Update von Apple für dieses Jahr. Erwarten Sie, dass iOS 16.3 mit zusätzlichen neuen Funktionen Anfang 2023 veröffentlicht wird.

Apple veröffentlicht iOS 16.2, iPadOS 16.2, macOS 13.1 Ventura, watchOS 9.2 und tvOS 16.2

von Adam Engst, tidbits.com • Übersetzung: KJM

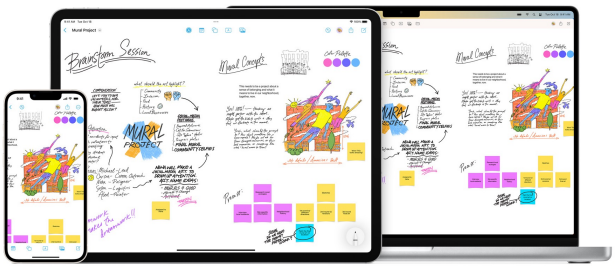
Apple hat in letzter Zeit Versprechen erfüllt und **Advanced Data Protection** für iCloud und Apple Music Sing in die Liste der Funktionen aufgenommen, die bis Ende dieses Monats ausgeliefert werden. Zu den früheren Versprechungen gehören das kollaborative digitale Whiteboard **Freeform**, externe Displayunterstützung für Stage Manager auf M1-iPads und eine längere Akkulaufzeit für die diesjährigen Apple Watch-Modelle während des Trainings. Alle diese Funktionen sind jetzt in iOS 16.2, iPadOS 16.2, macOS 13.1 Ventura, watchOS 9.2, tvOS 16.2 und HomePod Software 16.2 verfügbar.

Dies sind wichtige Feature-Releases, und mein Rat für solche Hauptversionen ist üblicherweise, mindestens eine Woche zu warten, bevor Sie aktualisieren. Dieses Mal schlage ich jedoch ein schnelles Update vor, da die neuen Versionen eine WebKit-bezogene Schwachstelle blockieren, von der Apple sagt, dass sie möglicherweise aktiv in freier Wildbahn „gegen iOS-Versionen, die vor iOS 15.1 veröffentlicht wurden“, ausgenutzt wurde. (Tatsächlich hat Apple auch iOS 15.7.2 und iPadOS 15.7.2 veröffentlicht, um diese schwerwiegende Schwachstelle zu beheben, und 16 andere — aktualisieren Sie ältere Geräte bald!)

Die Hauptausnahme ist das iPhone — wenn Sie auf iOS 16.1.2 aktualisiert haben, sind Sie bereits vor dieser Sicherheitsanfälligkeit geschützt und können das iOS 16.2-Update um ein wenig verzögern (siehe „iOS 16.1.2 optimiert die Absturzerkennung, verbessert die Kompatibilität des Mobilfunkanbieters“). iOS 16.1.2, für das Apple die Veröffentlichung von Sicherheitshinweisen verzögert Apple hat diese Ankündigung bis jetzt verschoben.

Einführung von Freeform

Zu den Änderungen in iOS 16.2, iPadOS 16.2 und macOS 13.1 gehört die Hinzufügung einer neuen gebündelten App: Freeform. Es ist eine digitale Whiteboard-App, die für kollaboratives Brainstorming entwickelt wurde und „den Benutzern hilft, Inhalte auf einer flexiblen Leinwand zu organisieren und visuell anzuordnen, so dass sie die Möglichkeit haben, alles an einem Ort zu sehen, zu teilen und zusammenzuarbeiten, ohne sich um Layouts oder Seitengrößen kümmern zu müssen“. Daten werden optional über iCloud mit Ihren anderen Geräten synchronisiert.



Ich bin mir immer noch nicht sicher, was ich über **Freeform** denken soll, und ich hoffe, es in den kommenden Wochen ausprobieren zu können. Es ist nicht so, dass ich vermute, dass Apple schlechte Arbeit geleistet hat (obwohl Jason Snell einige Ecken und Kanten gefunden hat) oder dass es schwierig zu bedienen sein wird (aber hier ist das Freeform-Handbuch, nur für den Fall). Nein, es ist so, dass ein kollaboratives digitales Whiteboard eine seltsame Wahl zu sein scheint, um das gesamte Apple-Erlebnis zu verbessern. Obwohl Apple in letzter Zeit sein Spiel in dieser Hinsicht verbessert hat, war die Zusammenarbeit nie eine der Stärken des Unternehmens — Apple geht es in erster Linie darum, den Einzelnen zu stärken, nicht die Gruppe. Digitale Whiteboard-Tools sind in Zoom und viele andere Videokonferenzplattformen integriert, die für die geschäftliche und pädagogische Zusammenarbeit wahrscheinlich viel beliebter bleiben werden als FaceTime.

Schließlich kann ich nicht sagen, dass ich jemals jemanden gehört habe, der nach einem digitalen Whiteboard von Apple gefragt hat, während es üblich ist, dass Benutzer nach einer Datenbank auf Verbraucherebene Wert legen, ähnlich dem, was die Leute in AppleWorks/ClarisWorks, frühen Versionen von FileMaker und sogar HyperCard verwendet haben.

Vielleicht bin ich nur griesgrämig, weil es für mich bei der Zusammenarbeit in erster Linie um schriftliche Dokumente geht, mit einer Reihe von Tabellenkalkulationen (ich habe es im vergangenen Jahr sehr geliebt, gruppenorientierte Tabellenkalkulationen in Google Sheets zu erstellen). Es ist auch möglich, dass sich Freeform bei einem Publikum von Teenagern und jungen Erwachsenen als sehr beliebt erweisen wird, die keine ernsthaften Tools für die Zusammenarbeit benötigen, aber gerne zusammen auf einer unendlichen Leinwand herumalbern. Probieren Sie es aus und sehen Sie, was Sie denken.

iOS 16.2 und iPadOS 16.2

Mit dem neuen iOS 16.2 und iPadOS 16.2 erhalten iPhones und iPads neue und verbesserte Funktionen, einige signifikante, andere weniger:

Erweiterter Datenschutz: Ich werde nicht sagen, dass es für die meisten Menschen ein Wendepunkt ist, aber **Advanced Data Protection für iCloud** trägt wesentlich dazu bei, Kritik an der Datenschutzposition von Apple mit iCloud zu berücksichtigen. Wie ich in „Apple's Advanced Data Protection Gives You More Keys to iCloud Data“ schrieb, bietet die Funktion **Ende-zu-Ende-Verschlüsselung** für viele weitere iCloud-Datentypen, und wenn Sie sich Sorgen über Verletzungen der Sicherheit von Apple oder Überschreitungen durch Strafverfolgungsbehörden machen, sollten Sie sie aktivieren. Umgekehrt halten Sie sich an Apples standardmäßigen iCloud-Datenschutz (der alle Daten bei der Übertragung und auf Apple-Servern verschlüsselt, aber mit Schlüsseln, die Apple kontrolliert), wenn Sie ältere Geräte haben, die eine Verbindung zu Ihrem iCloud-Konto herstellen müssen, aber nicht mit diesem Satz von OS-Updates kompatibel sind. Denken Sie daran, dass die Aktivierung des erweiterten Datenschutzes den Apple-Support daran hindert, Ihnen bei der Wiederherstellung Ihres iCloud-Kontos zu helfen, wenn Sie Ihr Passwort vergessen. Stellen Sie also sicher, dass Sie die Kontowiederherstellungsoptionen wie das Hinzufügen eines Wiederherstellungskontakts, das Erstellen eines Wiederherstellungsschlüssels oder beides einrichten - mindestens einer muss aktiviert sein, um ADP einzuschalten.

Apple Music Sing: Karaoke für Apple Music-Abonnenten auf Ihrem iPhone, iPad und Apple TV. Alkohol nicht inbegriffen.

