Der monatliche Security Awareness Newsletter für Computeranwender

OUCH!

IN DIESER AUSGABE...

- Was sollte wann gesichert werden
- Erstellung von Backups
- Wiederherstellung
- Weitere wichtige Punkte

Backup & Wiederherstellung

Überblick

Früher oder später wird etwas geschehen das zum Verlust Ihrer persönlichen Dateien, Dokumente und Fotos führt. Das kann zum Beispiel das versehentliche Löschen der falschen Dateien, ein Hardware-Fehler, ein verlorener Laptop oder eine Infektion des Rechners mit einem Schadprogramm sein. In solchen Momenten sind Sicherungskopien, engl. “Backups”, oft der einzige Weg diese digitalen Artefakte Ihres Lebens wiederherzustellen. In diesem Newsletter erläutern wir was Backups sind, wie Sie Ihre Daten sichern sollten, und wir entwickeln eine für Sie passende Sicherungsstrategie.

Gastautor

Heather Mahalik ist eine branchenweit anerkannte Expertin im Bereich digitaler Forensik und hat sich auf die Untersuchung von Smartphones spezialisiert. Sie ist Co-Autorin von “Practical Mobile Forensics”, technische Redakteurin von “Learning Android Forensics” und Co-Autorin der Kurse “FOR585 Advanced Smartphone Forensics” und “FOR518 Macintosh Forensics” des SANS Instituts. Folgen Sie Heather auf **Smarterforesnics.com** und bei Twitter: **@heathermahalik**.

Was sollte wann gesichert werden

Backups sind Kopien Ihrer Daten, die anderswo gespeichert sind. Wenn Sie wichtige Daten verlieren, können Sie diese aus Backups wiederherstellen. Leider machen die meisten Menschen keine derartigen Sicherungskopien, was um so bedauerlicher ist da es eine einfache und kostengünstige Maßnahme ist. Es gibt zwei Ansätze zu entscheiden, welche Daten gesichert werden sollten: (1) spezielle Daten die für Sie von Bedeutung sind; oder (2) alles, inklusive des kompletten Betriebssystems. Der erste Ansatz verschlankt Ihre Sicherungskopien und spart Festplattenplatz, der zweite Ansatz ist hingegen einfacher und vollumfänglich. Wenn Sie sich nicht sicher sind, was Sie sichern sollten, empfehlen wir den zweiten Ansatz zu verfolgen.

Ihre nächste Entscheidung betrifft die Häufigkeit der Sicherungen. Gängige Möglichkeiten umfassen stündliche, tägliche, wöchentliche Sicherungen und so weiter. Für die private Nutzung erlauben Datensicherungsprogramme wie “Apple Time Machine” oder “Microsoft Windows Backup and Restore” das Erstellen von automatischen Backupintervallen, um die Sie sich nach einmaliger Einrichtung nicht weiter kümmern müssen. Diese Lösungen sichern Ihre Daten den ganzen Tag unbemerkt im Hintergrund, während Sie am Computer arbeiten oder er unbenutzt läuft. Andere Lösungen bieten darüber hinaus “Echtzeitschutz” an, indem sie neue oder veränderte Dateien sofort sichern, wenn sie abgespeichert werden. Wir empfehlen, mindestens täglich Sicherungen durchzuführen. Alles läuft letztendlich auf die Frage hinaus: “Wieviele Daten kann ich mir leisten zu verlieren, wenn ich von einer Sicherung wiederherstellen muss?”

Backup & Wiederherstellung

Erstellung von Backups

Es gibt zwei Wege zur Sicherung Ihrer Daten: physische Medien oder Cloud-basierte Speicherdienste. Physische Medien werden alle Arten von Speicherhardware genannt, wie z.B. DVDs, USB Sticks oder externe Festplatten. Welches Medium Sie auch immer auswählen, sichern Sie Ihre Daten niemals auf das gleiche Gerät, auf dem die Daten bereits im Original gespeichert sind. Ein Problem bei der Nutzung von physischen Medien ist, dass Sie im Fall eines Ereignisses am Aufbewahrungsort (z.B. ein Feuer oder Diebstahl) ggf. nicht nur ihre Originaldaten, sondern auch gleichzeitig Ihre Sicherungskopien verlieren. Ihre Backupstrategie sollte daher die Lagerung der Medien an einem sicheren Ort außer Haus vorsehen - zum Beispiel bei Freunden oder am Arbeitsplatz. Stellen Sie dabei sicher, dass Sie die Datenträger beschriften um klar zu kennzeichnen, welche Daten von welchem Sicherungszeitpunkt enthalten sind. Zusätzlich sollten Sie die Daten auch verschlüsseln.

Automatisierte und zuverlässige Backups sind der letzte Rettungsanker zum Schutz Ihrer Daten.

