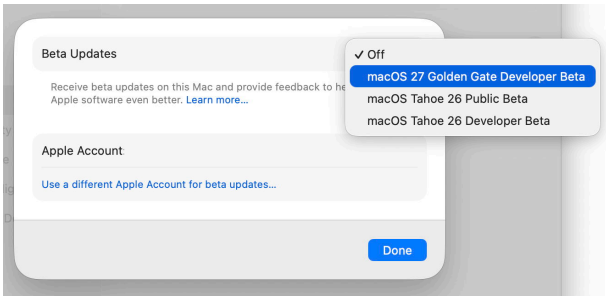
Soll man die Golden Gate-Beta ausprobieren?

von Howard Oakley, eclecticlight.co • Übersetzung: KJM

In den nächsten Wochen wird Apple voraussichtlich die erste öffentliche Beta-Version von macOS 27 „Golden Gate“ veröffentlichen. Dieser Artikel soll Ihnen bei der Entscheidung helfen, ob Sie dieses verlockende Angebot nutzen oder lieber ablehnen sollten.

Um die öffentliche Beta-Version zu installieren, müssen Sie keinen speziellen Enabler von einer geschlossenen Website herunterladen, da dies über eine zusätzliche Option in „Software-Update“ erfolgt. Sie müssen sich lediglich hier registrieren, und sobald die öffentliche Beta veröffentlicht ist, sollte sie in „Software-Update“ angeboten werden, sofern Ihr Mac mit dem Apple-Account angemeldet ist, mit dem Sie sich registriert haben. Dort gibt es auch eine Option für diejenigen, die einen anderen Apple-Account für Betas verwenden möchten.



Obwohl die endgültige Version wahrscheinlich eher als Update denn als vollständiges Upgrade mit eigener Installations-App bereitgestellt wird — vorausgesetzt, Sie führen ein Upgrade von macOS Tahoe durch —, wird Ihre erste Beta-Version wahrscheinlich fast die Größe einer IPSW-Image-Datei haben und nicht als App vorliegen. Sie enthält ein mBoot-Firmware-Update, von dem sie nur durch eine Wiederherstellung des Mac im DFU-Modus heruntergestuft werden kann, was es für die meisten zu einer Einbahnstraße macht.

Haben Sie einen Apple-Silicon-Mac in Reserve?

Anders als in den letzten Jahren läuft Golden Gate nur auf Apple-Silicon-Macs, die für viele mittlerweile ihre Arbeitsrechner sind. Man kann einen Intel-Mac in Reserve nicht umfunktionieren; wenn du also nicht mindestens zwei Macs mit Chips der M-Serie hast, ist es wahrscheinlich am klügsten, die Beta nicht auszuprobieren.

Mein Dank gilt allen Lesern, die mir helfen, die MACtreff-Köln-Homepage und den Newsletter zu finanzieren.

Wer meine Arbeit unterstützen möchte, den bitte ich um eine Spende auf mein Paypal-Konto: paypal.me/KJM54

Die gute Nachricht ist, dass Golden Gate auf allen Macs mit Apple Silicon läuft, sogar auf denen mit dem ursprünglichen M1. Die einzigen Einschränkungen betreffen die Ausführung fortgeschrittener KI auf dem Chip, wofür ein M3 oder neuer mit mindestens 12 GB Arbeitsspeicher erforderlich ist.

Was bietet die Beta?

Apples offizielle Übersicht über neue Funktionen fällt dieses Jahr recht kurz aus. Zu den wichtigsten Punkten gehören:

- Siri-KI und fortgeschrittene KI, die größtenteils erst später verfügbar sein werden,
- Kindersicherungsfunktionen,
- Optimierungen am Benutzeroberflächendesign,
- Schnellere Leistung.

Ich habe meine eigene Zusammenfassung der interessanten neuen Funktionen erstellt, die auf der WWDC vorgestellt wurden.

Sie sollten sich auch über einige der veralteten und entfernten Funktionen im Klaren sein, die ich hier untersucht habe. Die Time-Capsule-Unterstützung ist vielleicht die bedeutendste davon, und beachtet, dass der Zugriff auf verschlüsseltes HFS+ noch nicht entfernt wurde und erst mit macOS 28 im nächsten Jahr wegfallen wird.

Zwei Verbesserungen, die Ihnen höchstwahrscheinlich auffallen werden, betreffen die Benutzeroberfläche und die Leistung. Golden Gate macht die vielen Änderungen an der Benutzeroberfläche von Tahoe zwar nicht rückgängig, glättet aber einige Ecken und Kanten, und die meisten Nutzer empfinden die Version dadurch als deutlich besser. Leistungsverbesserungen sind durchweg spürbar, und die ausführliche Erklärung von CodeColorist ist sehr lesenswert.

Es scheint nur wenige Kompatibilitätsprobleme zu geben: Wenn eine App unter Tahoe einwandfrei läuft, sollte dies auch in den Golden-Gate-Betas der Fall sein. Apple stellt zudem umfangreiche Versionshinweise zur Verfügung, die eventuelle Probleme erklären könnten, auf die Sie stoßen.

Könnten Sie diesen Mac verlieren?

Die nächste Frage, die Sie sich stellen sollten, ist, ob Sie es sich leisten könnten, Ihren Mac für eine Weile komplett zu verlieren — als Folge eines Problems mit der Beta. Auch wenn dies höchst unwahrscheinlich ist, ist es ein Risiko, auf das du vorbereitet sein musst, wenn du eine Vorabversion von macOS installierst.