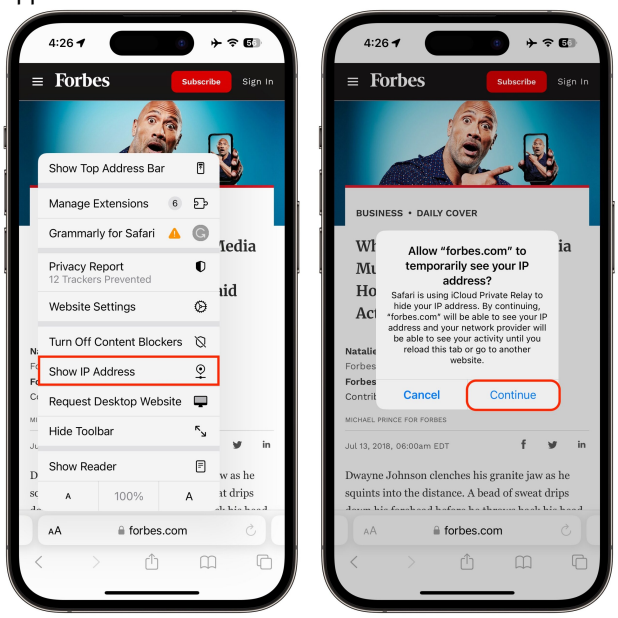
Game Center: Die Updates fügen GameCenter SharePlay-Unterstützung für Multiplayer-Spiele hinzu, damit Sie mit Personen in einem FaceTime-Anruf spielen können. Außerdem können Sie mit einem neuen Aktivitäts-Widget sehen, was Ihre Freunde auf Ihrem Startbildschirm spielen.

Home: Ich kann nicht ganz verstehen, warum Apple die Änderungen an der Home-App auflistet, die lediglich „verbesserte Zuverlässigkeit und Effizienz der Kommunikation zwischen Ihrem Smart-Home-Zubehör und Apple-Geräten“ bietet. Home war zu Beginn der iOS 16.0 Tage besonders fehleranfällig, so dass Apple vielleicht das Bedürfnis verspürt hat, den Benutzern zu versichern, es habe sich verbessert.

Nachrichten: Eine Suche in Nachrichten kann jetzt Fotos basierend auf ihrem Inhalt finden. Maschinelles Lernen ist dein Freund.

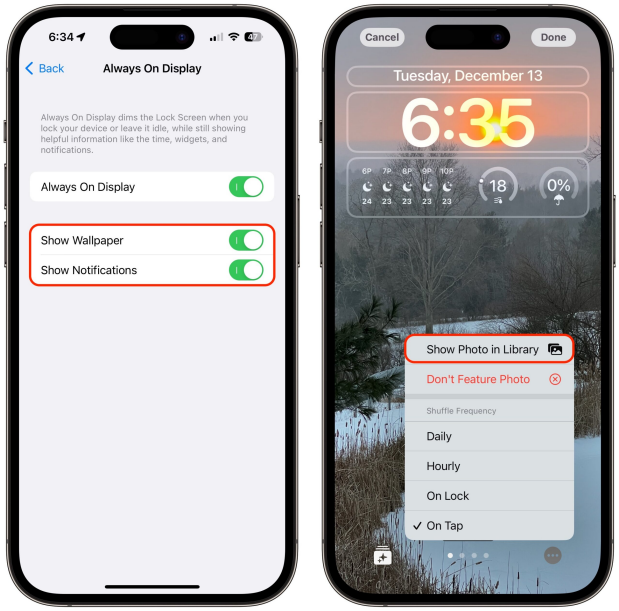
Wetter: Apple sagt, dass die Wetter-App jetzt wetterbezogene Nachrichtenartikel anzeigt, die mit dem aktuellen Standort verknüpft sind. Ich kann noch keinen Fall sehen, in dem dies funktioniert, auch nicht in den Teilen der USA, in denen derzeit auffälliges Wetter herrscht.

Privates iCloud-Relay: Wenn Sie Probleme mit iCloud Private Relay haben, die das ordnungsgemäße Laden einer Website in Safari verhindert, können Sie mit einer neuen Option den Dienst für eine bestimmte Website vorübergehend deaktivieren. Tippen Sie auf die AA-Schaltfläche in der Symbolleiste, tippen Sie auf IP-Adresse anzeigen und tippen Sie auf Weiter.



Notizen: Wenn Sie mit anderen in Notizen zusammenarbeiten, sehen Sie jetzt Live-Indikatoren, wenn Andere Aktualisierungen in einer freigegebenen Notiz vornehmen.

AirDrop: Wie gemunkelt, hat Apple AirDrop so optimiert, dass es erst nach 10 Minuten von allen zu Kontakten zurückkehrt (das neue Label lautet „Jeder für 10 Minuten"), um unerwünschte Anfragen zum Empfang von Inhalten zu verhindern. Das ist nicht unvernünftig, aber die Absicht wird durch die Tatsache in Frage gestellt, dass Apple es zum ersten Mal für iPhones in China implementiert hat, wo Demonstranten AirDrop zur Organisation verwendeten.



Weitere Sperrbildschirm-Widgets: Mit den neuen Schlaf- und Medikamenten-Widgets für den Sperrbildschirm können Sie Ihre neuesten Schlafdaten anzeigen und schnell auf Ihren Medikamentenplan zugreifen. Letzteres erscheint mir wichtig, da Medikamentenbenachrichtigungen etwas zu leicht zu ignorieren sind (siehe „Ein Apple pro Tag: iOS 16-Medikamentenfunktion bietet Warnungen, Protokollierung und Seelenfrieden").

Live-Aktivitäten für Apple TV: Sportfans werden die neuen Live-Aktivitäten für die Apple TV App zu schätzen wissen, mit der Sie Ihren Lieblingsteams mit Live-Ergebnissen auf dem Sperrbildschirm oder Dynamic Island auf dem iPhone 14 Pro und iPhone 14 Pro Max folgen können. Ich hoffe immer noch, dass Apple Leichtathletik und andere große Laufrennen zu seinem Sport-Tracking hinzufügen wird.

Mehrere zusätzliche Funktionen sind spezifisch für einzelne iPhone-Modelle:

Einstellungen für den Sperrbildschirm: Apple hat Einstellungen hinzugefügt, mit denen Sie das Hintergrundbild oder die Benachrichtigungen ausblenden können, wenn das Always-On-Display für ein iPhone 14 Pro oder iPhone 14 Pro Max aktiviert ist. Ich werde neugierig sein, sie auszuprobieren; ich habe festgestellt, dass ich das Always-On-Display nicht liebe, weil es das iPhone wahrscheinlicher macht, mir ins Auge zu fallen und mich von dem abzulenken, was ich tue. Es gibt auch eine neue Option Foto in Bibliothek anzeigen, wenn Sie das Foto-Shuffle-Hintergrundbild einrichten.

Die wichtigste versprochene iPad-Funktion in iPadOS 16.2 ist die Unterstützung von **Stage Manager auf externen Displays mit M1-iPad-Modellen**, einschließlich des iPad Air der fünften Generation, des 11-Zoll-iPad Pro und höher der dritten Generation und des iPad 12,9-Zoll-iPad Pro und höher der fünften Generation. Stage Manager unterstützt Displays mit Auflösungen von bis zu 6K (wenn Sie Ihr Pro Display XDR anschließen möchten), ermöglicht das Ziehen und Ablegen von Dateien und Fenstern vom iPad auf das Display und ermöglicht es Ihnen, bis zu vier Apps auf dem iPad-Bildschirm und weitere vier auf dem externen Display zu verwenden (siehe "Erste Eindrücke: Stage Manager auf dem iPad und Mac"

Die einzige andere iPad-spezifische Änderung scheint das Hinzufügen von **Tracking-Benachrichtigungen** zu sein, die Sie warnen, wenn sich ein von seinem Besitzer getrenntes AirTag in der Nähe befindet und kürzlich einen Ton abgespielt hat, um anzuzeigen, dass er sich bewegt. Mit anderen Worten, wenn ich richtig verstanden habe, kann das iPad Sie jetzt auf AirTag-Stalking aufmerksam machen, genau wie das iPhone.

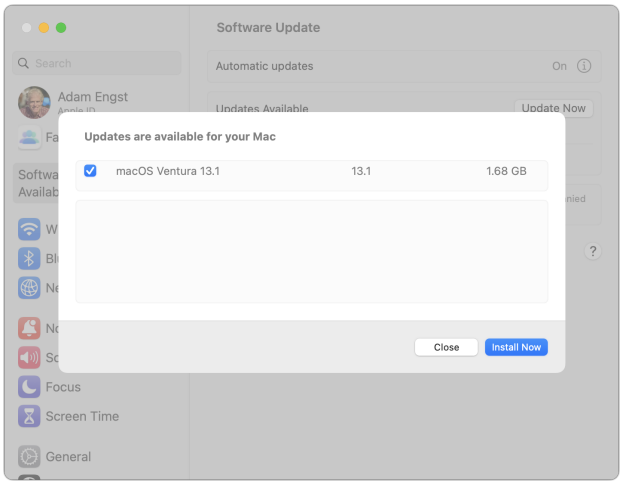
Die Updates beheben ein paar Fehler, einen für beide Plattformen, der dazu führte, dass einige Notizen nach der Aktualisierung nicht mit iCloud synchronisiert wurden, und einen iPad-spezifischen Fehler, der dazu führen konnte, dass Multi-Touch-Gesten bei der Verwendung der Zoom-Barrierefreiheitsfunktion nicht mehr reagierten.

iOS 16.2 und iPadOS 16.2 beheben auch 33 Sicherheitslücken, vermutlich einschließlich derjenigen, die in freier Wildbahn aktiv für diejenigen ausgenutzt wird, die noch nicht auf iOS 16.1.2 aktualisiert haben.

Update unter Einstellungen > Allgemein > Software-Update.

macOS 13.1 Ventura

Die Versionshinweise für macOS 13.1 Ventura sind deutlich kürzer als für iOS 16.2 und iPadOS 16.2, und sie sind noch kürzer, wenn Sie die Änderungen beseitigen, die allen dreien gemeinsam sind, einschließlich Freeform, Advanced Data Protection, verbesserter Suche in Nachrichten, Teilnehmercursors in Notizen und der Korrektur für Notizen, die nicht ordnungsgemäß synchronisiert werden.



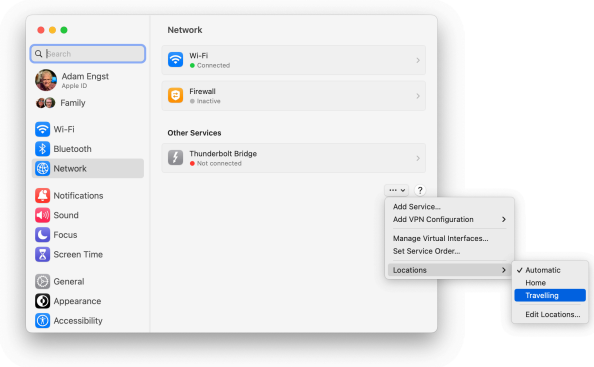
Als ich mein M1 MacBook Air aktualisiert habe, wurden in den Systemeinstellungen keine Freigabeinformationen angezeigt. Anscheinend müssen Sie das Update auswählen, auch wenn es nur eines gibt.

Das lässt nur eine Verbesserung und eine Fehlerbehebung, übrig, die einzigartig für Ventura ist:

Find My: Sie können jetzt AirTags, AirPods Pro-Hüllen der zweiten Generation und Find My Netzwerkzubehör in der Nähe finden, indem Sie einen Ton darauf abspielen. Ich wusste nicht, dass dies nicht bereits möglich ist, aber es ist sicherlich willkommen.

Keine Eingabe: macOS 13.1 behebt einen Fehler, der den Verlust der Tastatur- und Mauseingabe in einigen Apps und Spielen verursachte. Ich habe keine Ahnung, wie häufig dieser Fehler war, aber es wäre wahnsinnig ärgerlich, also wäre die Lösung Grund genug, auf macOS 13.1 zu aktualisieren.

Nicht von Apple erwähnt, aber von Howard Oakley bemerkt, ist die Tatsache, dass macOS 13.1 die Funktion „Netzwerkstandorte“ in den Systemeinstellungen wiederhergestellt hat.



Wirklich, ein hierarchisches ••• Pop-up-Menü?

macOS 13.1 behebt auch 33 Sicherheitslücken, einschließlich des WebKit-Bugs, der bereits aktiv ausgenutzt wurde.

Installieren Sie das Update unter Systemeinstellungen > Allgemein > Softwareupdate oder verwenden Sie die Benachrichtigung „Softwareupdate verfügbar“ in den Systemeinstellungen.

watchOS 9.2

Ganz andere Änderungen finden Sie unter watchOS 9.2. Vor allem hält es frühere Funktionsversprechen ein, indem es die **Race Route-Funktion** einführt, mit der Sie gegen sich selbst antreten können, indem Sie frühere Zeiten beim Outdoor Run-, Outdoor-Radfahren und Outdoor-Rollstuhl-Training vergleichen. Und wenn Sie auf Laufstrecken laufen, die die Uhr erkennt, erkennt das Outdoor Run-Training automatisch den Standort und bietet „streckenspezifische Metriken“.

Weitere Änderungen in watchOS 9.2 sind:

Neuer **benutzerdefinierter Kickboxing-Algorithmus** in der Workout-App für genauere Metriken

Geräusch-App, die anzeigt, wenn der Umgebungsgeräuschpegel reduziert wird, jetzt mit AirPods Pro und AirPods Max der ersten Generation verfügbar, wenn aktive Geräuschunterdrückung verwendet wird.

Benutzer des **Familien-Setup**s können zur Home-App eingeladen werden, um HomePod-Lautsprecher und Smart-Home-Zubehör zu steuern und Türen mit Home-Schlüsseln in Wallet zu entsperren.

Unterstützung der Barrierefreiheit zur Visualisierung, wenn Sirene auf einer Apple Watch Ultra verwendet wird.

Handgestensteuerung für AssistiveTouch und Quick Actions: Verbesserte Reaktionszeit und Genauigkeit

Optimierungen der Absturzerkennung auf der zweiten Generation der Apple Watch SE, der Apple Watch Series 8 und der Apple Watch Ultra (vermutlich um Fehlalarme zu vermeiden, die Menschen auf Achterbahnen und Skipisten erlebt haben)

Behebung eines Fehlers, der dazu führte, dass die Zeit unmittelbar nach dem Ausschalten eines Alarms in Sleep Focus falsch angezeigt wurde

Behebung eines Fehlers, der zu Unterbrechungen von Achtsamkeitssitzungen führte

Es gibt 23 Sicherheitslücken, die in watchOS 9.2 behoben wurden, aber es war nicht anfällig für den WebKit-Fehler, der die anderen Betriebssysteme plagte. Mit anderen Worten, beeilen Sie sich nicht aus Sicherheitsgründen, um zu aktualisieren. Die anderen Funktionen scheinen sich jedoch zu lohnen.

Sie können das watchOS 9.2-Update in der Watch-App auf Ihrem iPhone unter Meine Uhr > Allgemein > Software-Update installieren. Ihre Apple Watch muss an ein Ladegerät angeschlossen und auf mindestens 50% aufgeladen sein.

tvOS 16.2

Zum Schluss kommt tvOS 16.2, das mehr Änderungen erhält, als tvOS im Allgemeinen rechtfertigt. Vor allem sind Verbesserungen an Siri, die jetzt bis zu sechs verschiedene Familienmitglieder erkennen können, in einer anderen Sprache als der arbeiten, die Ihr Apple TV anzeigt (unser Sohn Tristan spricht gerne mit Siri auf seinem iPhone auf Französisch, während er den Rest der Benutzeroberfläche auf Englisch lässt) und mehr Sprachunterstützung hat (Dänisch in Dänemark, Französisch und Deutsch in Luxemburg und Englisch in Singapur), um

Apple hat auch die Unterstützung des Apple TV für Apple Music verbessert. Es bietet jetzt Echtzeit-Texte, die mit Musik synchronisiert sind (angeblich zum Mitsingen, aber auch nützlich, um herauszufinden, was sie sagen), und wenn Sie ein Apple TV 4K der dritten Generation haben, können Sie auch die Stimmlautstärke steuern, vermutlich für Karaoke-Enthusiasten.

tvOS 16.2 behebt 26 Sicherheitslücken, und obwohl es schwer zu betonen ist, dass ein Apple TV gehackt wird, kommen diese Korrekturen dank Apple-Betriebssystemen, die so viel von ihrem Code miteinander teilen.

Sie können tvOS 16.2 installieren, indem Sie zu Einstellungen > System > Software-Update gehen oder es einfach selbst installieren lassen.

HomePod-Software 16.2

Apple sagt nichts über dieses Update, außer dass es „allgemeine Leistungs- und Stabilitätsverbesserungen enthält“. Es sollte schon bald automatisch installiert werden, oder Sie können in iOS 16 die Zubehörkachel des HomePod berühren und halten und Zubehördetails auswählen. Scrollen Sie nach unten, tippen Sie auf das Zahnrad und tippen Sie dann auf Aktualisieren.