

OUCH!

Der monatliche Security Awareness Newsletter für Sie

Haben Sie Backups?

Übersicht

Wenn Sie einen Computer oder ein mobiles Gerät lange genug benutzen, wird früher oder später etwas schief gehen. Sie können versehentlich die falschen Dateien löschen, einen Hardwarefehler haben oder ein Gerät verlieren. Oder noch schlimmer, Malware (z.B. Ransomware) könnte Ihre Dateien löschen und/oder den Zugriff darauf blockieren. Für solche Fälle sind Backups oft die einzige Möglichkeit, Ihr digitales Leben wieder aufzubauen.

Was, Wann und Wie

Backups sind Kopien Ihrer Informationen, die an anderer Stelle als auf Ihrem Computer oder mobilen Gerät gespeichert sind. Wenn Sie wertvolle Daten verlieren, können Sie Ihre Daten aus Backups wiederherstellen. Der erste Schritt ist die Entscheidung, was Sie sichern möchten, (1) bestimmte Daten, die für Sie wichtig sind; oder (2) alles, einschließlich Ihres gesamten Betriebssystems. Viele Backup-Lösungen sind standardmäßig so konfiguriert, dass sie den ersten Ansatz verwenden, sie sichern die am häufigsten verwendeten Ordner. Wenn Sie sich nicht sicher sind, was Sie sichern sollen, oder wenn Sie besonders vorsichtig sein wollen, sichern Sie alles.

Anschließend entscheiden Sie, wie oft Sie ein Backup durchführen möchten. In Betriebssysteme eingebaute Backup-Programme wie Apples Time Machine oder Windows Sicherung und Wiederherstellung ermöglichen es Ihnen, einen automatischen "Einmal eingestellt, läuft immer" Plan zu erstellen. Zu den üblichen Optionen gehören stündlich, täglich, wöchentlich, usw. Andere Lösungen bieten einen "kontinuierlichen Schutz", bei dem neue oder geänderte Dateien bei jedem Speichern eines Dokuments sofort gesichert werden. Als Basisschutz empfehlen wir Ihnen eine automatische, tägliche Sicherung kritischer Dateien vorzunehmen.

Entscheiden Sie sich, wie Sie Ihre Daten sichern wollen. Es gibt zwei Möglichkeiten: lokale oder Cloud-basierte Lösungen. Lokale Sicherungen basieren auf Geräten, die Sie verwalten, wie z.B. externe USB-Laufwerke oder über WLAN erreichbare Netzwerkgeräte. Der Vorteil des lokalen Backups liegt in der schnellen Sicherung und Wiederherstellung großer Datenmengen. Der Nachteil ist, dass sich eine Infektion mit Malware, z.B. Ransomware, möglicherweise auf Ihre Backups ausbreitet. Auch wenn sich eine Katastrophe, wie z.B. ein Feuer oder Diebstahl, ereignet, kann es dazu führen, dass Sie nicht nur Ihren Computer, sondern auch die Backups verlieren. Wenn Sie externe Geräte für Backups verwenden, lagern Sie eine Kopie außerhalb an einem sicheren Ort und stellen Sie sicher, dass Ihre Backups sinnvoll beschriftet sind.

Cloud-basierte Lösungen sind Online-Dienste, die Ihre Dateien im Internet speichern. Normalerweise installieren Sie eine Anwendung auf Ihrem Computer, die Anwendung sichert dann automatisch Ihre Dateien entweder nach einem Zeitplan oder wenn Sie sie verändern. Ein Vorteil von Cloud-Lösungen ist ihre Einfachheit, Backups erfolgen oft automatisch und Sie können normalerweise von überall auf Ihre Dateien zugreifen. Da sich Ihre Daten in der Cloud befinden, haben Schadensereignisse an Ihrem Standort, wie Feuer oder Diebstahl, keinen Einfluss auf Ihr Backup. Außerdem können Cloud-Backups Ihnen helfen, Malware-Infektionen, wie Ransomware, zu überstehen. Nachteile gibt es beim Sichern und Wiederherstellen der Daten, die Dauer ist abhängig von der Menge der Daten und der Geschwindigkeit Ihrer Internetanbindung. Sie sind sich nicht sicher, ob Sie lokale oder Cloud-basierte Backups verwenden möchten? Wenn Sie auf Nummer sicher gehen wollen, benutzen Sie beide Varianten.

Bei mobilen Geräten sind die meisten Ihrer Daten bereits in der Cloud gespeichert. Jedoch sind die Konfigurationen Ihrer Apps, Ihre aktuellen Fotos und Systemeinstellungen dort möglicherweise nicht gesichert. Durch die Sicherung Ihres mobilen Geräts erhalten Sie nicht nur diese Daten, sondern es ist auch einfacher, Ihre Daten auf ein neues Gerät zu übertragen.

Die wichtigsten Punkte



- Die Sicherung Ihrer Daten ist nur die halbe Miete; Sie müssen sicher sein, dass Sie sie wiederherstellen können. Testen Sie regelmäßig, ob Ihre Backups funktionieren, indem Sie eine Datei wiederherstellen und öffnen.
- Wenn Sie ein System aus einem Backup wiederherstellen, stellen Sie sicher, dass Sie die neuesten Sicherheitspatches und -aktualisierungen erneut installieren, bevor Sie es verwenden.
- Wenn Sie eine Cloud-Lösung verwenden, wählen Sie eine, die für Sie einfach zu bedienen ist und prüfen Sie die Sicherheitsoptionen. So ist beispielsweise wichtig, ob die Lösung eine zweistufige Authentifizierung unterstützt, um Ihr Online-Konto zu schützen.

Backups sind eine einfache und kostengünstige Möglichkeit, Ihr digitales Leben zu schützen.

Gastredakteur

Matt Bromiley ist ein professioneller Cybersicherheitsexperte und Vorfallsbearbeiter, der mit Unternehmen jeder Größe zusammengearbeitet hat. Er ist auch ein SANS-Trainer und unterrichtet in den Kursen FOR508 Advanced Incident Response und FOR572 Advanced Network Forensics. Sie können ihm auf Twitter folgen [@mbromileyDFIR](https://twitter.com/mbromileyDFIR).



Weiterführende Informationen

Einfache Passwörter erzeugen: <https://www.sans.org/u/TqR>
Malware stoppen: <https://www.sans.org/u/TqW>
Ein Cybersicheres Zuhause: <https://www.sans.org/u/Tr1>

OUCH! wird von SANS Security Awareness veröffentlicht und unter der [Creative Commons BY-NC-ND 4.0 license](https://creativecommons.org/licenses/by-nc-nd/4.0/) zur Verfügung gestellt. Die Erlaubnis zur Weitergabe dieses Newsletters oder Verwendung in einem Weiterbildungsprogramm wird gewährt, solange der Newsletter unverändert bleibt. Für Übersetzungen und weitere Informationen kontaktieren Sie bitte www.sans.org/security-awareness/ouch-newsletter. Redaktionsleitung: Walt Scrivens, Phil Hoffman, Alan Waggoner, Cheryl Conley