macOS – Versteckte Schätze

Mehrere Objekte im Finder umbenennen

von SHARON ZARDETTO, tidbits.com
Übersetzung: Kurt J. Meyer und DeepL.com

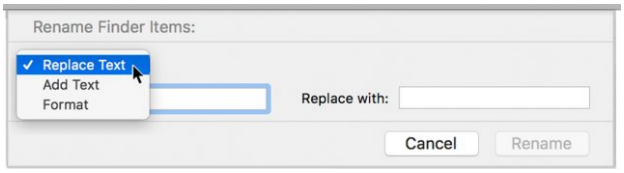
Als ich Inline-Grafiken - kleine Bilder, die in eine Textzeile eingebettet sind - für mein Buch Take Control of Numbers vorbereitete, war ich fast fertig, als ich mich auf einmal daran erinnerte, dass die Dateinamen eine Namenskonvention einhalten mussten: Sie mussten mit `_inline` enden. An die 50 Dateien mussten umbenannt werden. Einem kurzen Moment des Schreckens folgte die erleichterte Erkenntnis, dass der Finder mit seiner Batch-Rename-Fähigkeit dies für mich tun konnte.

Sie wussten gar nicht, dass der Finder eine Batch-Umbenennungsfunktion hat? Das liegt daran, dass die Option als scheinbar nutzloser **Umbenennen**-Befehl im Menü Datei getarnt ist. Schließlich kann man eine Datei einfach durch Klicken und Tippen umbenennen. Der Befehl Umbenennen hat also keinen Grund zur Existenz - bis Sie mehrere Elemente ausgewählt haben. Dann ändert er sich in **Umbenennen [X] Elemente** (Das X steht für die Anzahl der gewählten Elemente). Aber woher wissen Sie das, da Sie wahrscheinlich keine Menüs durchsuchen, nachdem Sie eine Reihe von Dateien oder Ordnern ausgewählt haben?

Und so fängt man an: Wählen Sie mehrere Elemente in einer beliebigen Fensteransicht (einschließlich, falls erforderlich, einer Mischung aus Dateien und Ordnern) und wählen Sie **Datei > Umbenennen [X] Elemente.** (Für den Rest dieses Artikels beziehe ich mich auf diesen Befehl einfach als „Umbenennen von Elementen".

Batch-Umbenennungs-Optionen

Wenn Sie für eine Auswahl *Elemente umbenennen* wählen, erscheint ein Dialog. (Wenn Sie in einem Fenster arbeiten, rutscht er aus der Titelleiste; wenn Sie Elemente auf dem Desktop ausgewählt haben, erhalten Sie eine frei schwebende Version.



Das Popup-Menü bietet drei Möglichkeiten:

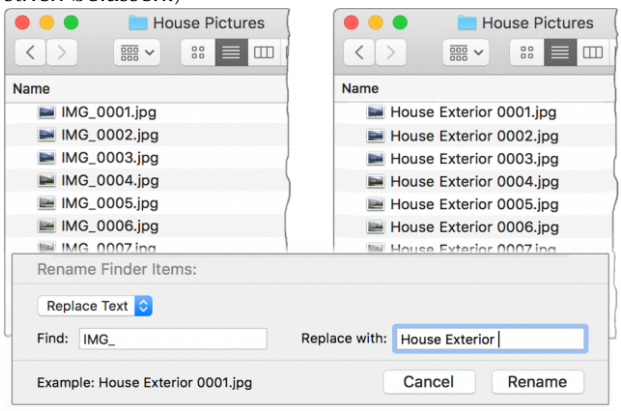
- Text ersetzen: Ändern Sie einen beliebigen Teil des vorhandenen Dateinamens in einen anderen Text. Mit dieser Option können Sie auch Zeichen aus Dateinamen löschen, indem Sie den vorhandenen Text durch nichts ersetzen.
- Text hinzufügen: Fügen Sie Text vor oder nach dem Dateinamen hinzu.
- Formatieren: Fügen Sie eine Index- oder Zählernummer (letztere verwendet führende Nullen für eine feste Anzahl von Ziffern) oder das aktuelle Datum und die aktuelle Uhrzeit an den Dateinamen an. Sie können die Nummer vor oder nach dem Dateinamen platzieren, den Dateinamen durch einen anderen Text ersetzen oder den ursprünglichen Namen komplett löschen.

Wir schauen uns nun die drei Optionen in Aktion an.

Dateinamentext ersetzen oder löschen

Wie viele Dateien haben Sie, deren Namen mit `IMG_` beginnen? Jedes Mal, wenn Sie Bilder von Ihrer Kamera auf Ihren Mac übertragen, werden sie mit diesem Präfix benannt, gefolgt von einer 4-stelligen Nummer. Ersetzen Sie diese führenden Zeichen durch einen Deskriptor, damit Sie wissen, was los ist:

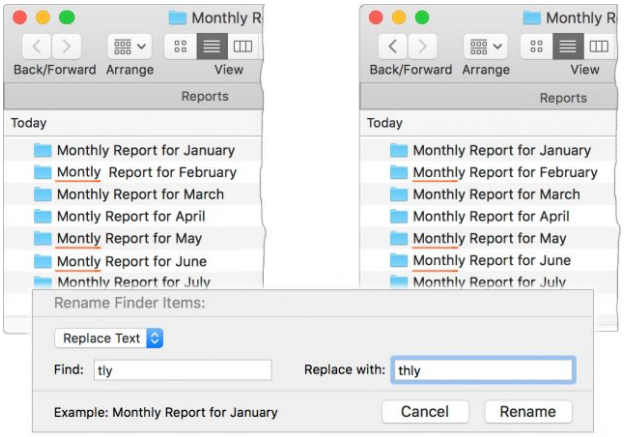
1. Wählen Sie im Finder-Fenster mit den Fotodateien **Bearbeiten > Alles auswählen** und dann **Datei > Elemente umbenennen**.
2. Wählen Sie Text ersetzen aus dem Popup-Menü des Dialogs.
3. Geben Sie im Feld *Suchen* `IMG_` ein.
4. Geben Sie für *Ersetzen durch* eine Beschreibung ein: `Pool Party`, `Abschluss`, `Disney World`. Stellen Sie sicher, dass hinter dem Text ein Leerzeichen oder ein anderes Trennzeichen steht. (Alternativ können Sie auch nur `IMG` ersetzen und den Unterstrich belassen.)



5. Wenn das Beispiel unten links im Dialogfeld korrekt aussieht, klicken Sie auf Umbenennen.

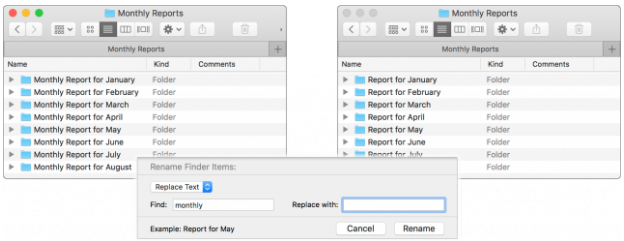
Haben Sie schon mal mit einem Reihe von `montly` Reports geendet, die unter Ihren `monthly`- Reports oder ähnlichen, sich wiederholenden Schreibfehlern verstreut waren? Um den Typo `montly` durch `monthly` (monatlich) zu ersetzen:

1. Markieren Sie die Zieldateien und wählen Sie **Datei > Elemente umbenennen**.
2. Wählen Sie **Text ersetzen** aus dem Popup-Menü.
3. Geben Sie im Feld *Suchen* `montly`, im Feld *Ersetzen durch* `monthly` ein. Oder verwenden Sie eine kürzere Textersetzung, wie z.B. das Ersetzen von `tly` durch `thly`, solange es keinen anderen Text in den Dateinamen stören würde.



Sie könnten versucht sein, den noch kürzeren Wechsel von `ly` zu `hly` zu verwenden; mit diesem Ansatz würden einige der Dateien jedoch, wenn sie von Anfang an richtig benannt wären, mit einem zusätzlichen `h-monthly` Ergebnis enden. Ich empfehle, ganze Wörter zu verwenden, um Probleme zu vermeiden, die Sie vielleicht nicht bemerken, solange sie noch leicht rückgängig zu machen sind - obwohl ich gestehe, dass dies ein Fall von *„Tu, was ich sage, aber nicht, wie ich es mache“* ist. Wenn es zu spät ist, den Fehler rückgängig zu machen, ist es in der Regel ein Kinderspiel, eine zweite, vorsichtigere Umbenennung vorzunehmen, um das Problem zu beheben. (Undo-Details sind in der „Schnelle Tipps“-Liste am Ende dieses Artikels aufgeführt.)

Sie können auch die Option *Text ersetzen* verwenden, um Text aus einem Dateinamen zu löschen: Geben Sie einfach das Löschziel in Suchen ein und lassen Sie Ersetzen durch leer. Wenn Sie also entschieden haben, dass `Monthly Report for January` und die nachfolgenden Monate etwas überflüssig sind, setzen Sie „Suchen“ auf `Monthly ` und stellen Sie sicher, dass das Leerzeichen am Ende enthalten ist - und lassen Sie das Feld *Ersetzen durch* einfach leer.



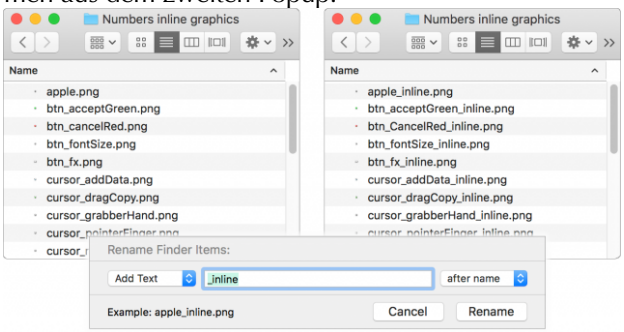
Ein weiteres Beispiel für das Löschen von Dateinamen-Texten finden Sie unter „Umbenennen mit mehreren Durchgängen“.

Text zu Dateinamen hinzufügen

Mit der Option *Text hinzufügen* im Dialogfeld **Umbenennen** können Sie Text an den Anfang oder das Ende des Dateinamens hinzufügen: Wählen Sie *Text hinzufügen* aus dem Menü, geben Sie den zusätzlichen Text ein und geben Sie an, ob er vor oder nach dem Namen steht.

Das ist, was ich gewöhnlich tue, um `_inline` zu meinen Grafiken hinzuzufügen — die Aufgabe, die ich am Anfang dieses Artikels erwähnte. Möglicherweise müssen Sie einen Projektnamen zu einer Gruppe von Dateien hinzufügen, oder Sie haben vergessen, Ihre Initialen an Revisionen von freigegebenen Dokumenten anzuhängen. Und so nimmt man eine einfache Einstellung wie diese vor:

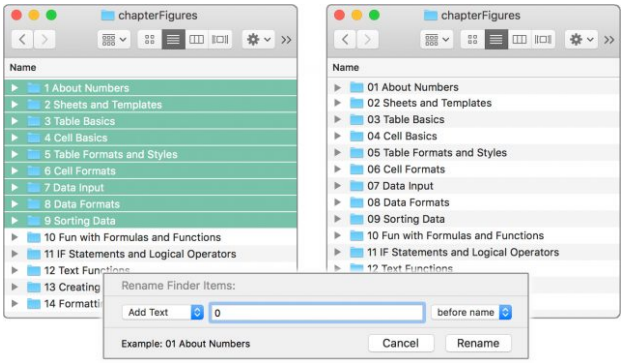
1. Wählen Sie die Zieldateien aus.
2. Wählen Sie **Datei > Elemente umbenennen**.
3. Wählen Sie im Dialogfeld **Text hinzufügen** aus dem Popup-Menü, geben Sie den Text ein und wählen Sie Vor dem Namen oder Nach dem Namen aus dem zweiten Popup.

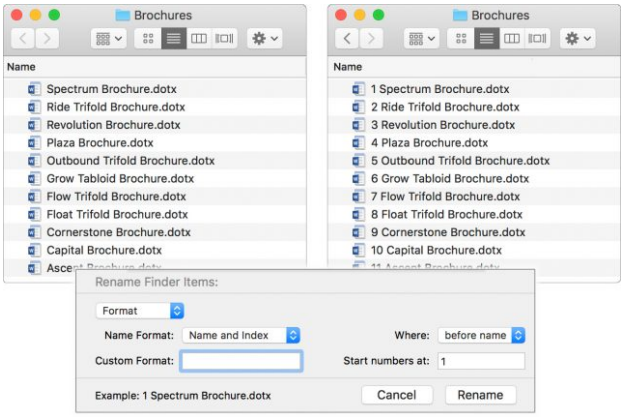


4. Klicken Sie auf **Umbenennen**.

Wie Sie im obigen Screenshot sehen können, ignoriert ein *„Nach dem Namen“*-Zusatz die Dateierweiterung (.png), da sie nicht als Teil des Dateinamens betrachtet wird.

Ich verwende diese Methode häufig, um führende Nullen an den Anfang von einstelligen Zahlen anzuhängen, damit ich den Text in einer Liste von nummerierten Dateinamen leichter scannen kann. Wenn nur die einstelligen Dateien ausgewählt sind, setze ich die Option Umbenennen auf Text hinzufügen, gebe eine Null in das Textfeld ein und wähle *Vor dem Namen* aus dem zweiten Menü.



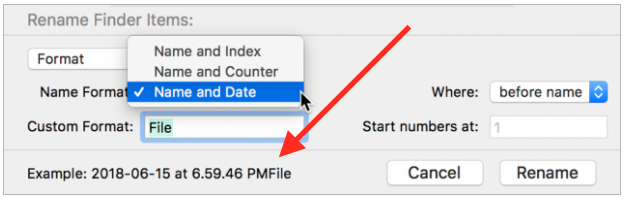


Dateinamen mit Zahlen oder Datumsangaben formatieren

Die Menüauswahl Format im Umbenennen-Dialog ist kein leuchtendes Beispiel für die Nomenklatur, weder für ihren Titel noch für ihren Inhalt. Die Formatierungsoptionen sind:

- Name und Index: Fügt fortlaufende Nummern hinzu, beginnend bei 1 oder einer von Ihnen angegebenen Nummer.
- Name und Zähler: Fügt fortlaufende Nummern hinzu, die ebenfalls bei 1 oder einer bestimmten Zahl beginnen, erzeugt aber bei Bedarf fünfstellige Nummern durch Auffüllen mit führenden Nullen: 00001 und 00237, zum Beispiel.
- Name und Datum: Fügt das aktuelle Datum sowie die Uhrzeit sekundengenau im Format 2018-05-23 um 9.27.55 Uhr hinzu.

Mit jeder dieser Optionen können Sie den ursprünglichen Dateinamen beibehalten oder ersetzen, indem Sie das umständlich benannte Feld *Benutzerdefiniertes Format* verwenden. Seltsamerweise beginnt es normalerweise mit *Datei* als Standardvorschlag (ohne den Komfort eines führenden Leerzeichens, wie Sie in der Beispielzeile des Dialogs in diesem Bild sehen können).



Um die aktuellen Dateinamen durch einen gemeinsamen Namen zu ersetzen — z.B. nur durch eine Index- oder Zählernummer (`Field Test 1`, `Field Test 2`) - geben Sie diesen Namen in das Feld *Benutzerdefiniertes Format* ein. Wenn der ursprüngliche Name erhalten bleiben soll, muss das Feld *Benutzerdefiniertes Format* leer sein, wie im folgenden Bild gezeigt.

Es ist nicht sofort ersichtlich, wie eine der beiden Nummerierungsoptionen auf ausgewählte Dateien angewendet wird. Hier ist der Trick: Wenn Sie in einer Listenansicht arbeiten, die wie fast immer die Namen in der ersten Spalte hat, werden die Nummern der Reihe nach auf diese Namen angewendet. Kein Wunder, aber der steuernde Faktor ist eigentlich die Sortierreihenfolge des Fensters - z.B. *Erstellt* oder *Größe* -, die sich natürlich auf die Reihenfolge der Namen auswirkt. Stellen Sie also sicher, dass Ihre Dateien in der richtigen Reihenfolge vorliegen, bevor Sie sie umbenennen.

Umbenennen mit mehreren Durchgängen

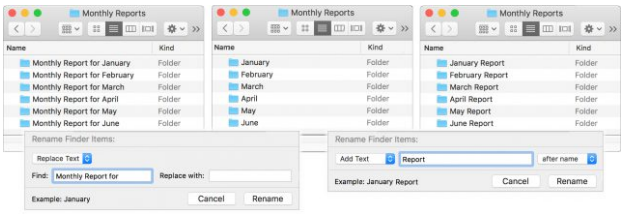
Manchmal erfordert das Umbenennen mehr als einen Durchgang: das Ändern des Namens, dann das Hinzufügen eines Datums und schließlich das Löschen des Zeitstempels, der das Datum begleitet. Aber die Bearbeitung ist einfach einzurichten und dauert nur wenige Sekunden, so dass mehrere Durchläufe nicht sehr zeitaufwändig sind.

Dateinamen umbenennen

Wenn Dateien `Monatsbericht für [Monat]` heißen und Sie sie lieber als `[Monat] Bericht` bezeichnen wollen, jagen Sie sie zweimal durch die Umbenennungs-Mühle, indem Sie zuerst das `Monatsbericht für` löschen und dann das Wort `Bericht` an das Ende der Dateinamen hinzufügen:

1. Markieren Sie die Zieldateien und wählen Sie **Datei > Elemente umbenennen**.
2. Wählen Sie Text ersetzen aus dem Popup-Menü und geben Sie `Monatsbericht für` (einschließlich eines Leerzeichens) im Feld Suchen ein. Lassen Sie *Ersetzen durch* leer, und klicken Sie auf *Umbenennen*. Die Dateien sind jetzt nur noch mit dem Monat benannt.
3. Wenn die Dateien noch ausgewählt sind, wählen Sie erneut **Datei > Elemente umbenennen**. Wählen Sie *Text hinzufügen* aus dem Popup-Menü und geben Sie `Bericht` in das Textfeld ein; wählen Sie

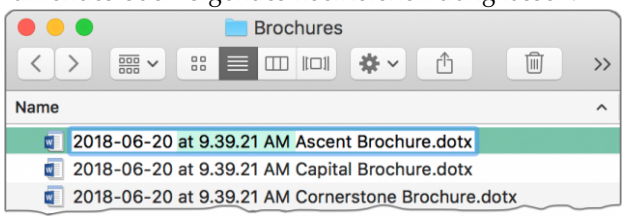
Nach dem Namen aus dem zweiten Popup-Menü und klicken Sie auf **Umbenennen**.



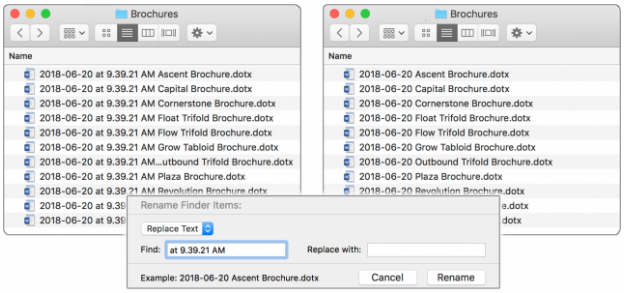
Das Entfernen der Zeit aus Datum & Zeit

Ich bin der festen Überzeugung, dass die Anwendung eines Datumsstempels von einem Zeitstempel getrennt sein sollte, aber Apple hat es leider versäumt, mich in dieser Angelegenheit zu konsultieren. Zum Glück ist es recht leicht, die Zeitangabe zu löschen:

1. Holen Sie sich den genauen Wortlaut des Zeitstempelteils der umbenannten Dateien, indem Sie ihn aus einem der Dateinamen kopieren: Wählen Sie eine der Dateien aus, aktivieren Sie ihren Namen durch Anklicken oder Drücken der Eingabetaste, und ziehen Sie den Cursor über den Zeitstempelteil einschließlich des `at`, wobei Sie ein führendes oder folgendes Leerzeichen übrig lassen.



2. Markieren Sie alle Zieldateien und wählen Sie **Datei > Elemente umbenennen**.
3. Wählen Sie **Text ersetzen** aus dem Popup-Menü.
4. Fügen Sie den kopierten Zeitstempel in das Feld *Suchen* ein und lassen Sie das Feld *Ersetzen durch* leer.
5. Klicken Sie auf **Umbenennen**.



Schnelle Tipps

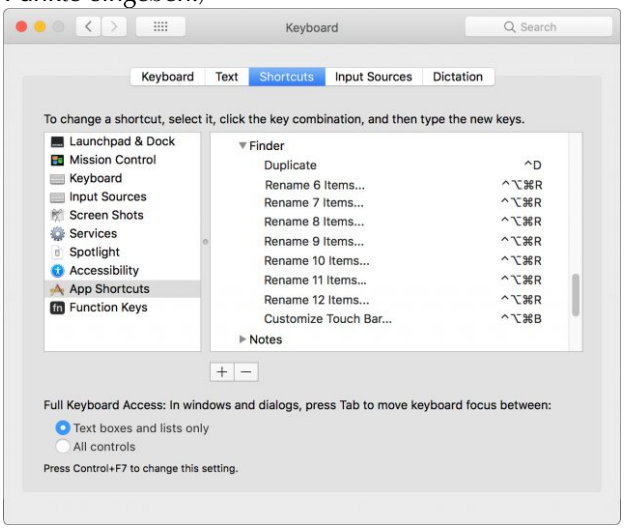
Hier sind noch ein paar Dinge, die Sie wissen sollten:

- Schneller Zugriff auf den Befehl Umbenennen: Sind Sie es leid, in das Menü Datei für den Befehl Elemente umbenennen zu gelangen? Ich habe drei Lösungen für Sie. Rechts-klicken Sie auf eine der ausgewählten Dateien für ein **Kontextmenü**, das den Befehl **Umbenennen** enthält, verwenden Sie das **Aktionsmenü** (das Zahnradsymbol) in der Symbolleiste des Fensters, oder … die dritte erhält ihren eigenen Tipp als nächstes.
- Tastaturkürzel für den Befehl **Umbenennen**: Wenn Sie den Befehl *Umbenennen* häufig verwenden und die Art der Person sind, die Tastaturbefehle bevorzugt, dann werden Sie enttäuscht sein, wenn Sie feststellen, dass Sie keine Tastenkombination für einen Befehl einrichten können, dessen Wortlaut sich ständig ändert (4 Elemente umbenennen, 12 Elemente umbenennen....). Außer, dass Sie - in einer Art Kreisverkehr - Verknüpfungen für viele verschiedene Versionen des Befehls einrichten und allen die gleiche Verknüpfung zuweisen können. (Wer hätte das gedacht? Ich dachte es nicht, bis ich mich entschied, es auszuprobieren, weil ich Tastaturkürzel für fast alles bevorzuge. Die Methode unterscheidet sich nicht von der Einrichtung anderer Tastaturkürzel:

  1 Gehen Sie zu **Systemeinstellungen > Tastatur > Shortcuts** und klicken Sie auf **App-Kurzbefehle** in der Kurzbefehle-Liste.

  2 Klicken Sie auf die Schaltfläche **+** unterhalb der Verknüpfungsliste und wählen Sie Finder aus dem Popup-Menü im Dialogfeld. (Wenn der Finder noch nicht in der Verknüpfungsliste enthalten ist, wird er durch diese Prozedur hinzugefügt; wenn er bereits aufgelistet ist, müssen Sie ihn noch als Ziel auswählen.

  3 Geben Sie im Feld Menütitel den Text Umbenennen 6 Elemente … ein. (Sie müssen nicht das Ellipsenzeichen verwenden, das mit Option-Semikolon eingegeben wurde - Sie können einfach drei Punkte eingeben.)



  4 Gehen Sie zum Feld Tastaturkürzel und drücken Sie die gewünschte Tastenkombination.

  5 Wiederholen Sie diesen Vorgang für andere

Anzahlen von Dateien im Befehlsnamen mit der gleichen Tastenkombination.

- Ich habe festgestellt, dass Systemeinstellungen gelegentlich die Verwendung derselben Verknüpfung für mehrere Befehle ablehnen, aber das nur milde: manchmal werden nicht alle Befehle in ihrem Fenster korrekt aufgelistet, wobei nur eine Ellipse (…) anstelle des Befehlsnamens angezeigt wird. Aber die Tastenkombinationen bleiben angezeigt, die Befehlsnamen kehren bei einem späteren Öffnen der Systemeinstellungen zurück, und alle Tastenkombinationen funktionieren in der Zwischenzeit, so dass dies nur ein kleiner Fehler ist.
- Großschreibungs-Unempfindlichkeit: Im Dialogfeld *Umbenennen* wird der zu ersetzende oder zu löschende Text unabhängig von Groß- und Kleinbuchstaben eingegeben. Aber jeder Ersatztext wird genau so verwendet, wie Sie ihn eingeben.
- Einen Umbenennungsfehler rückgängig machen: Ob Sie versehentlich einen Tippfehler beim Umbenennen von Dateien eingeführt haben, die falsche Option gewählt haben (z.B. Zähler statt Seriennummern) oder feststellen, dass die Umbenennung einfach nicht das ist, was Sie wollen, können Sie den Befehl **Bearbeiten > Rückgängig machen** verwenden, um die Änderungen rückgängig zu machen. Wenn Sie Ihre Meinung ändern, gibt es **Bearbeiten > Wiederholen** zur Rettung. Sie können sogar mehrere Undo-Level durchlaufen: Wenn Sie eine Seriennummer am Anfang der Datei und dann einen korrigierten Projektnamen am Ende hinzugefügt haben, können Sie jede einzelne rückgängig machen, um zu den ursprünglichen Dateinamen zurückzukehren. Selbst wenn Sie das Fenster geschlossen und andere geöffnet haben, können Sie zum Ordner der umbenannten Dateien zurückkehren und die Änderungen rückgängig machen. Es gibt natürlich einige Einschränkungen wie z.B., wenn man anderswo im Finder gar nichts Widerrufbares gemacht hat.

Ein A-Z-Leitfaden zu Cyber-Sicherheitsbedrohungen und wie man mit ihnen umgeht

Quelle: intheblack.com, Übersetzung KJM und DeepL.com

Cyber-Attacken haben einen langen Weg zurückgelegt, seit Sie über Ihr Hotmail-Konto eine zufällige Nachricht von einem nigerianischen Prinzen erhielten, der Ihnen eine Million Dollar leihen wollte. Nach Vorfällen wie dem jüngsten Cambridge Analytica-Facebook-Skandal und dem Ausbruch von WannaCry im vergangenen Jahr ist die weltweite Sorge um Privatsphäre und Cybersicherheit auf einem historischen Höchststand.

So sollte es auch sein, denn es steht viel auf dem Spiel. Cyber-Attacken, bei denen Kundendaten oder kritische Geschäftsdaten verloren gehen, dürften australische Unternehmen mit 100 bis 500 Mitarbeitern durchschnittlich rund 1,9 Millionen AUD kosten, so die Studie des Sicherheitsunternehmens Webroot.

Dieser A-Z-Leitfaden zu Cyber-Bedrohungen hilft Ihnen, alles zu verstehen und sich gegen alles zu wappnen, von Android-Malware bis hin zu Zero-Day-Exploits (Angriffe, die eine bislang unbekannte Sicherheitslücke ausnutzen).

Schwachstelle, Exploit oder Malware?

Nein, sie sind nicht alle gleich. Bevor wir auf spezifische Bedrohungen eingehen, beschreiben Schlüsselbegriffe die verschiedenen Arten von Cyber-Bedrohungen.

Schwachstelle ist ein Hardware- oder Softwarefehler, der Systeme für potenzielle Angriffe oder Verletzungen offen lässt. Ein **Exploit** ist der Akt, diese Schwachstelle auszunutzen, um ein System oder Netzwerk in einer bestimmten Weise anzugreifen oder zu durchbrechen.

Eine Möglichkeit, dies zu tun, ist die Entwicklung von **Malware** - ein Sammelbegriff für bösartige Software, einschließlich Computerviren, Würmer, Trojanische Pferde, Spyware und andere bösartige Software.

A

Erweiterte persistente Bedrohung (APT)

Ein APT ist eine Reihe von Angriffen, die sich gegen eine bestimmte Organisation richten, die über hochwertige Daten verfügt, wie zum Beispiel eine Behörde, eine Bank oder einen Hersteller. Die Hacker sind in der Regel hoch qualifiziert und sehr hartnäckig in ihren Versuchen, ungehinderten Zugang zum Netzwerk der Organisation zu erhalten.

Ihr Ziel ist es, lange Zeit unentdeckt zu bleiben, damit sie möglichst viele Daten aus verschiedenen Gründen, wie z.B. Wirtschaftsspionage, stehlen können.

Android-Malware

Je beliebter ein Betriebssystem wird, desto anfälliger wird es für Malware, und das ist bei Android sicherlich der Fall. Mittlerweile gibt es weltweit mehr als 2,5 Milliarden Android-Geräte und 20 Millionen Malware-Bedrohungen, so der Sicherheitsforscher AV-test.org.

Google selbst gab zu, dass es im Jahr 2017 mehr als 700.000 "schlechte" Apps aus seinem Google Play Store entfernt hat.

B

BlueBorne Bluetooth Schwachstellen

Der Sicherheitsanbieter Armis Labs identifizierte eine Reihe von Bluetooth-Schwachstellen, die zusammen als BlueBorne bekannt sind und sich auf mehr als 8,2 Milliarden Computer und Geräte mit Android, iOS, Windows und Linux auswirken könnten — einschließlich der intelligenten Lautsprecher von Amazon und Google.

Es gibt keine bekannten Fälle von Hackern, die die BlueBorne-Schwachstellen ausnutzen, aber sie könnte es Hackern ermöglichen, die Kontrolle über jedes anfällige Gerät zu übernehmen oder Malware zu verbreiten, wenn Bluetooth eingeschaltet ist.

Botnetz

Ein Botnet ist eine (typischerweise) große Anzahl von kompromittierten verbundenen Geräten, die von Bots übernommen werden, die Geräte dazu bringen sollen, an bestimmten DDoS (Distributed Denial of Service), Spam und anderen Angriffen teilzunehmen.

Brute-Force-Angriff

Dies ist eine Versuchs-und-Fehler-Methode zur Gewinnung von Informationen, wie z. B. ein Passwort. Hacker verwenden in der Regel Software, um den Prozess zu automatisieren und stark zu beschleunigen.

C

Krypto-Währungshacker

Krypto-Währungen wie z.B. Bitcoin hängen von Bitcoin-Minenarbeitern ab, die ihre eigenen Systeme verwenden, um bei der Verarbeitung von Transaktionen zu helfen. Die Vergrößerung eines Bergbaubetriebes erfordert jedoch Investitionen in Computer und kann viel Strom verbrauchen. Stattdessen können Hacker die Computer anderer Leute entführen, um sie in die Mine zu stecken.

Diese Systeme sind in der Regel über Drive-by-Code infiziert (siehe nebenstehend), und ein Tool namens Coinhive (mehrere Sicherheitsfirmen haben dies kürzlich als die größte bösartige Bedrohung für Web-Benutzer identifiziert), hat dies einfach zu implementieren gemacht. Laut Malwarebytes waren die Australier allein im Oktober 2017 von mehr als 12 Millionen Vorfällen auf Coinhive-Basis betroffen.

Crime-as-a-Service

Als ob es nicht genug Hacker gäbe, können jetzt auch nicht-technische Kriminelle Lösegeld, DDoS (Distributed Denial of Service), Hacking und andere Tools kaufen, um Online- und Offline-Kriminalität zu begehen, so die Internet Organised Crime Threat Assessment 2017 von Europol. Zusammenfassend werden diese Instrumente als Crime-as-a-Service bezeichnet.

D

DDoS-Angriffe

Ein DDoS ist ein gezielter Angriff, der darauf abzielt, ein Computernetzwerk oder Server zu zerstören, indem er sie mit Daten überflutet, die gleichzeitig von vielen einzelnen Geräten gesendet werden. Der Sicherheitsanbieter Kaspersky hat einen DDoS-Angriff identifiziert, der mehr als 320 Stunden dauerte.

Typische DDoS-Ziele sind Regierungen, Medien und andere hochkarätige Websites. Doch in einem Fall im Jahr 2016 soll ein junger Hacker seine Website so konfiguriert haben, dass er automatisch 911 Anrufe tätigt und die Rettungsdienste in drei US-Bundesstaaten mit gefälschten Anrufen überschwemmt.

Drive-by-Downloads

Immer häufiger werden Systeme über Drive-by-Code auf Webseiten infiziert, die absichtlich oder durch Dritte kompromittiert werden. Dies kann auf verschiedene Weise geschehen, z. B. durch Cross-Site-Scripting (XSS)-Schwachstellen oder durch JavaScript- oder SQL-Code-Injektionen.

Wie auch immer, das Ziel ist in der Regel, Malware ohne ihr Wissen auf die Systeme der Website-Besucher herunterzuladen.

E

E-Mail-Bedrohungen

E-Mail ist nach wie vor eine der beliebtesten Methoden zur Verbreitung von Malware. Über 2016-17 zeigten Berichte an das Cybercrime Online Reporting Network der australischen Bundesregierung Verluste von mehr als 20 Mio. AUD aufgrund von E-Mail-Kompromissen bei Unternehmen - eine Steigerung von 230 Prozent gegenüber dem Vorjahr.

Phishing - gefälschte E-Mails, die angeblich von seriösen Unternehmen stammen und dazu bestimmt sind, Informationen wie Passwörter und Kreditkartennummern zu erhalten - ist immer noch weit verbreitet. Der Sicherheitsanbieter MailGuard berichtet regelmäßig über Phishing-E-Mails, die sich als vertrauenswürdige Marken ausgeben, darunter ATO, ASIC, Telstra, EnergyAustralia, Xero, Commonwealth Bank, Netflix, Amazon und viele mehr.

H

Hacktivismus

Nicht alle Hacker sind finanziell motivierte Kriminelle. Aktivisten, die politische oder gesellschaftliche Veränderungen anstreben, wenden sich ebenfalls Hacking-Techniken zu. Die vielleicht bekannteste hacktivistische Gruppe ist Anonymous, die die Verantwortung für viele hochkarätige DDoS-Angriffe übernommen hat, darunter einen auf die Scientology-Kirche.

I

Internet der Dinge Schwachstellen

Das Internet der Dinge (IoT) verändert die Abläufe in Produktionsstätten, Bauernhöfen, Bergwerken und sogar ganzen Städten, aber es hat eine Achillesferse - die Sicherheit der angeschlossenen Geräte und Sensoren, die für die Bereitstellung der für IoT-Anwendungen erforderlichen Daten so wichtig sind.

Diese kostengünstigen Geräte und Sensoren sind oft ungesichert und daher für eine Reihe von Bedrohungen offen. Eine davon ist Mirai-Malware, die Millionen von IoT- und anderen angeschlossenen Geräten infiziert und in Botnets verwandelt hat. Ein solches Botnet war für einen massiven DDoS-Angriff verantwortlich, der 2016 das Internet für den größten Teil der US-Ostküste zum Erliegen brachte.

K

Keylogger

Keylogger zeichnen jeden Tastendruck auf den Systemen auf, auf denen sie installiert sind. Sie wurden von Überwachungsorganisationen verwendet, sind aber auch eine Art von Malware, die Informationen wie Passwörter und Kreditkartendaten an Cyberkriminelle zurückschickt.

KRACK Wi-Fi-Schwachstelle

Von einem Sicherheitsforscher im Jahr 2017 entdeckt, ist KRACK (kurz für Key Reinstallation Attack) eine Wi-Fi-Schwachstelle, die das Potenzial hat, Millionen von Systemen und Geräten zu beeinträchtigen. Der Fehler liegt im WPA2-Verschlüsselungsprotokoll, das Daten in drahtlosen Netzwerken schützt.

Im Allgemeinen sind Wi-Fi-Netze - und insbesondere öffentliche Netze - als hohe Sicherheitsrisiken bekannt.

M

Mac-Malware

Verlassen Sie sich nicht darauf, dass „Macs keine Viren bekommen". Der Sicherheitsanbieter Malwarebytes meldete sogar einen Anstieg der Mac-Malware um 270 Prozent im Jahr 2017. Zwar wird die tatsächliche Zahl noch immer durch die Menge der Windows-Viren in den Schatten gestellt, aber Selbstgefälligkeit kann und wird zu Lösegeld und anderen Malware-Infektionen auf Macintosh-Geräten führen.

Malvertising

So wie kompromittierte Webseiten Drive-by-Downloads ausliefern können, haben sich Web-Anzeigen als Quelle für versteckte Malware erwiesen. Es ist besonders unangenehm, weil viele legitime Websites Werbung von Drittanbietern enthalten.

Meltdown und Spectre

Meltdown und Spectre sind die bekannt gewordenen und schwerwiegenden Fehler im Prozessordesign, die es Schurkenprogrammen ermöglichen könnten, auf Daten zuzugreifen, die gesichert werden sollten. Meltdown betrifft alle Intel x86 und einige ARM-Prozessoren, während Spectre Intel, AMD und ARM-Chips betrifft. Es bedeutet, dass praktisch alle modernen Computer und viele andere Geräte gefährdet sind.

P

Potentiell unerwünschte Programme (PUPs)

Zu den PUPs gehören Spyware, Adware, Browser-Symbolleisten und andere lästige Programme, die absichtlich installiert wurden, wie z. B. Huckepack bei der Installation einer anderen Anwendung. Sie sind vielleicht nicht so gefährlich wie Malware, aber sie können sehr ärgerlich und schwer zu beseitigen sein.

R

Ransomware

Ransomware wurde 2017 nach einer Reihe von weltweiten Ausbrüchen, darunter *WannaCry* und *Petya*, zum Staatsfeind Nummer eins. Was könnte schlimmer sein als Malware, die alle Ihre Dateien verschlüsselt und Sie dazu auffordert, ein Lösegeld für den Entschlüsselungsschlüssel zu zahlen?

Laut einem globalen Bericht des Softwareunternehmens Symantec aus dem Jahr 2018 kostete WannaCry Unternehmen im asiatisch-pazifischen Raum in den drei Monaten nach seiner Veröffentlichung 300 Millionen US-Dollar.

Rootkit

Ein Rootkit ist eine bösartige Software, die dazu bestimmt ist, privilegierten (und oft auch Administrator-basierten) Zugriff auf einen Computer oder ein Betriebssystem zu erhalten, während ihre Anwesenheit versteckt wird.

Sony BMG wurde 2005 beschuldigt, im Rahmen seiner CD-Kopierschutzmaßnahmen ein Rootkit verwendet zu haben, doch seitdem sind Rootkits im Allgemeinen Malware.

S

Smart Home Schwachstellen

Ähnlich wie geschäftsorientierte IoT-Geräte sind auch viele Smart Home-Geräte offen für Angriffe. Bestimmte Sicherheitskameras, Fernseher und sogar angeschlossenes Kinderspielzeug wurden von Sicherheitsforschern als verwundbar eingestuft.

Soziale Medien

Wir haben den Facebook-Cambridge Analytica-Skandal in der Juni-Ausgabe 2018 von INTHEBLACK untersucht. Doch schon vorher gab es Sicherheitsprobleme mit Social Media. Beispielsweise identifizierte der Sicherheitsanbieter Check Point im Jahr 2016 Bilder auf Facebook, LinkedIn und anderen Diensten, die bösartige Downloads auslösten.

Spam

Die Zahlen sind sehr unterschiedlich, aber bestenfalls rund 39 Prozent aller E-Mails weltweit sind unerwünschte Nachrichten, so das Forschungsunternehmen Statista. Oder anders ausgedrückt: Jede Minute werden mehr als eine Milliarde Spam-Mails versendet.

W

Whaling

Auch als Speer-Phishing bekannt, ist der Walfang eine Art sehr gezieltes Phishing, das sich oft an Führungskräfte richtet und sie dazu verleitet, vertrauliche Unternehmensinformationen oder Passwörter für Finanzsysteme oder Konten bereitzustellen.

Z

Zero-Day-Angriff

Ein Zero-Day ist der Tag, an dem ein Anbieter von einer Schwachstelle seines Systems oder seiner Software erfährt. Ein Zero-Day-Exploit erfolgt in der Zeit vor diesem Tag und nachdem Cyberkriminelle den Fehler entdeckt und dann ausgenutzt haben, typischerweise mit Malware.

Wie man Cyber-Bedrohungen bekämpft

Dies sind nur einige der Cyber-Bedrohungen da draußen, also was können Sie dagegen tun? Hier sind ein paar Optionen.

Halten Sie Ihre Systeme und Software auf dem neuesten Stand.

Schwere Schwachstellen werden in der Regel schnell mit Sicherheitsupdates von Anbietern gepatcht - wie dies bei den Schwachstellen BlueBorne, KRACK, Meltdown und Spectre der Fall war. Es läuft aber nicht immer nach Plan. Beispielsweise hat Intel seine ersten Sicherheitsupdates für Meltdown und Spectre aufgrund von Performance-Problemen zurückgezogen. Ebenso zog Microsoft sein erstes Meltdown/Spectre-Update für Windows zurück, nachdem einige PCs mit AMD-Chips nach der Installation des Patches nicht mehr booten konnten. Die neuesten Patches scheinen jedoch in Ordnung zu sein, und in der Regel überwiegen die Vorteile von schnellen System-Updates bei weitem die Alternative: anfällige Systeme.

Verwenden Sie den Endpunkt-Schutz.

Das bedeutet, Computer, Smartphones und andere Endgeräte zu schützen - zum Glück zeigt AV-Test.org, dass die Sicherheitssoftware von Android jetzt sehr effektiv ist. Neben herkömmlicher Antivirensoftware kann der Endgeräteschutz auch sichere Browsing- und Anti-Betrugs-Tools umfassen, mit denen Drive-by-Downloads und Diebstahl von Kreditkarten und anderen sensiblen Informationen durch Phishing-Angriffe oder kompromittierte Wi-Fi-Netzwerke verhindert werden können.

Fortgeschrittene Werkzeuge wie maschinelles Lernen. Heuristik (ein Algorithmus, der eine beschleunigte, akzeptable Lösung liefert) und Sandboxing (Isolierung von Anwendungen von kritischen Systemen) können helfen, Zero-Day-Exploits und andere unbekannte Bedrohungen abzuschwächen.

Sichern Sie regelmäßig.

Es war schon immer wichtig, aber es ist besonders wichtig für den Schutz vor Lösegeldern. Backups sollten "offline oder anderweitig von Computern getrennt sein", da Lösegeld und andere Malware "leicht zugängliche Backups verschlüsseln, beschädigen oder löschen können", so die hochgeschätzte Cybersicherheitsstrategie des Australian Signals Directorate.

DDoS-Minderungsdienste in Betracht ziehen

Hochkarätige Organisationen oder solche, die sich keine Ausfälle leisten können, sollten mit ihrem ISP oder einem spezialisierten Anbieter über DDoS-Minderungsdienste sprechen.

IoT-Sicherheit übernehmen

Es ist wichtig, dass Organisationen, die IoT-Anwendungen einsetzen, die verschiedenen angebotenen Sicherheitslösungen untersuchen.

Informieren Sie sich und Ihre Mitarbeiter.

E-Mail-Sicherheitsdienste wie MailGuard können betrügerische E-Mails filtern, aber letztendlich ist Bildung die erste Waffe im Kampf gegen Phishing und andere Bedrohungen, die auf Menschen und nicht auf Maschinen abzielen. Lektion Nummer eins: Verwenden Sie lange, zufällige Passphrasen - und eine andere für jedes Login, um Brute-Force und andere Angriffe zu verhindern. Ein Passwortmanager (wie Keeper Security, Dashlane, LogMeOnce oder Sticky Password) ist ein Muss.

Erwägen Sie einen erweiterten Schutz vor Bedrohungen.

Es gibt andere Arten von Sicherheitsprodukten, die von Unternehmen in Betracht gezogen werden können und sollten, wie z. B. Endpoint Detection and Response (EDR) und Threat Intelligence Services, um fortgeschrittene Bedrohungen wie APTs (Advanced Persistent Threats) abzuschwächen.

CPA Australia bietet auch Informationen zu Cyber-Bedrohungen als Teil unserer Professional Resources an. Besuchen Sie cpaaustralia.com.au/cyber für weitere Informationen.

6 Strategien zum Schutz vor Cyberangriffen
von CPA Australia

Empfehlungen der Redaktion:

Nach der zitierten australischen Werbung möchte ich es nicht versäumen, auf ein paar elementare Sicherheits-Stützpfeiler am Mac hinzuweisen:

- **Aktuelles macOS** mit den enthaltenen Sicherheitsmechanismen SIP, Gatekeeper, Malwareschutz
- **ClamXAV**: Virenscanner mit Echtzeit-Komponente ClamXAV Sentry („Wächter“), die gut geeignet ist, Viren oder Trojaner in Downloads oder Mail-Anhängen in dem Moment zu erkennen und zu isolieren, wenn sie auf den Mac geladen werden.
- **Malwarebytes** erkennt Adware, Malware und PUPs. Die Grundversion zum gelegentlichen Scannen des Macs ist kostenlos, eine Premiumversion mit Echtzeitschutz ist kostenpflichtig erhältlich.
- **DetectX Swift** identifiziert ebenfalls Adware, Malware und PUPs.
- **EtreCheck** ist ein Diagnose-Werkzeug, mit dem man den Mac und installierte Programme und Erweiterungen überprüfen kann. Zudem gibt es Auskunft über die jüngsten Crashs und ihre möglichen Ursachen.