Cloud-basierte Lösungen unterscheiden sich insofern, dass Ihre Daten irgendwo im Internet gespeichert sind. Je nach dem wieviele Daten Sie sichern möchten, kann es sich dabei um einen kostenpflichtigen Dienst handeln. Zur Nutzung muss ein Programm auf Ihrem Computer installiert werden, welches automatisch alle Dateien für Sie sichert. Der Vorteil dieser Lösung besteht darin, dass Ihre Originaldaten vor lokalen Schadensereignissen geschützt sind, da sie sich in der Cloud befinden. Zusätzlich können Sie auf die Sicherungen, oft auch auf einzelne Dateien daraus, von überall zugreifen, auch auf Reisen. Der Nachteil ist, dass Cloud-basierte Sicherungen (und die Wiederherstellung) langsamer als lokale Sicherungen sein können, insbesondere bei großen Datenmengen. Wenn Sie sich nicht sicher sind, welche Option für Sie die beste ist, nutzen Sie einfach beide Varianten.

Zu guter letzt sollten Sie auch Ihre Mobilgeräte sichern. Daten auf diesen Geräten sind fast immer bereits in der Cloud gespeichert, zum Beispiel Ihre E-Mail, Kontakte und Kalendereinträge. Darüber hinaus gibt es auf den Geräten aber auch Daten die evtl. noch nicht in der Cloud lagern, wie z.B. Einstellungen von Apps, kürzlich aufgenommene Fotos oder Systemeinstellungen. Indem Sie von Ihrem Mobilgerät Sicherungen erstellen erhalten Sie nicht nur diese Informationen, sondern erleichtern sich auch das Neuaufsetzen eines Mobilgeräts (z.B. beim Kauf eines Neuen). Ein iPhone oder iPad kann automatisch mit Apples iCloud synchronisiert werden. Bei Android und anderen mobilen Geräten hängt es vom Hersteller oder Diensteanbieter ab. In manchen Fällen ist es notwendig, spezielle Apps zu kaufen, die das Erstellen von Sicherungskopien ermöglichen.

Wiederherstellung

Das Sichern Ihrer Daten ist nur die halbe Miete. Sie müssen sich auch vergewissern, dass die Daten wiederherstellbar sind. Prüfen

Backup & Wiederherstellung

Sie die Funktionsfähigkeit Ihrer Backups am besten monatlich, indem Sie eine Datei daraus wiederherstellen und ihren Inhalt prüfen. Zusätzlich sollten Sie vor jeder größeren Änderung an Ihrem System (z.B. dem Ersetzen der Festplatte oder der Wechsel auf einen neuen Computer) eine vollständige Sicherung erstellen und prüfen, dass die Daten daraus wiederherstellbar sind.

Weitere wichtige Punkte

- Automatisieren Sie das Erstellen von Sicherungskopien soweit wie möglich, und prüfen Sie diese regelmäßig.
- Wenn Sie das ganze System aus einem Backup wiederherstellen, installieren Sie unbedingt die aktuellsten Sicherheitsupdates, bevor Sie es verwenden.
- Veraltete Backups können zu einer Belastung werden und sollten zerstört werden, um zu verhindern, dass sie in die Hände Unberechtigter fallen.
- Bei einer Cloud-basierten Sicherungslösung sollten Sie sich die Richtlinien des Anbieters durchlesen und seine Reputation überprüfen, um sicherzustellen, dass sich diese mit Ihren Anforderungen decken. Sie sollten sich z.B. folgende Fragen stellen: Verschlüsselt der Anbieter Ihre Daten? Wer hat Zugriff auf Ihre Backups? Unterstützt der Anbieter starke Authentisierungsmechanismen wie z.B. Zwei-Wege-Authentifizierung?

Weiterführende Informationen

Passwortsätze:	http://www.securingthehuman.org/ouch/2015#april2015
Zwei-Wege-Authentifizierung:	http://www.securingthehuman.org/ouch/2013#august2013
Cloud Sicherheit:	http://www.securingthehuman.org/ouch/2014#september2014
Verschlüsselung:	http://www.securingthehuman.org/ouch/2014#august2014

Informieren Sie Sich

Abonnieren Sie den monatlichen OUCH! Security Awareness Newsletter, greifen Sie auf die OUCH! Archive zu und lernen Sie mehr über SANS Security Awareness Angebote unter http://www.securingthehuman.org.

Deutsche Ausgabe

Diese OUCH! Ausgabe wurde von Marek Kreul und René Wiedewilt aus dem Englischen übersetzt. Beide arbeiten für das CERT eines DAX-Konzerns und haben sich auf IT-Forensik spezialisiert. Sie haben langjährige Erfahrung im Bereich IT-Sicherheit und sind mehrfach GIAC zertifiziert.

Redaktionsleitung: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis