Welche App und welche Website darf den Aufenthaltsort sehen?

Quellen: mactechnews.de, Howard Oakley

Viele Programme benötigen Zugriff auf den aktuellen Standort des Geräts – oder hätten ihn zumindest gern. Manche Programme täuschen ein legitimes Interesse lediglich vor und nutzen Ortsinformationen für ein möglichst detailliertes Nutzerprofil. Um letzteres zu vermeiden oder wenigstens einzuschränken, können Mac-Nutzer genau einstellen, wie Ortungsinformationen erfasst werden. Die Anlaufpunkte in macOS, in denen man diese Einstellungen vornehmen kann, sind an unterschiedlichen Stellen zu finden.

Anders als iPhones und Apple Watches (sowie iPads mit Mobilfunkchips) haben Macs keine integrierte GPS-Ortung. Stattdessen leiten sie den Standort des Geräts indirekt aus anderen Informationen ab, etwa der IP-Adresse oder den in direkter Nähe befindlichen WLAN-Netzwerken. Was mit diesen Daten geschieht, entscheidet der Anwender.

1. Einstellungen/Datenschutz & Sicherheit

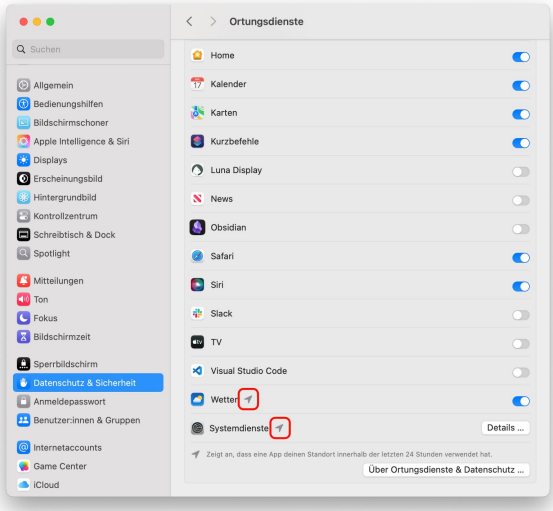
Die Ortungsdienste haben im Haupteintrag „Datenschutz & Sicherheit“ ein Untermenü namens „Ortungsdienste“. Ganz oben können Sie generell entscheiden, ob Sie Ortungsdienste nutzen oder generell unterbinden wollen. Darunter erscheinen die Detaileinstellungen. Jede App, welche Ortungsinformationen anfordert, listet dieses Menü auf. Nutzer können von hier aus einem Programm den Zugriff auf Ortsinformationen gewähren – und diese Genehmigung wieder entziehen. Hilfreich bei dieser Entscheidung: Das kleine Pfeilspitzensymbol kennzeichnet Programme, welche in den vergangenen 24 Stunden auf diesem Gerät eine Ortung angefordert haben. Fragt die App aktuell den Ort ab, erscheint die Pfeilspitze farbig. Wenn Ihnen nicht einleuchtet, wofür eine App Ihren Aufenthaltsort benötigen könnte, schalten Sie dies ab. Beispiele sind Chat-Programme (Slack, Discord) ebenso wie Programmierumgebungen.

Bitte um Unterstützung

Mein Dank gilt allen Lesern, die mir bereits geholfen haben, die MACtreff-Köln-Homepage und den Newsletter weiterhin zu finanzieren.

Unterstützt meine Arbeit bitte auch dieses Jahr durch eine Spende auf mein Paypal-Konto, indem Ihr auf den folgenden Link klickt paypal.me/KJM54 und dort Euren gewünschten Betrag eingebt.

Kurt J. Meyer



Die Pfeilspitze signalisiert, dass ein Programm kürzlich auf Ortsinformationen zugegriffen hat.

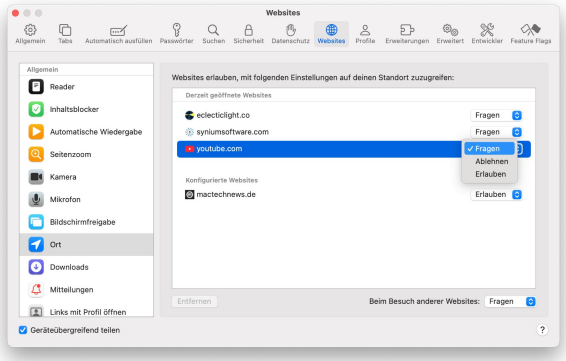
2. Untermenü „Systemdienste“

Innerhalb dieses Dialogs gibt es zusätzliche Unterpunkte, welche über den Button „Detail ...“ erreicht werden. Ganz unten in der Liste erscheinen die Systemdienste, die Sie ebenfalls überprüfen sollten. Hier können Sie entscheiden, ob etwa Kurzbefehle auf Ortsinformationen zugreifen dürfen oder ob die Suchfunktion Ihren Aufenthaltsort einbeziehen darf. Der Eintrag „Wichtige Orte“ bietet einen weiteren Unterdialog; hier finden Sie heraus, welche Aufenthaltsorte macOS für Sie als relevant gekennzeichnet hat. Wollen Sie genau beobachten, wann welche Programme auf Ortsinformationen zugreifen, aktivieren Sie „Standortsymbol im Kontrollzentrum anzeigen“.

Wer wissen will, wann welche App auf Ortsinformationen zugreift, bekommt dies über das Kontrollzentrum angezeigt.

3. Safari/Einstellungen/Websites

Der vorinstallierte Browser ist standardmäßig so eingestellt, dass er nachfragt, bevor eine Website Ortsinformationen abruft. Möchten Sie einer Webseite generellen Zugriff auf Ihren Standort einräumen (oder diesen wieder entfernen), wird ein Ausflug in die Einstellungen von Safari notwendig (Tastenkürzel: cmd-Komma). Im Reiter „Websites“ wählen Sie in der linken Spalte „Ort“ aus. Die Websites, die hier erscheinen, haben entweder eine vorab festgelegte Einstellung zu Ortsinformationen oder sind gerade in einem Browserfenster geöffnet. Über ein Aufklappmenü können Sie für jede Seite zwischen Fragen, Ablehnen und Erlauben wählen.



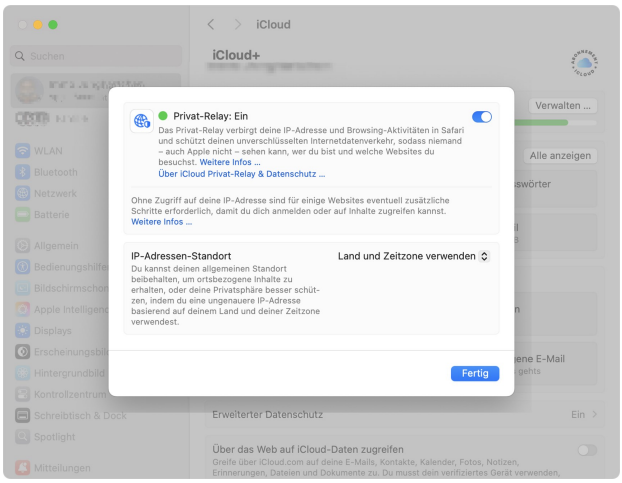
In Safari legen Sie unter Websites/Ort seitenspezifische Einstellungen fest.

4. Alternative Browser

Verwenden Sie weitere Browser, sollten Sie deren Einstellungen aufsuchen, um dort ebenso festzulegen, welche Websites Ortsinformationen abrufen. Bei Firefox beispielsweise finden Sie diese im Bereich „Einstellungen & Sicherheit“: Unter „Berechtigungen“ klicken Sie rechts neben „Standort“ auf „Einstellungen…“, um seitenspezifische Konfigurationen hinzuzufügen oder zu entfernen. Im Brave Browser gehen Sie auf Einstellungen/Datenschutz & Sicherheit/Standort — bei diesem Programm können Sie Websites generell den Zugriff auf Ortsinformationen verwehren.

5. Einstellungen/iCloud

Wenn Sie ein Bezahlabo bei iCloud verwenden, haben Sie Zugriff auf zusätzliche Privatsphäre-Funktionen, welche Apple als iCloud+ subsumiert. Ein Teil davon ist „Private Relay“ — hier können Sie Ihren Aufenthaltsort zusätzlich verschleiern, indem Sie auf „Land & Zeitzone verwenden“ umschalten. Dies müssen Sie allerdings auf jedem Mac separat einmalig aktivieren.



Wer bei iCloud für zusätzlichen Speicherplatz bezahlt, erhält obendrein erweiterte Privatsphäre-Funktionen.

Einige Ortungsdienste sind notwendig, andere nicht abschaltbar

In seinem Blog-Beitrag zu Ortungsdiensten in macOS rät Howard Oakley davon ab, diese systemweit auszuschalten — essenzielle Funktionen wie „Wo ist?“ sind auf sie angewiesen. Einen Kritikpunkt bringt er ebenfalls an: Der Zugriff von Systemdiensten wie z.B. die Teilen-Funktion von macOS lässt sich nicht separat deaktivieren. Zudem gibt Oakley noch Einblicke in Systeminterna und erklärt, welche Dienste für Ortsinformationen verantwortlich zeichnen.

Es folgt der oben zitierte Originalartikel:

Verwaltung des Zugriffs auf Standortinformationen

Howard Oakley (eclecticlight.co) • Übersetzung KJM

Macs und fast alle Geräte sammeln Informationen über ihren Standort aus lokalen Wi-Fi-Netzwerken, GPS-Systemen (nicht Macs) und anderen Quellen. Der Zugriff auf Standortinformationen wird in macOS in den Einstellungen für Datenschutz und Sicherheit gesteuert, aber im Gegensatz zu den meisten dort aufgeführten Punkten wird er nicht über TCC verwaltet, sondern über einen eigenen Dienst in den Standortdiensten.

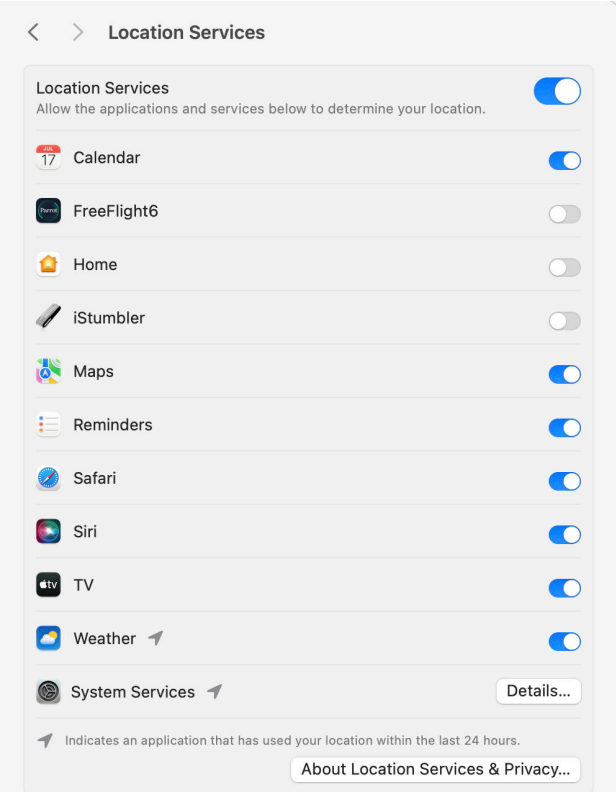
Tracking

Zusätzlich zu diesen Einstellungen verfügen Safari und andere Browser über eigene Kontrollmöglichkeiten für Tracking und Standortbestimmung. In Safari sind diese im Abschnitt „Datenschutz“ der Einstellungen und im Punkt „Standort“ unter „Websites“ zu finden. Wenn Sie iCloud+ abonniert haben, können Sie in Ihrem Apple-Konto im Abschnitt „iCloud+“ auf „Private Relay“ zugreifen.

Freigabe und Find My…

Standortdienste sind insofern einzigartig, als dass Standortdaten, wenn sie aktiviert sind, unweigerlich in iCloud freigegeben werden. Die einzige Möglichkeit, die Freigabe von Standortdaten auf Ihren mit iCloud verbundenen Geräten zu unterbinden, besteht darin, den gesamten Dienst zu deaktivieren, was auch für iOS- und iPadOS-Geräte gilt. Auch wenn es verlockend erscheint, die Ortungsdienste ganz zu deaktivieren, geht diese Verbesserung der Privatsphäre auf Kosten einiger wertvoller Dienste: insbesondere Find My… und Aktivierungssperre, und viele Systemdienste und Apps benötigen ebenfalls aktivierte Ortungsdienste.

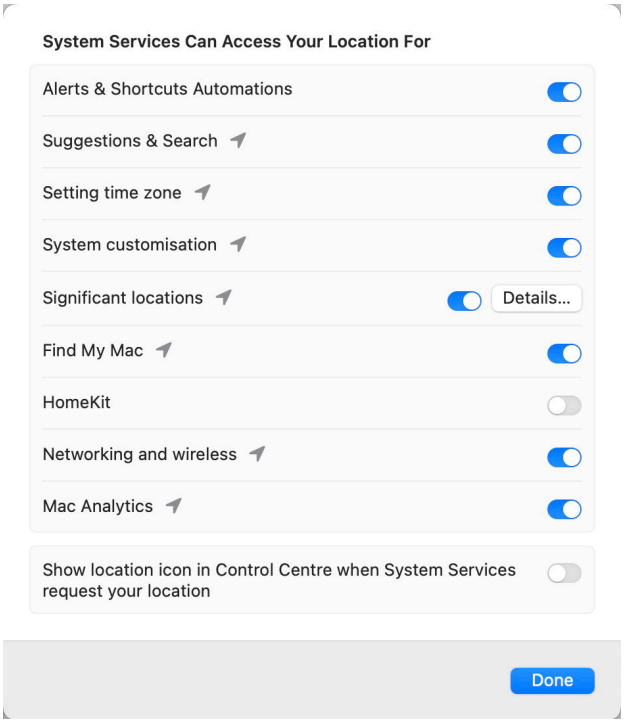
Einstellungen



Die Ortungsdienste sind der komplexeste Abschnitt in den Datenschutz- und Sicherheitseinstellungen und viele ihrer Steuerelemente sind tief verschachtelt. Dieser Bereich stammt noch aus den Tagen der Systemeinstellungen und wurde noch nicht umgestaltet, um die Vorteile der Systemeinstellungen zu nutzen. Über dem letzten Punkt, Systemdienste, befindet sich eine Liste der Anwendungen, deren Zugriff auf Standortdaten Sie direkt steuern können, obwohl diese nur aktiviert oder deaktiviert und nicht aus der Liste entfernt werden können.

Ungewöhnlicherweise öffnet die Schaltfläche **Über Ortungsdienste und Datenschutz** ein Fenster mit einer Mischung aus Hilfe- und Datenschutzinformationen, die es wert sind, gelesen zu werden, um einen besseren Einblick in die Verwaltung und Weitergabe von Daten zu erhalten. Darin wird auf einen wichtigen Punkt hingewiesen: Wenn Sie einer Drittanbieter-App Zugriff auf Ihren Standort gewähren, hat der Anbieter dieser App die Kontrolle über Ihre Standortdaten gemäß seinen Bestimmungen und Datenschutzrichtlinien, nicht denen von Apple. Wenn Ihre Standortdaten sensibel sind, sollten Sie Drittanbieter-Apps nur dann Zugriff darauf gewähren, wenn Sie sicher sind, dass sie diese Daten angemessen schützen.

Weitere wichtige Steuerungen werden in einem anderen Fenster angezeigt, wenn Sie auf die Schaltfläche **Details… für Systemdienste** klicken. Hier werden einige der Zwecke aufgelistet, für die macOS Standortdaten verwendet, und Sie haben eine genaue Kontrolle darüber.



Die letzte Schicht dieser Zwiebel kommt zum Vorschein, wenn Sie auf die Schaltfläche „Details…“ neben „**Wichtige Orte**“ klicken: eine Auflistung aller Orte, die macOS als „wichtig“ einstuft. Auf einem stationären Mac mit mobilen iOS-Geräten basieren diese größtenteils auf den Standortdaten, die von diesen Geräten gesammelt wurden, und werden in ähnlichen Listen auf jedem Gerät wiedergegeben.

Wenn Sie sich diese wichtigen Orte noch nie angesehen haben, werden Sie vielleicht überrascht sein, wie viele Details sie enthalten: die genaue Position, die auf einer lokalen Straßenkarte angezeigt wird, mit Zeiträumen, über die letzten Monate. Daraus lässt sich vielleicht ein Großteil Ihres Lebens und Ihrer Aktivitäten rekonstruieren. In diesem Fenster können Sie den Verlauf löschen, wenn Sie nicht wollen, dass jemand weiß, wo Sie waren.

Internes

Dahinter verbirgt sich der Systemdienst `locationd` und seine Datenbank, die in /var/db/locationd untergebracht ist. Die offizielle Beschreibung von locationd lautet, dass er geografische Standortdaten abruft und den Zugriff darauf verwaltet. Wenn Sie aufgefordert werden, Zugriff auf Standortdaten zu gewähren, ist das der CoreLocationAgent, der in seinem Namen handelt. Anwendungen, die Standortdaten von den Location Services anfordern können, sollten über die Berechtigung *com.apple.security.personal-information.location* verfügen und *NSLocationUsageDescription*-Informationen bereitstellen, was Sie mit Apparency *(siehe S. 8)* überprüfen können.

Das Verzeichnis /var/db/locationd enthält eine einfach zu lesende Datei mit wichtigen Informationen, die clients.plist, sowie verschiedene undurchsichtige Datendateien. Ein Unterverzeichnis /Library enthält eine überraschende Sammlung von Skripten und zwischengespeicherten Daten.

clients.plist ist eine Standardeigenschaftsliste, die ein Wörterbuch aller Anwendungen und anderer Software enthält, die auf Location Services-Daten zugreifen können. Bei denjenigen, die derzeit Zugriff haben, ist der Schlüssel Authorized auf <true> gesetzt. Im Allgemeinen sollten diese mit den Apps und anderen Elementen in der Location Services-Liste in den Datenschutz- und Sicherheitseinstellungen übereinstimmen, obwohl dies nicht für öffentliche oder private Frameworks gilt, die enthalten sind. Es gibt auch eine Markierung für den Schlüssel Ausblenden, die darauf hindeutet, dass einigen Apps oder Diensten Zugriff auf Standorte gewährt werden kann, diese aber nicht in den Einstellungen für die Standortdienste angezeigt werden.

Während andere Datenschutzmaßnahmen mit dem Befehlstool tccutil verwaltet werden können, gibt es für die Ortungsdienste keine Entsprechung. Außerdem würde sich das Löschen der Datenbank auf viele Systemdienste auswirken, darunter **Wo ist?** und **Aktivierungssperre**, was wiederum Auswirkungen auf die Sicherheit hat.

Da die Ortungsdienste auf Hardware- und Netzwerkfunktionen angewiesen sind, funktionieren sie nicht in virtuellen Maschinen, die auf Apple-Silizium-Macs ausgeführt werden, auch wenn Sie sie optional aktivieren können.

Zusammenfassung

- Geografische Standortdaten werden von Wi-Fi-Netzwerken und anderen Quellen abgeleitet und über die Standortdienste bereitgestellt.
- Obwohl die Steuerelemente in den Einstellungen für Datenschutz und Sicherheit enthalten sind, funktionieren sie anders als andere, da sie den Ortungsdienst und nicht TCC (*Transparency Consent and Control*) verwenden.
- Die Ortungsdienste sind für Find My..., Aktivierungssperre und andere macOS Apps und Dienste erforderlich.
- Wenn Sie einer App eines Drittanbieters Zugriff auf Ihren Standort geben, hat der Anbieter dieser App die Kontrolle über Ihre Standortdaten in Übereinstimmung mit seinen Bedingungen und Datenschutzrichtlinien, nicht mit denen von Apple.
- **Wichtige Orte** kann einen detaillierten Überblick über Ihre Bewegungen geben.
- Es gibt im Terminal kein Befehlswerkzeug zur Verwaltung der Ortungsdienste.

Was kann der Wiederherstellungsmodus auf Apple-Silicon-Macs?

Quellen: mactechnews.de, Howard Oakley

Ein Mac lässt sich selten aus der Fassung bringen. Passiert es aber doch, sieht macOS ein eigenständiges System vor, um Fehler zu beheben, Probleme auf den Grund zu gehen oder das Betriebssystem neu zu installieren: die Wiederherstellungspartition. Sie wird automatisch als verstecktes APFS-Volume installiert und beherbergt ein abgespecktes macOS inklusive Installationsassistent sowie der wichtigsten Dienstprogramme. Um einen Apple-Silicon-Mac von der Wiederherstellungspartition zu starten, fährt man ihn herunter und hält beim erneuten Hochfahren den Einschaltknopf dauerhaft gedrückt. Erscheint eine Übersicht mit Startsystem(en) und dem „Optionen“-Button, befindet sich der Mac im Wiederherstellungsmodus. Bereits in dieser Ansicht können Tastenkürzel etwas ausrichten.

Start im sicheren Modus

Links vom Optionen-Button erscheinen erkannte Startlaufwerke; in den meisten Fällen handelt es sich um einen einzigen Eintrag mit dem Titel „Macintosh HD“. Wird er angeklickt, erscheint darunter der Button „Fortfahren“. Halten Sie die Shift-Taste gedrückt, verändert er sich: Nun steht dort „Im sicheren Modus fortfahren“. Klicken Sie bei weiterhin gedrückter Shift-Taste darauf, führt macOS eine Überprüfung des Startvolumes durch, um das System anschließend ohne Erweiterungen, Startobjekte und zusätzliche Schriften hochzufahren. Verfügt der Mac über mehrere Start-Volumes, kann man zwischen diesen wählen — und sie durch Gedrückthalten der Option- oder Control-Taste zum Standard-Startsystem erklären.

Funktionstasten bei Auswahl des Startlaufwerks

Shift	im sicheren Modus fortfahren
Ctrl	immer verwenden
Option	immer verwenden

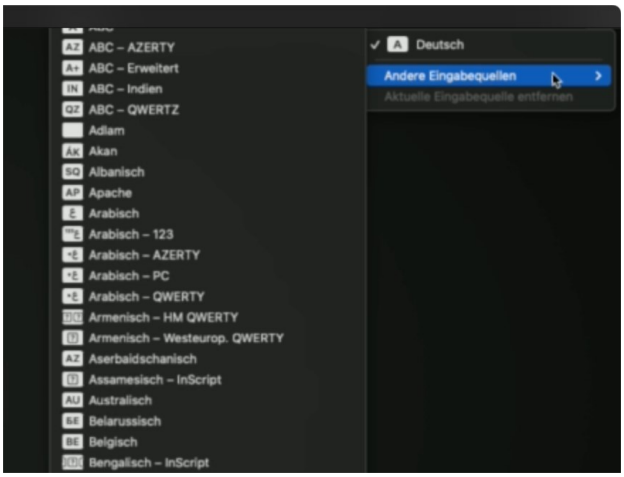
Systemdiagnose anfertigen

In manchen Situationen, etwa bei Fehlerberichten via Apple Feedback, erbittet Apple das Anfertigen einer Systemdiagnose. Dies gelingt aus dem Begrüßungsdialog heraus mit einem Tastenkürzel: Drücken Sie +. (Punkt) – der Bildschirm leuchtet einmal hell auf. Es dauert einige Zeit, bis die Diagnoseinformationen zusammengestellt sind. Zum Abschluss erscheint ein Speicherdialog. Schließen Sie ein externes Laufwerk an, etwa einen USB-Stick oder eine SSD im APFS-, HFS- oder FAT-Format, und legen die Datei darauf ab.

shift+ctrl+cmd+.	**Systemdiagnose erstellen**

Wiederherstellungsassistent

Sämtliche weiteren Optionen erfordern, dass Sie den „Optionen“ betitelten Zahnrad-Button auswählen und auf „Fortfahren“ klicken. Im nächsten Schritt müssen Sie sich als Administrator authentifizieren und Ihr Kennwort eingeben. Gelingt dies nicht, schauen Sie in der oberen rechten Ecke nach, ob die richtige Tastaturbelegung ausgewählt ist. Nach der geglückten Anmeldung erscheint die macOS-Wiederherstellung in der Mitte des Bildschirms. Deren zwei obere Optionen sind recht selbsterklärend: „Aus Time Machine wiederherstellen“ sowie „macOS [Version] erneut installieren“ machen genau dies. „Safari“ öffnet ein Browserfenster mit der lokalisierten Supportseite zur macOS-Wiederherstellung. Das „Festplattendienstprogramm“ hilft beim Aufspüren sowie Beheben von Problemen mit Festspeichern sowie Volume-Strukturen. Um aus Safari oder dem Festplattendienstprogramm wieder zum Hauptmenü zurückzukehren, beenden Sie das jeweilige Programm (+Q).



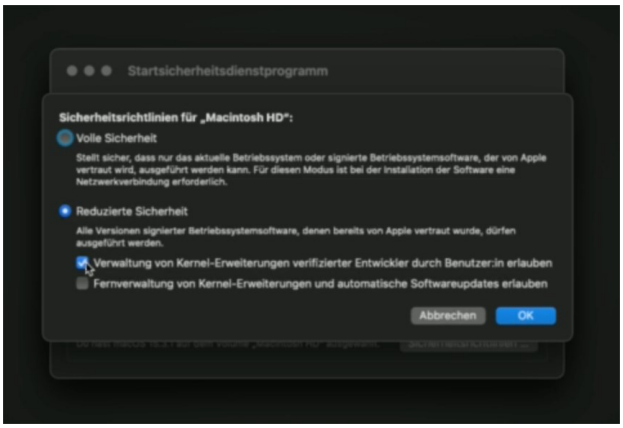
In der oberen rechten Ecke lässt sich die Tastaturbelegung umstellen.

Werkzeuge in der Menüleiste

Weitere Programme stehen in der Menüleiste am oberen Rand bereit: Im Menü „Fenster“ können Sie ein Wiederherstellungsprotokoll einblenden lassen, um detaillierte Informationen bei einer Systeminstallation oder der Wiederherstellung eines Backups angezeigt zu bekommen. Über das Menü „Dienstprogramme“ stehen drei weitere Tools zur Auswahl: Startsicherheitsdienstprogramm, Terminal sowie „Volume teilen“.

Startsicherheitsdienstprogramm

Seit macOS 14 (Sonoma) sind auf Macs standardmäßig keine Kernelerweiterungen von Drittanbietern erlaubt. Will man doch noch welche verwenden, muss die System Integrity Protection (SIP) deaktiviert werden. Dafür ist dieses Startsicherheitsdienstprogramm gedacht. Ein übersichtliches Menü erlaubt den Wechsel zwischen sicherem und unsicheren Modus; für letzteren stehen zwei weitere Optionen zur Auswahl. Wer einen Mac mit mehreren Startvolumes betreibt, sollte überprüfen, mit welchem System er gerade interagiert: Jede macOS-Installation bringt ihr eigenes Wiederherstellungssystem mit und kann nur für dieses die SIP-Einstellungen ändern, erklärt Howard Oakley in einem Blog-Beitrag. Um zwischen Systemen zu wechseln, müssen Sie zunächst in das andere macOS starten, dann den Mac ausschalten und erneut den Wiederherstellungsmodus aktivieren.



Im Startsicherheitsdienstprogramm kann man macOS dazu bringen, Kernelerweiterungen von Drittherstellern zuzulassen.

Volume teilen

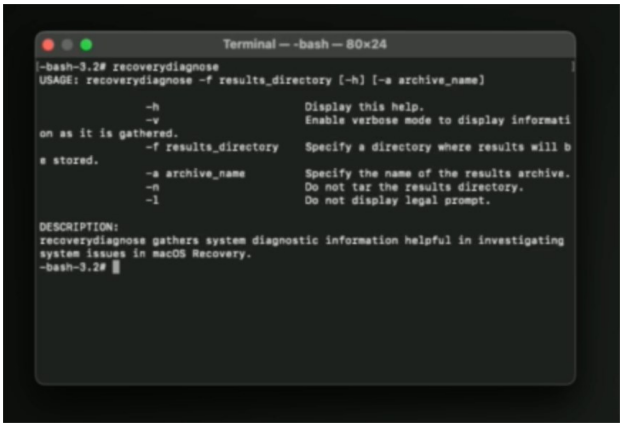
Wollen Sie auf die Schnelle einige Daten auf einen anderen Mac kopieren, wählen Sie das Dienstprogramm „Volume teilen“. In diesem Fall verbinden Sie beide Rechner über ein Thunderbolt- oder USB-C-Kabel. Darüber wird eine Netzwerkverbindung initiiert, und der Mac im Wiederherstellungsmodus erscheint als SMB-Freigabe am verbundenen Zweit-Mac.

Terminal

Die Kommandozeile ist ein mächtiges, wenn auch gewöhnungsbedürftiges Werkzeug. Die meisten Programme mit grafischer Bedienoberfläche im Wiederherstellungsmodus verfügen über ein zusätzliches Kommandozeilen-Pendant. Darin stehen mehr Optionen bereit – allerdings muss man sich vorher über diese informieren: Der „man“-Befehl, der ein Handbuch für so ziemlich jedes Terminal-Programm ausgibt, fehlt in der macOS-Wiederherstellung. Um sich über die Nomenklatur eines Programms zu informieren, empfiehlt sich eine vorherige Recherche im Normalbetrieb des Macs.

Terminal-Befehle im Wiederherstellungsmodus

fsck	Überprüfung des Dateisystems (HFS+)
fsck_apfs	Überprüfung des Dateisystems (APFS)
mount	Laufwerk aktivieren (HFS+)
mount_apfs	Laufwerk aktivieren (APFS)
csrutil	SIP selektiv (de-)aktivieren
asr	Apple Software Restore
nvram	Firmware-Einstellungen bearbeiten
spctl	Notarisierung (de-)aktivieren
sysctl	Kernel-Status ändern
recoverydiagnose	Diagnose für Wiederherstellungsmodus



Im Recovery-Modus verwendet das Terminal die bash-Shell.

Wenn der Wiederherstellungsmodus nicht startet

Manchmal versagt der Wiederherstellungsmodus selbst. In diesem Fall kann man in manchen Fällen das „**Fallback Restore**“ aufrufen. Dafür drücken Sie den macOS-Startknopf, lassen ihn kurz wieder los, um ihn dann wieder lang gedrückt zu halten. In diesem Fall startet das Restore-Image einer vorherigen macOS-Installation — sofern eine solche noch auf dem Mac residiert. Falls auch dies scheitert, bleibt noch der Umweg über einen zweiten Mac und den DFU-Modus.

Programme starten trotz fehlender aktueller Apple-Verifizierung

Quellen: mactechnews.de, Howard Oakley

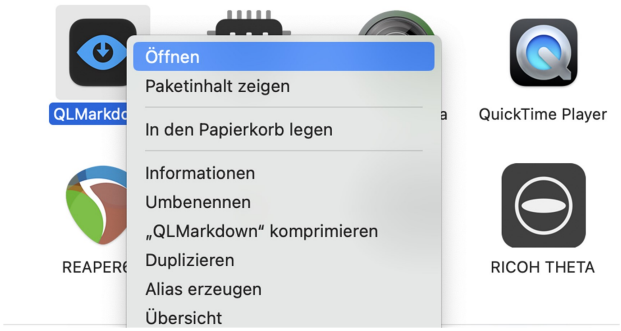
Apple entwickelt die Sicherheitsfunktionen von macOS kontinuierlich weiter. Ein Teil des Maßnahmenpakets stellt „Gatekeeper“, ein Notarisierungssystem für Software. Das zugrunde liegende Prinzip: Wer Software entwickelt, die anstandslos auf Macs starten soll, muss sich als verifizierter Entwickler registrieren und die eigene Software bei Apple zur Überprüfung auf Malware einreichen. Dies bedeutet neben zusätzlichem Aufwand auch Kosten: Apple verlangt eine Pauschale von jährlich 100 US-Dollar für diesen Dienst. Manche Open-Source-Projekte und Hobby-Entwickler scheuen diese Ausgabe. Manchmal hat der Anbieter sein Apple-Developer-Abonnement beendet, weil er sie nicht mehr weiterentwickelt. Um derlei Software-Titel zum Laufen zu bringen, muss man der App eine Ausnahme einräumen.

Dass eine App nicht notarisiert ist, erkennt man beim Versuch, sie aus dem Programme-Ordner heraus zu starten. In diesem Fall erscheint eine Fehlermeldung mit der Warnung, dass Apple die Applikation nicht auf Schadsoftware untersuchen konnte. Anwendern werden nur zwei Optionen geboten: Mit „Fertig“ den Dialog zu schließen oder das Programm direkt in den Papierkorb zu befördern.

Die Details der Fehlermeldung bei nicht verifizierten Software-Titeln beschränken sich aufs Wesentliche und geben keinen Hinweis auf Umgehung.

Umgehung per Sekundärklick

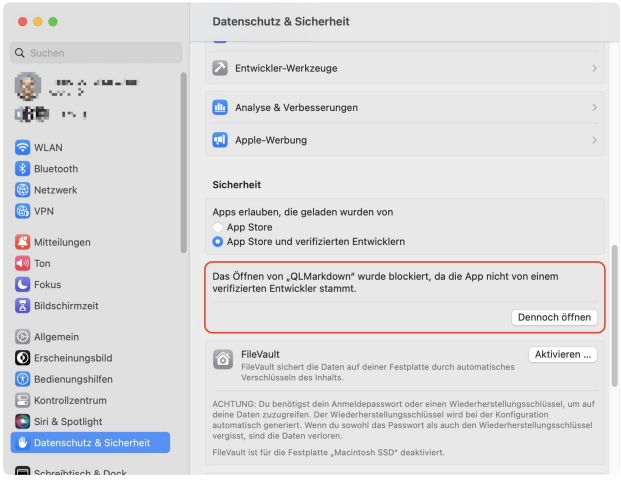
Um die betroffene App trotzdem zu öffnen, genügt oftmals der Start per Kontextmenü: Anstatt das Icon doppelzuklicken, klicken Sie es bei gedrückter ctrl-Taste an. Im Kontextmenü wählen Sie „Öffnen“. Bestätigen Sie Ihre Entscheidung im aufploppenden Dialog. Eventuell müssen Sie dafür ein Admin-Kennwort eingeben oder sich über Touch ID authentifizieren.



Über das Kontextmenü genehmigen Sie den Programmstart ohne aktuelle Notarisierung.

Freischalten in „Datenschutz & Sicherheit“

Eine weitere Methode, eine App trotz fehlender Apple-Verifizierung zu starten, führt über die Einstellungen-App, genauer: den Dialog „Datenschutz & Sicherheit“. Nach einem gescheiterten Startversuch einer nicht notarisierten App erscheint in diesem Dialog eine zusätzliche Option. Scrollen Sie im Dialog nach unten, bis zum Punkt „Sicherheit“. Zwischen „Apps erlauben von“ und „FileVault“ findet sich hier für kurze Zeit der Eintrag „Das Öffnen von ‚[Programm]‘ wurde blockiert, da die App nicht von einem verifizierten Entwickler stammt“. Klicken Sie auf „Dennoch öffnen“, um eine Ausnahme hinzuzufügen. Auch hier müssen Sie noch einen warnenden Dialog bestätigen und sich als Administrator authentifizieren.



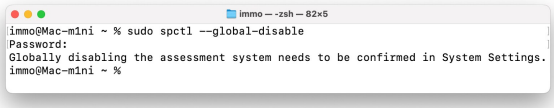
Ein temporärer Eintrag in den Einstellungen ermöglicht das Ausführen nicht genehmigter Programme.

Freibrief für nicht verifizierte Software

Die dritte Möglichkeit stellt den Zustand wieder her, wie er vor einigen Jahren für macOS galt: Anwender konnten wählen, ob sie Software nur aus dem Mac App Store, aus dem Mac App Store und verifizierten Entwicklern oder von überall zulassen wollen. Die dritte Option ist auf produktiv genutzten Macs keine empfehlenswerte Option. Doch auf Testsystemen ohne relevante Nutzerdaten oder in virtuellen Maschinen kann diese Einstellung durchaus einen Sinn erfüllen. Um sie zurückzuerhalten, ist ein Ausflug ins Dienstprogramm „Terminal“ notwendig. Hierin geben Sie den Befehl

```
sudo spctl --global-disable
```

ein und bestätigen mit der Enter-Taste. Dann müssen Sie Ihr Admin-Kennwort eingeben und wiederum mit Enter bestätigen. Daraufhin erscheint ein entscheidender Hinweis: Der Notarisierungs-Check ist damit nicht deaktiviert, sondern muss in den Einstellungen ausgewählt werden.



Über das Terminal reaktiviert man eine zusätzliche Option in den Systemeinstellungen.

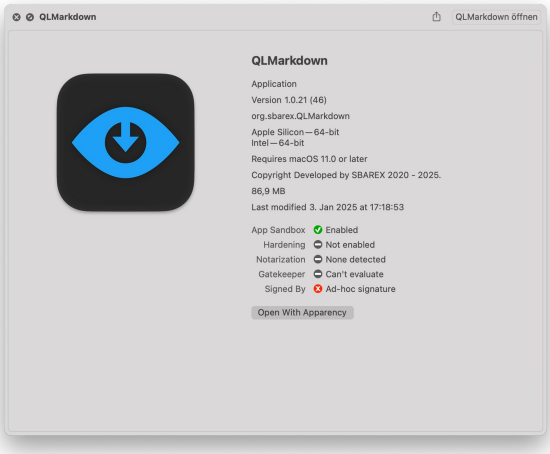
Zur Bestätigung folgt ein Ausflug in die Kategorie „Datenschutz & Sicherheit“ der Einstellungen-App. Im Aufklappmenü „Apps erlauben von“ erscheint nun der zusätzliche Eintrag „Überall“. Auch das bestätigen Sie mit Ihrem Kennwort. Dann erscheint eine erneute Warnung; um die Verifizierung auszuschalten, müssen Sie auf den Button mit der Aufschrift „Keine Einschränkungen“ in roten Lettern klicken. Um diese Option aus den Sicherheitseinstellungen verschwinden zu lassen, geben Sie im Terminal den folgenden Befehl ein:

```
sudo spctl --global-enable
```

Um macOS dauerhaft von der Notarisierungsüberprüfung zu entbinden, muss man sich mehrfach authentifizieren und Warnungen durchlesen.

Mehr Details mit Apparency

Auch wenn die macOS-Warnungen drastisch sind, verraten sie gleichzeitig wenig Details über den Status und die Herkunft einer App. Apples Sicherheitsmaßnahmen haben durchaus ihre Berechtigung; im Allgemeinen sind Anwender gut damit beraten, der Apple-Verifikation zu vertrauen. Um eine qualifizierte Entscheidung für eine Ausnahme treffen zu können, bedarf es möglichst vieler Information zum Programm und dessen Entwickler. Wer mehr über ein heruntergeladenes Programm wissen will, kann das kostenlose Werkzeug Apparency installieren. Es analysiert den Sicherheitsstatus einer App, liefert ausführliche Details und verrät, von wem sie stammt.



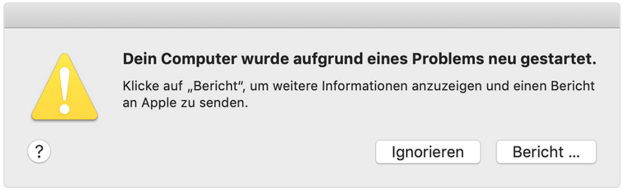
Apparency gibt detaillierte Informationen zu einer App über die Quicklook-Funktion.

Was tun bei Kernel Panics?