Installieren Sie unter keinen Umständen eine Beta-Version von macOS auf einem Mac, den Sie für produktive Zwecke nutzen. Betas bringen ausnahmslos Firmware-Updates mit sich; selbst wenn Sie die Beta auf einer externen Festplatte installieren, wird dadurch die Firmware Ihres Macs geändert. Um dies rückgängig zu machen, benötigen Sie ei-

nen zweiten Mac und ein USB-C-Kabel, müssen den betroffenen Mac in den DFU-Modus versetzen und ihn aus einer Tahoe-IPSW-Image-Datei wiederherstellen. Danach müssen Sie ihn von Grund auf neu einrichten und Ihre Dateien aus einem Backup migrieren. Auch wenn dies eine wertvolle Funktion von Macs mit Apple-Silicon ist, sollte es nicht notwendig sein, dass man dies tun muss, um seinen Mac wieder nutzbar zu machen.

Beta-Versionen enthalten in der Regel auch aktualisierte Versionen wichtiger Komponenten wie iCloud, das APFS-Dateisystem und Time Machine. Überlegen Sie sorgfältig, welche verheerenden Folgen dies haben könnte, falls ein Fehler vorliegt, der andere von diesem Mac genutzte Speichermedien und dessen Backups beeinträchtigt.

Interne oder externe SSD?

Eine Möglichkeit, das durch Beta-Versionen von macOS ausgehende Risiko zu verringern, besteht darin, diese auf einem externen Speichermedium zu installieren. Das sorgt zwar für eine gewisse Trennung und einen gewissen Schutz, bedeutet aber dennoch, dass die Firmware aktualisiert wird, was ein erhebliches Risiko für einen Totalausfall birgt. Versuchen Sie dies nicht mit einem Mac, den Sie im Alltag nutzen — auch nicht von einer externen Festplatte aus.

Wenn Sie die Beta-Version auf einer externen Festplatte installieren möchten, müssen Sie mit dem Verfahren für Apple-Silicon-Macs vertraut sein. Auch wenn es mit etwas Übung recht einfach wird, scheinen manche Nutzer überhaupt nicht damit zurechtzukommen. Ein entscheidendes Detail ist, dass die Installation durchgeführt wird, während die externe SSD an einen Nicht-DFU-Anschluss angeschlossen ist.

Mehrere Systeme auf derselben Festplatte

Sie können auch mehrere Startvolume-Gruppen auf derselben Festplatte installieren, sodass Sie wählen können, von welcher Version von macOS Sie starten möchten. Dies bietet noch weniger Trennung und Schutz als die Installation auf separaten Festplatten und sollte daher niemals auf einem Mac im produktiven Einsatz versucht werden.

Apple empfiehlt, dies in separaten Startvolume-Gruppen innerhalb desselben APFS-Containers zu tun, was den großen Vorteil hat, dass sie sich denselben freien Speicherplatz innerhalb dieses Containers teilen. Es gibt jedoch Situationen, in denen sich dies nachteilig auswirken kann, und möglicherweise ziehen Sie stattdessen separate Container vor. Die Entscheidung liegt bei Ihnen.

Virtuelle Maschine

Manche halten es für die beste Methode, um Probleme beim Ausprobieren von Beta-Versionen von macOS zu vermeiden, diese in einer virtuellen Maschine (VM) zu installieren. Dadurch kann die Firmware des Macs, auf dem die VM läuft, nicht verändert werden, und schon das allein macht die Vorgehensweise wesentlich sicherer. Verwenden Sie einen beliebigen Virtualisierer, darunter Parallels, UTM und mein eigenes Viable.

Theoretisch müsst ihr lediglich die Golden-Gate-Beta-IPSW eurer Wahl über den Link von Mr. Macintosh zu den Apple-Servern herunterladen und damit eine neue VM erstellen. In der Praxis kann dies jedoch fehlschlagen, sofern der Vorgang nicht auf einem Host durchgeführt wird, auf dem Golden Gate läuft. Um den Vorgang erfolgreich abzuschließen, veröffentlicht Apple möglicherweise einen Systemsoftware-Enabler. Falls dies nicht der Fall ist (was häufig vorkommt), haben Sie möglicherweise mehr Glück, wenn Sie die aktuelle Beta von Xcode 27 auf dem Host installieren. Jemand hat dieses Problem sogar umgangen, indem er sein iPhone an seinen Mac angeschlossen hat.

Eine Methode, die bereits erfolgreich mit Golden Gate angewendet wurde, besteht darin, eine Tahoe-VM mit dem vollständigen Installationsprogramm für die Beta zu aktualisieren, obwohl diese VM anschließend nicht mehr auf spätere Versionen aktualisiert werden konnte — ein weiteres häufiges Problem bei VMs, auf denen Betaversionen laufen.

Kernel-Panics

Falls Sie sich entscheiden, die Golden-Gate-Beta zu installieren, oder dies bereits getan haben, möchte ich Sie im Namen von zig Millionen Nutzern und der meisten Apple-Ingenieure um einen großen Gefallen bitten. Schauen Sie sich die neuen Funktionen auf jeden Fall genau an und geben Sie Apple reichlich Feedback dazu, was Sie davon halten. Aber bitte achten Sie besonders auf die Grundlagen und testen Sie Ihren Mac mit Peripheriegeräten wie externen Bildschirmen und Hubs. Sollten Sie Probleme entdecken, arbeiten Sie bitte mit Apple zusammen, um sicherzustellen, dass das Unternehmen davon erfährt. Wenn möglich, testen Sie Funktionen wie Time Machine (achten Sie dabei darauf, Ihre bestehenden Backups nicht zu gefährden), die von Betatestern selten beachtet werden.

Senden Sie insbesondere Feedback-Berichte zu jedem Kernel-Panic, den Ihr Mac während der Ausführung einer Beta-Version aufweist. Das normale Panikprotokoll, das nach dem Neustart Ihres Mac gesendet wird, ist hilfreich, aber weitere Details sind noch besser. Selbst Betaversionen sollten niemals Kernel-Panics aufweisen; sollte dies bei Ihrem Mac der Fall sein, helfen Sie bitte den Apple-Ingenieuren, dieses Problem zu beheben, bevor Golden Gate veröffentlicht wird.

Allen, die Golden Gate als Betatester testen, wünsche ich viel Erfolg und hoffe, dass sie Spaß am Testen haben und Apple dabei helfen, macOS für uns alle noch besser zu machen.

Was tun, wenn der Mac zu heiß wird?

von Howard Oakley, eclecticlight.co • Übersetzung: KJM

Da ein Großteil Europas letzte Woche unter der Hitze litt, ist es an der Zeit, uns die Warnzeichen in Erinnerung zu rufen, die darauf hindeuten, dass unsere Macs zu heiß werden. Da Macs bei Hitze nicht so „schwitzen" wie wir, ist es außerdem wichtig zu wissen, was wir tun können, um sie abzukühlen.

Eines der ernstesten Warnzeichen für einen drohenden Hitzschlag beim Menschen erscheint paradox: Die Betroffenen hören auf zu schwitzen, und ihre Haut wird eher blass als rot. Das liegt daran, dass ihr Kreislauf zusammengebrochen ist, und wenn sie nicht sehr schnell abgekühlt werden, besteht ein echtes Risiko für schwere Verletzungen oder den Tod.

Überhitzte Macs haben ihr eigenes Paradoxon: Öffnen Sie den Aktivitätsmonitor, wählen Sie die CPU-Ansicht aus, und ganz oben in der Liste der CPU-Auslastung steht `kernel_task`, die die CPU-Kerne mit 100 % oder mehr beansprucht, statt wie üblich mit etwa 4 %. Widerstehen Sie der Versuchung, diesen Prozess zu beenden, in der Hoffnung, dass er von selbst verschwindet, denn er hat die Kontrolle über Ihren Mac übernommen, *um ihn abzukühlen*.

Ursachen

Jeder Mac verfügt über mehrere Temperatursensoren, die vom Core-Duet-Subsystem überwacht werden, wodurch der System Management Controller (SMC) die internen Umgebungsbedingungen und Dienste steuern kann. Wenn ein Prozess außer Kontrolle gerät und die Kerne übernimmt oder interne Temperatursensoren ungewöhnlich hohe Temperaturen registrieren, reagiert Core Duet mit einer Reihe von Maßnahmen, um die Kühlung zu verstärken. Dazu gehören das aktive Lüftungssystem, dessen Lüfter auf Hochtouren laufen, um Kühlluft über empfindliche Komponenten zu blasen, sowie die Reduzierung der CPU-Auslastung, um die Wärmeentwicklung zu senken. Wo möglich, wird dadurch die Prozessorgeschwindigkeit gedrosselt und jeder außer Kontrolle geratene Prozess blockiert, indem die CPU mit `kernel_task` ausgelastet wird.

Was auch immer Sie tun — versuchen Sie auf keinen Fall, `kernel_task` daran zu hindern, seine Arbeit zu verrichten. Das ist in etwa so, als würde man jemanden daran hindern, zu trinken, um den durch Schweiß verursachten Flüssigkeitsverlust auszugleichen, und wird die Situation nur verschlimmern. Wenn die Lüfter laut werden und `kernel_task` Ihre CPU in Beschlag nimmt, ist es an der Zeit, alles zu tun, um Ihren Mac abzukühlen.

Es gibt seltene Fälle, in denen die Lüfter auf Hochtouren laufen und `kernel_task` außer Kontrolle gerät, ohne dass ein thermisches Problem vorliegt. Bei Intel-Macs hilft in der Regel ein Zurücksetzen des SMC, doch dies könnte stattdessen auch auf einen Fehler in einem Temperatursensor oder im SMC selbst zurückzuführen sein. Eine Hardware-Diagnose sollte dir weitere Aufschlüsse geben. Die mit Abstand häufigste Ursache für anhaltende Probleme sind Staub und Schmutz in den Lüftungskanälen sowie bei einigen Intel-Mac-Notebooks eine Überhitzung der linken USB-C-Anschlüsse. Weitere Details findest du in Apples Hinweis zu `kernel_task`, der auch bestätigt, was ich hier geschrieben habe.

Warnzeichen

Eines der besten Frühwarnzeichen für eine Überhitzung — selbst wenn Ihr Mac keine hörbaren Lüfter hat — ist eine träge Bedienung, die darauf zurückzuführen ist, dass `kernel_task` die CPU-Kerne in Beschlag nimmt. Das Scrollen in Fenstern mit Videos und Bildern wird ruckelig, die Reaktion auf Bedienelemente verzögert sich und das Wechseln zwischen Apps dauert merklich lange. Dies kann durch beliebige Aufgaben verursacht werden, die übermäßig viel CPU-Leistung beanspruchen, und es dauert nur wenige Sekunden, im Aktivitätsmonitor zu überprüfen, was vor sich geht.

Sie können dann nach und nach geöffnete Apps beenden, die möglicherweise zur Überhitzung beitragen, und dabei `kernel_task` in der CPU-Ansicht im Auge behalten. So können Sie auch feststellen, welche Apps am stärksten dafür verantwortlich sind und nach dem Abkühlen Ihres Macs wieder sicher geöffnet werden können. Dies ist besonders nützlich für Intel-Macs, die mehr Wärme erzeugen.

Maßnahmen

Wenn Ihr Mac erste Anzeichen thermischer Belastung zeigt und noch läuft, fördern Sie die Wärmeabgabe, indem Sie sofort:

- den Deckel vollständig öffnen, wenn der Mac im Clamshell-Modus ist,
- sicherstellen, dass alle Lüftungsöffnungen im Gehäuse frei von Hindernissen sind,
- Platz rund um das gesamte Gehäuse, einschließlich der Unterseite, schaffen, um die Konvektionskühlung zu unterstützen,
- den Mac in den Schatten stellen, wenn er in der Sonne steht,
- einen externen Lüfter einschalten, um das Gehäuse durch erzwungene Konvektion zu kühlen,
- den Mac an einen kühleren Ort bringen, falls eine Klimaanlage verfügbar ist.

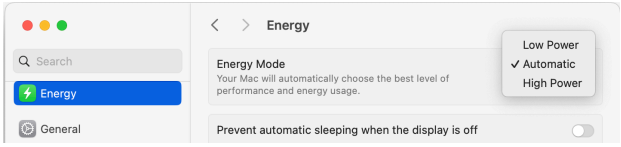
Reduzieren Sie die Wärmeentwicklung sofort, indem Sie:

- alle geöffneten Apps beenden und gegebenenfalls solche, die sich nicht schließen lassen, zwangsweise beenden,
- alle nicht unbedingt notwendigen Prozesse im Aktivitätsmonitor beenden, die mehr als 5–10 % der CPU-Leistung beanspruchen (mit Ausnahme von `kernel_task`),
- das Netzladekabel abziehen, sofern der Akku ausreichend geladen ist.

Verfügt ein Mac über Lüfter, ist es besser, ihn laufen zu lassen, da ein Herunterfahren auch verhindert, dass diese Lüfter weiterhin Kühlluft ins Innere blasen. Manche legen gerne Kühlakkus an das Gehäuse an, wodurch die Außenseite schneller gekühlt werden kann als mit einem externen Lüfter. Wenn Sie das ausprobieren möchten, achten Sie darauf, dass kein Kondenswasser in den Mac eindringt, insbesondere nicht über die Tastatur oder die Lüftungsöffnungen, und blockieren Sie weder die Tastatur noch die Lüftungskanäle.

Hochleistungs- und Energiesparmodus

Einige Macs bieten in ihren Akku- oder Energieeinstellungen einen oder zwei Energiemodi an. Sofern verfügbar, können diese nützlich sein, um die Wärmeentwicklung und den Wärmeabfluss eines Macs zu steuern, funktionieren jedoch ganz unterschiedlich. Auch ihre Bezeichnung kann verwirrend sein: Sie werden als **Energy Mode** angeboten, doch die Menüoptionen beziehen sich eigentlich auf den **High Power Mode** und den **Low Power Mode**. Apple stellt detaillierte Informationen dazu bereit und gibt an, welche Modelle die jeweiligen Modi unterstützen.



Der **Energiesparmodus** reduziert die Wärmeentwicklung, indem er die Taktraten der CPU- und GPU-Kerne begrenzt, sodass die maximale Wärmeentwicklung geringer ist und der Akku mit einer Ladung länger hält. Dadurch laufen die Lüfter zudem leiser.

Der **Hochleistungsmodus** bewirkt nicht das Gegenteil und erhöht die Wärmeentwicklung gegenüber dem Normalbetrieb nicht. Stattdessen setzt der Mac seine Lüfter intensiver ein, um bei langen und anspruchsvollen Aufgaben länger kühl zu bleiben.

Wenn Sie versuchen, Ihren Mac abzukühlen, weil er zu heiß geworden ist, sollten Sie den Modus „Automatisch“ oder „Hohe Leistung“ als am besten geeignet empfinden, sobald Sie alle Apps geschlossen haben — obwohl Core Duet die Kontrolle übernehmen und das tun sollte, was zu diesem Zeitpunkt am effektivsten ist.

Anhaltende Probleme

Bei extremer Hitze, wenn Sie Ihren Mac nicht an einem klimatisierten Ort nutzen können und `kernel_task` weiterhin mit hoher CPU-Auslastung läuft, sollten Sie Ihren Mac so weit wie möglich abkühlen, bis die Auslastung von `kernel_task` unter 10 % sinkt; dann können Sie möglicherweise mit jeweils nur einer geöffneten App weiterarbeiten. Wenn das nicht funktioniert, lassen Sie Ihren Mac am besten im Leerlauf abkühlen und fahren Sie ihn dann herunter, bis die Temperaturen gesunken sind.

Bleiben Sie cool!

Haben meine Daten ein Leck?

Quelle: SoftMaker

Alle paar Wochen taucht eine Meldung auf: Millionen Kundendaten gestohlen, Passwörter im Darknet aufgetaucht, Datenleck bei einem großen Onlinedienst. Man liest es, denkt sich „betrifft mich hoffentlich nicht“ – und scrollt weiter.

Aber was, wenn es Sie längst betrifft?

Datenlecks sind keine Ausnahme – sie sind Alltag

Die Vorstellung, dass ein Datenleck etwas Seltenes ist, das nur großen Firmen passiert und nur unvorsichtige Nutzer trifft, ist leider überholt. In Wahrheit wurden in den vergangenen Jahren *Milliarden* von Datensätzen gestohlen – bei LinkedIn, bei Adobe, bei Dropbox, bei Facebook und bei Hunderten weniger bekannter Dienste.

Die gestohlenen Daten landen in Sammlungen, die im Darknet gehandelt werden. Dort stehen dann E-Mail-Adressen, Passwörter, manchmal auch Telefonnummern und Geburtsdaten – ordentlich sortiert und durchsuchbar. Kriminelle nutzen diese Daten für automatisierte Angriffe: Sie probieren die gestohlenen Passwörter bei anderen Diensten aus, verschicken gezielte Phishing-Mails oder versuchen, mit den persönlichen Informationen Identitätsbetrug zu begehen.

Das Heimtückische daran: Sie merken davon nichts. Es gibt keinen Alarm, keine Benachrichtigung, kein rotes Lämpchen. Es sei denn, Sie prüfen es selbst.

Have I Been Pwned – der bekannteste Leck-Prüfer

Der australische IT-Sicherheitsexperte Troy Hunt hat 2013 einen Dienst ins Leben gerufen, der genau diese Lücke schließt: Have I Been Pwned (kurz HIBP – das „Pwned“ stammt aus der Gamer-Sprache und bedeutet so viel wie „erwischt“ oder „gehackt“).

Das Prinzip ist denkbar einfach: Sie geben Ihre E-Mail-Adresse ein, klicken auf „pwned?“ – und innerhalb von Sekunden erfahren Sie, ob diese Adresse in einem bekannten Datenleck auftaucht. Falls ja, zeigt Ihnen die Seite, *welche* Dienste betroffen waren und *welche Art* von Daten gestohlen wurde – zum Beispiel Passwörter, IP-Adressen oder Geburtsdaten.

Ich habe das vor ein paar Jahren zum ersten Mal ausprobiert, eher aus Neugier. Das Ergebnis war ernüchternd: Meine Haupt-E-Mail-Adresse tauchte in sechs verschiedenen Datenlecks auf. Darunter ein Onlineshop, bei dem ich mich kaum noch erinnern konnte, jemals ein Konto gehabt zu haben. Das Passwort, das ich dort verwendet hatte? Dasselbe wie bei drei anderen Diensten. Ein unangenehmer Moment der Selbsterkenntnis.

Ist das sicher?

Die naheliegende Frage: Kann ich einer Website, die nach Datenlecks sucht, meine E-Mail-Adresse anvertrauen? Bei Have I Been Pwned: ja. Der Dienst speichert keine Suchanfragen, erfordert keine Anmeldung und gehört mittlerweile zu den am häufigsten empfohlenen Sicherheitstools weltweit. Selbst das FBI liefert Daten aus beschlagnahmten Datenleck-Sammlungen an HIBP, damit Betroffene gewarnt werden können.

Für die Passwortprüfung (dazu gleich mehr) wird sogar ein besonders datenschutzfreundliches Verfahren eingesetzt: Ihr Passwort wird lokal auf Ihrem Gerät in einen Hash umgewandelt – eine Art digitalen Fingerabdruck. An den Server werden nur die ersten fünf Zeichen dieses Hashs gesendet. Der Server antwortet mit einer Liste möglicher Treffer, und Ihr Browser prüft den Abgleich lokal. Das eigentliche Passwort verlässt also nie Ihren Rechner.

Was tun, wenn Ihre Adresse betroffen ist

Falls Have I Been Pwned einen Treffer meldet – und bei den meisten Lesern wird das der Fall sein –, ist das zunächst kein Grund zur Panik. Es bedeutet, dass Ihre E-Mail-Adresse und möglicherweise ein Passwort in einer gestohlenen Datenbank aufgetaucht sind. Was Sie jetzt tun:

- **Passwort sofort ändern** – bei dem betroffenen Dienst, aber auch überall sonst, wo Sie dasselbe Passwort verwendet haben.
- **Jedes Konto bekommt ein eigenes Passwort** – das ist die wichtigste Regel überhaupt. Wenn ein Dienst gehackt wird und Sie dort ein einzigartiges Passwort verwenden, bleibt der Schaden begrenzt.
- **Passwort-Manager nutzen** – niemand kann sich 80 verschiedene Passwörter merken. Programme wie

Bitwarden, KeePass oder 1Password übernehmen das für Sie. Ein Thema, dem wir uns in einem späteren Beitrag ausführlich widmen werden.

- **Benachrichtigungen aktivieren** – bei HIBP können Sie Ihre E-Mail-Adresse registrieren und werden automatisch informiert, wenn sie in einem neuen Datenleck auftaucht.

Andere nützliche Prüftools

Have I Been Pwned ist das bekannteste Tool, aber nicht das einzige. Hier ein kurzer Überblick über seriöse Alternativen:

Have I Been Pwned – Passwortprüfung: Auf der Unterseite Pwned Passwords können Sie prüfen, ob ein bestimmtes Passwort in einem bekannten Datenleck aufgetaucht ist. Der Abgleich funktioniert über das oben beschriebene Hash-Verfahren – das Passwort selbst wird nicht übertragen. Erschreckend: „123456“ taucht in über 40 Millionen Datenlecks auf.

HPI Identity Leak Checker: Der Identity Leak Checker des Hasso-Plattner-Instituts in Potsdam ist eine deutsche Alternative. Sie geben Ihre E-Mail-Adresse ein und erhalten per E-Mail einen Bericht darüber, welche Daten betroffen sind. Für Nutzer, die ihre Daten lieber bei einer deutschen Institution als bei einem australischen Dienst eingeben möchten, eine gute Option.

Mozilla Monitor: Mozilla bietet mit Mozilla Monitor einen Dienst an, der auf den Daten von Have I Been Pwned basiert, aber in eine übersichtliche Oberfläche verpackt ist. Wer Firefox nutzt, kann sich direkt im Browser warnen lassen.

Was diese Tools nicht leisten

So nützlich diese Dienste sind — sie haben eine wichtige Einschränkung: Sie kennen nur *bekannte* Datenlecks. Wenn Ihre Daten bei einem Einbruch gestohlen wurden, der nie öffentlich wurde, tauchen sie in keiner dieser Datenbanken auf. Die Abwesenheit eines Treffers bedeutet also nicht, dass Ihre Daten garantiert sicher sind. Sie bedeutet nur, dass sie in keiner *bekannten* Sammlung gefunden wurden.

Und noch etwas: Diese Tools prüfen E-Mail-Adressen und Passwörter, aber nicht Ihre gesamte digitale Identität. Ob Ihre Kreditkartendaten, Ihre Personalausweisnummer oder Ihre Adresse in einem Datenleck stecken, erfahren Sie auf diesem Weg in der Regel nicht.

Fünf Minuten, die sich lohnen

Datenlecks gehören leider zur Realität des digitalen Lebens. Wir können nicht verhindern, dass ein Onlinedienst gehackt wird, bei dem wir vor zehn Jahren ein Konto erstellt haben. Was wir aber tun können: regelmäßig prüfen, ob unsere Daten betroffen sind – und die richtigen Konsequenzen daraus ziehen.

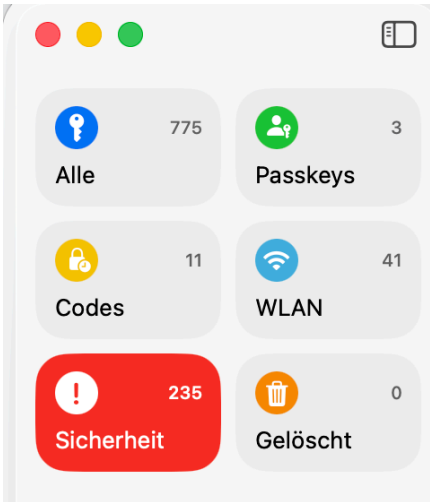
Der Aufwand ist minimal: Adresse eingeben, Ergebnis lesen, betroffene Passwörter ändern. Fünf Minuten, die im Ernstfall viel Ärger ersparen können.

Mein Vorschlag: Probieren Sie es gleich aus. Öffnen Sie haveibeenpwned.com, geben Sie Ihre meistgenutzte E-Mail-Adresse ein – und schauen Sie, was passiert. Falls Sie mutig sind, testen Sie auch gleich Ihr Lieblingspasswort auf der Passwortprüfung.

Anmerkung KJM:

Das Blog der Firma SoftMaker, die für ihre Office-Alternative SoftMaker Office (für Windows, Mac, Linux, iPhone, iPad und Android), für ihr PDF-Programm FlexiPDF (für Windows) und für verschiedene Schriften-Pakete bekannt ist, ist nicht gerade Mac-lastig.

Daher will ich hier ergänzen, dass Apples auf Macs, iPhones und iPads vorhandene Anwendung **Passwörter** einen separaten Abschnitt „Sicherheit“ enthält, in dem die App *„deine Passwörter privat und sicher überwacht und dich informiert, wenn sie leicht zu erraten sind, mehrfach verwendet wurden oder in Datenlecks von Websites aufgetaucht sind.“* Zudem bietet sie für gefundene problematische Passwörter Hilfe an, diese direkt auf der betroffenen Website zu ändern.



Apple: Sicherheitsupdates sollen vor KI-Hacks schützen

Quelle: macgadget.de

Die Schattenseiten der sog. „KI“ werden noch immer viel zu wenig thematisiert. Sie schadet der menschlichen Kreativitität (Bilder und Musik auf Knopfdruck erzeugen, gänzlich ohne künstlerischen Wert; was ist heutzutage noch echt, was Fake?) und schadet dem selbstständigen und kritischen Denken (Chatbot-Antworten, die nach wie vor häufig unvollständig-unpräzise-irreführend bis hin zu komplett falsch sind, wird zu oft ohne Hinterfragen vertraut) — von Dauerbrenner-Fragen hinsichtlich Urheberrecht (durften die LLMs die Daten, die fürs Training genutzt wurden, überhaupt verwenden?), Ethik (soll „KI“ über Menschen bestimmen?), Umweltschutz (irrsinniger Aufwuchs von Rechenzentren mitsamt Energiebedarf und Kühlung), Datenschutz (alle eigenen Daten einfach der „KI“ zur Verfügung stellen?) usw. ganz abgesehen. Nun kommt ein weiterer wichtiger Aspekt hinzu.

Auf die Softwareentwicklung spezialisierte LLMs können inzwischen die mühsame Handarbeit beim Programmieren über große Strecken übernehmen, d. h. die Eingabe von Code. Entwickler haben dadurch mehr Zeit für Konzeption, Qualitätssicherung, Support, Vertrieb und die vielen anderen Aspekte, die mit der Softwareentwicklung zusammenhängen (mit dem Coden allein ist es ja nicht getan). Auch können LLMs inzwischen recht gut Sicherheitslücken aufspüren — doch genau hier lauert eine neue Gefahr.

Derartige LLMs werden inzwischen auch zur Entwicklung einer nächsten Generation an Schadsoftware eingesetzt. Für die Großen der Branche wie Apple, Microsoft und Google ist dies ein zweischneidiges Schwert. LLMs vereinfachen zwar die Suche nach Schwachstellen und haben in den letzten Monaten dabei mitgeholfen, eine riesige Zahl (vierstellig; vielleicht schon fünstellig?) an Lücken abzudichten. Auf der anderen Seite sehen sich die Hersteller neuartigen Bedrohungen durch KI-gestützte Malware ausgesetzt.

So gab Apple nun bekannt, dass die zu Wochenbeginn veröffentlichten Sicherheitsaktualisierungen eine Reaktion auf Bedrohungen durch mögliche KI-Hacks sind. Gegenüber der Nachrichtenagentur Reuters teilte das Unternehmen mit, „dass es sich an die Tatsache anpasse, dass es angesichts der Fähigkeit künstlicher Intelligenz, die Entwicklung bösartiger Hacking-Tools zu beschleunigen, die Zeitspanne zwischen der ersten Veröffentlichung von Updates und deren Bereitstellung für die Kunden verkürzen müsse.“

Demnach seien die Sicherheitskorrekturen von Version 26.5.2 eigentlich für die Version 26.6 geplant gewesen.

macOS/iOS/iPadOS 26.6 liegt jedoch nur als Betaversion vor und erreicht bislang nur einen sehr kleinen Nutzerkreis. Mit der Version 26.5.2 werden diese wichtigen Sicherheitskorrekturen nun mehrere Wochen vor der Veröffentlichung von Version 26.6 für alle Anwender ausgerollt, wobei Apple betont, dass die Lücken (zumindest bislang) nicht aktiv ausgenutzt werden.

Zurück zu „KI“: Sollte man die neuen Werkzeuge und Möglichkeiten gänzlich in Grund und Boden verdammen? Nein, natürlich nicht! Zu einer ausgewogenen Betrachtungsweise gehört eben, dass diese neuen Werkzeuge (der Begriff „Künstliche Intelligenz“ ist, wie schon mehrfach ausgeführt, unzutreffend und irreführend) in nicht wenigen Bereichen eine große Hilfe sind und sogar für Durchbrüche sorgen können:

Die modernen Werkzeuge können beispielsweise in der Medikamentenforschung neue Ansätze aufzeigen, indem sie durch die Analyse riesiger Datenmengen bislang nicht bekannte Wirkstoffkombinationen entdecken und die Entwicklung neuer Wirkstoffe beschleunigen. Die Qualität von Übersetzungen (auch in Echtzeit via Spracherkennung) wurde duch LLMs auf eine neue Stufe gehoben. Informationen können aus umfangreichen Dokumentensammlungen effizient extrahiert und zusammengefasst werden. Aber auch Bereiche wie Materialforschung, Wettervorhersage oder Verkehrsplanung und Routenoptimierung profitieren — alles unter der Prämisse, dass diese modernen Werkzeuge nicht unfehlbar sind. Sie können wichtige Assistenten für den Menschen sein (und bedürfen der Verifikation und Überwachung durch den Menschen), aber eben nicht mehr.

Was passiert mit meinen Accounts, wenn ich sterbe?

Quelle: SoftMaker

Testament, Vorsorgevollmacht, Patientenverfügung — viele von uns haben ihre wichtigsten Angelegenheiten geregelt. Aber eine Frage wird dabei fast immer vergessen: Was passiert eigentlich mit meinen digitalen Konten, wenn ich nicht mehr da bin?

Die Antwort ist ernüchternd: Die meisten digitalen Konten verschwinden nicht. Sie laufen weiter — auf Kosten der Hinterbliebenen.

Das Problem, über das niemand spricht

Wer heute stirbt, hinterlässt nicht nur ein Bankkonto, eine Wohnung und vielleicht ein Auto. Sondern auch ein E-Mail-Postfach, ein Amazon-Konto, Streaming-Abonnements, Cloud-Speicher voller Fotos, soziale Netzwerke, Online-Banking-Zugänge und dutzende weitere Accounts, die sich über ein ganzes digitales Leben angesammelt haben.

Und anders als beim analogen Nachlass gibt es für den digitalen kein Amtsgericht, das automatisch eine Bestandsaufnahme macht. Niemand weiß, welche Konten existieren. Niemand hat die Zugangsdaten. Und kostenpflichtige Abonnements laufen im schlimmsten Fall monatelang weiter, weil sie per Lastschrift oder Kreditkarte abgebucht werden — von einem Konto, das die Erben nicht sofort überblicken.

Als ich mich vor einiger Zeit selbst mit dem Thema beschäftigt habe — nicht aus traurigem Anlass, sondern schlicht aus Vernunft —, war ich überrascht, wie viele Konten ich hatte, von denen meine Frau nicht einmal wusste.

Was die großen Anbieter anbieten

Die gute Nachricht: Einige der großen Plattformen haben mittlerweile Vorsorge-Funktionen eingebaut. Die schlechte Nachricht: Fast niemand nutzt sie.

- **Google (Kontoinaktivität-Manager):** Google bietet eine der durchdachtesten Lösungen an. Unter myaccount.google.com/inactive können Sie festlegen, was passiert, wenn Ihr Konto über einen bestimmten Zeitraum – drei, sechs, zwölf oder achtzehn Monate – nicht mehr genutzt wird. Sie können Vertrauenspersonen benennen, die dann Zugriff auf ausgewählte Daten erhalten: E-Mails, Fotos, Drive-Dateien, YouTube-Inhalte. Alternativ können Sie festlegen, dass das Konto nach Ablauf der Frist automatisch gelöscht wird. Die Einrichtung dauert keine fünf Minuten.
- **Apple (Nachlasskontakt):** Seit iOS 15.2 und macOS Monterey können Sie in den Einstellungen unter „Apple-ID“ einen oder mehrere Nachlasskontakte hinterlegen. Diese Personen können nach Ihrem Tod mit einem speziellen Zugangscode und Ihrer Sterbeurkunde Zugriff auf Ihre iCloud-Daten beantragen – Fotos, Notizen, E-Mails, Dateien. Die Einrichtung finden Sie unter „Passwort & Sicherheit“ → „Nachlasskontakt“.
- **Facebook und Instagram (Gedenkzustand):** Meta bietet die Möglichkeit, einen Nachlasskontakt zu benennen, der Ihr Profil nach Ihrem Tod in einen Gedenkzustand versetzen kann. Das Profil wird dann mit dem Hinweis „In Erinnerung an“ versehen. Alternativ können Sie verfügen, dass Ihr Konto nach Ihrem Tod gelöscht wird. Die Einstellung finden Sie unter „Einstellungen“ → „Persönliche Informationen“ → „Kontoinhaber und Kontrolle“.
- **Microsoft:** Microsoft hat keinen Kontoinaktivität-Manager. Angehörige müssen sich mit einer Sterbeurkunde an den Support wenden, um Zugriff auf ein Outlook- oder OneDrive-Konto zu erhalten. Der Prozess dauert und ist nicht immer unkompliziert.

Unterschätztes Problem: laufende Abonnements

Viele Menschen unterschätzen, wie viele kostenpflichtige Dienste an ihr Konto gebunden sind. Streaming-Dienste, Cloud-Speicher, App-Abonnements, Zeitschriften-Abos, Fitnesstracker-Premium, Passwort-Manager, VPN-Dienste – die Liste ist oft erstaunlich lang. Und all diese Dienste buchen weiter ab, solange niemand kündigt.

Für Hinterbliebene bedeutet das: Sie müssen nicht nur die Konten finden, sondern auch herausfinden, welche davon Geld kosten. Ohne eine Übersicht ist das wie eine Suche im Nebel. Besonders unangenehm wird es, wenn die Abbuchungen über eine Kreditkarte laufen, die nicht sofort gesperrt wird.

Was Sie jetzt tun können – ganz praktisch

Die gute Nachricht: Vorsorgen ist weder kompliziert noch morbide. Es ist schlicht eine Frage der Organisation — vergleichbar mit dem Ordner, in dem Sie Ihre Versicherungspolicen abheften.

1. Erstellen Sie eine Übersicht Ihrer digitalen Konten. Das muss keine perfekte Tabelle sein. Eine einfache Liste reicht: Welche Dienste nutze ich? Wo bin ich registriert? Welche davon sind kostenpflichtig? Denken Sie dabei auch an Konten, die Sie selten nutzen — das vergessene PayPal-Konto, der alte eBay-Account, die Fotoplattform, auf der noch Urlaubsbilder liegen.

2. Regeln Sie den Zugang zu Ihren Passwörtern. Der sicherste Weg ist ein Passwort-Manager wie Bitwarden oder KeePassXC, dessen Master-Passwort an einem sicheren Ort hinterlegt ist — zum Beispiel in einem versiegelten Umschlag im Bankschließfach oder beim Notar. Alternativ gibt es spezielle Notfallblätter, die manche Passwort-Manager anbieten: ein ausgedrucktes Blatt mit dem Master-Passwort und einer kurzen Anleitung, wie man den Tresor öffnet.

3. Nutzen Sie die Vorsorge-Funktionen der großen Anbieter. Richten Sie Googles Kontoinaktivität-Manager ein. Hinterlegen Sie bei Apple einen Nachlasskontakt. Bestimmen Sie bei Facebook, was mit Ihrem Profil passieren soll. Das sind jeweils wenige Minuten Aufwand, die Ihren Angehörigen Stunden oder Tage ersparen können.

4. Halten Sie eine Vertrauensperson informiert. Ihre Partnerin, Ihr Partner, ein erwachsenes Kind oder ein enger Vertrauter sollte wissen, dass eine solche Liste existiert und wo sie zu finden ist. Die Liste selbst muss nicht offen herumliegen — aber jemand muss wissen, dass es sie gibt.

5. Nehmen Sie den digitalen Nachlass in Ihre Vorsorgevollmacht auf. Wer bereits eine Vorsorgevollmacht hat, sollte prüfen, ob sie auch digitale Konten abdeckt. Ein einfacher Zusatz wie „Die bevollmächtigte Person ist berechtigt, auf meine digitalen Konten und Online-Dienste zuzugreifen, diese zu verwalten und gegebenenfalls zu kündigen oder zu löschen“ kann im Ernstfall viel bewirken. Ohne eine solche Regelung haben Angehörige bei vielen Anbietern keinen rechtlichen Anspruch auf Zugang — selbst mit Erbschein.

Was das Gesetz sagt

Der Bundesgerichtshof hat 2018 in einem viel beachteten Urteil entschieden, dass digitale Inhalte grundsätzlich vererbbar sind — konkret ging es um den Facebook-Account einer Verstorbenen. Erben treten in den Nutzungsvertrag ein, so wie sie auch in einen Mietvertrag eintreten würden.

In der Praxis sieht es allerdings oft anders aus. Viele Anbieter sitzen im Ausland und kennen deutsche Erbrechtsurteile nicht oder ignorieren sie. Wer nur mit einem Erbschein beim Support anklopft, erlebt nicht selten wochenlange Wartezeiten. Eine Vorsorgevollmacht, die digitale Konten ausdrücklich erwähnt, ist der deutlich schnellere Weg.

Vorsorge, nicht Angst

Ich weiß: Über den eigenen Tod nachzudenken gehört nicht zu den angenehmsten Nachmittagsbeschäftigungen. Aber genau darum geht es hier ja nicht. Es geht darum, Ordnung zu schaffen – so wie man einen Ordner mit Versicherungsunterlagen führt oder einmal im Jahr die Kontoauszüge sortiert. Nicht weil man das Schlimmste erwartet, sondern weil man es den Menschen, die einem wichtig sind, nicht unnötig schwer machen möchte.

Meine eigene Liste hat übrigens keine Stunde gedauert. Das Schwierigste war, sich hinzusetzen und anzufangen.

Checkliste: Digitaler Nachlass in fünf Schritten

- **Liste erstellen:** Alle digitalen Konten und Abonnements aufschreiben – auch die vergessenen.
- **Passwörter sichern:** Passwort-Manager einrichten, Master-Passwort sicher hinterlegen.
- **Anbieter-Funktionen nutzen:** Google Kontoinaktivität-Manager, Apple Nachlasskontakt, Facebook Gedenkzustand.
- **Vertrauensperson informieren:** Jemand muss wissen, dass die Liste existiert und wo sie liegt.
- **Vorsorgevollmacht ergänzen:** Digitale Konten ausdrücklich aufnehmen.