Quellen: mactechnews.de, Howard Oakley

Selten bekommt ein Mac-Anwender es mittlerweile zu Gesicht, das dunkelgraue Bildschirm-Overlay mit dem Symbol des Power-Buttons im Hintergrund und der Aufforderung in fünf Sprachen, den Mac auszuschalten. Umso dringlicher gerät die Ursachenforschung, um dessen wiederholtes Erscheinen zu vermeiden. Eine Kernel Panic, welche dieser Bildschirm signalisiert, beendet sämtliche laufenden Prozesse. Die Folge sind potenzielle Datenverluste und eventuell sogar eine beschädigte Dateihierarchie. Howard Oakley, versierter Mac-Experte und -Entwickler, gibt Tipps, wie Anwender dem Ursprung des Fehlers auf die Schliche kommen.

Der wichtigste Schritt, so Oakley, stellt dabei die Indiziensicherung dar, welche beim Neustart direkt nach der Kernel Panic notwendig wird. Nachdem der macOS-Schreibtisch geladen wurde, erscheint binnen einer Minute eine Meldung (Panic Alert) mit der Überschrift „Dein Mac wurde aufgrund eines Problems neu gestartet“, gefolgt von einer Aufforderung, den Fehlerbericht an Apple zu senden. Dafür klickt man auf den Button „Bericht …“, um die Fehlermeldung einzusehen. Deren Inhalt müsse ein Nutzer eigenständig markieren, kopieren und in ein neues TextEdit-Dokument kopieren. Erst nach dem Speichern dieser Datei sollten Anwender auf den Button „An Apple senden“ klicken. Das Verschicken führe nämlich keineswegs dazu, dass Apple die Meldung studiere und sich zeitnah zurückmelde. Panic Logs würden lediglich maschinell verarbeitet; Oakley ist kein Fall bekannt, bei dem Apple-Entwickler nach einem Panic Log bei Anwendern gemeldet hätten.



Nach einem Klick auf „Bericht …“ erhält man Einblick ins Panic-Log. (Quelle: Apple Support)

Fehlersuche bei Hardware

Nach dieser Maßnahme sollten Anwender zunächst die wahrscheinlichsten Fehlerquellen ausschließen. Diese sind in überwiegenden Fällen in der angeschlossenen Hardware zu suchen. Vorsorglich stöpselt man alle externen Geräte ab, welche zum Zeitpunkt der Kernel Panic verbunden waren. Taucht in diesem Fall der Fehler nicht mehr auf, wird ein Gerät nach dem anderen wieder mit dem Mac verbunden. Gibt es beim Anschließen eines Geräts erneute Kernel Panics, haben Sie wahrscheinlich den Verursacher gefunden.

Um die Mac-eigene Hardware zu überprüfen, nutzen Sie den Diagnosemodus. Je nach Chip gibt es dafür ein anderes Vorgehen:

- Intel: Neustart bei gedrückter D-Taste
- Apple-Silicon: Power-Button gedrückt halten, im Start-Menü cmd+D drücken.

Daraufhin lädt der Mac ein aktuelles Diagnosesystem übers Netz und überprüft Gerätekomponenten auf Fehler. Erscheint hier etwas anderes als „Keine Fehler gefunden“, wendet man sich am besten an einen autorisierten Apple-Techniker.

Systemerweiterungen können schuld sein

Seit macOS 14 (Sonoma) erlaubt Apple keine Erweiterungen (Kernel Extensions) mehr von Drittanbietern. Man muss eigenständig die System Integrity Protection deaktivieren, bevor eine Installation möglich ist. Auf älteren Systemen kann der Bestand an Erweiterungen weiterhin Probleme auslösen. Um solche (und die Apple-eigenen, welche Teil von macOS sind) als Ursache auszuschließen, startet man einen Intel-Mac bei gedrückter Shift-Taste. Bei Macs mit M-Prozessoren halten Sie den Startknopf gedrückt, bis der Wiederherstellungsmodus erscheint. Nachdem Sie das Startvolume ausgewählt haben, halten Sie die Shift-Taste gedrückt, sodass der darunterliegende Button mit „Im sicheren Modus fortfahren“ beschriftet ist. Klicken Sie darauf, startet macOS ohne Systemerweiterungen und zusätzliche Schriften.

Erscheinen Kernel Panics regelmäßig, bleiben aber im sicheren Modus aus, ist die Wahrscheinlichkeit groß, dass dies an einer Systemerweiterung eines Drittanbieters liegt. In diesem Fall sollten Sie in Betracht ziehen, den Bestand an Kernel Extensions zu löschen.

Fehlerbericht analysieren

Wenn weder Hardware noch Kernel Extensions Schuld an Kernel Panics sind, muss der Fehlerbericht nach einer Ursache durchgeforstet werden. Mehrfache Abstürze sind in diesem Fall tatsächlich hilfreich, sofern Sie bei jedem den Fehlerbericht gesichert haben. So entdecken Sie eventuell Gemeinsamkeiten. Dies stellt sich als aufwendig heraus: Bei einem Speicherleck eines Programms oder einer Systemkomponente erscheint gegebenenfalls ein Hinweis wie „Backtrace suspected of leaking“ im Bericht. Zeilen, die mit „Panicked Task“ beginnen, geben in vielen Fällen einen Hinweis auf die Software-Ursache des Fehlers. Auf eine einfache Lösung können Sie in solchen Fällen kaum hoffen; hier ist ein geduldiges Beobachten und Sammeln von Fehlerberichten gefragt. Liegt die wahrscheinliche Ursache in Apples Einflussbereich, etwa in Form einer Systemkomponente oder eines Programms, sollte man ein zusätzliches Melden via Apple Feedback in Betracht ziehen, so Oakley.

Ergänzende Artikel:

Mac-Wartung: Alte Kernel-Erweiterungen entfernen

macOS-Praxis: Was kann der Wiederherstellungsmodus unter Apple Silicon?