Der monatliche Security Awareness Newsletter für Jedermann

OUCH!

IN DIESER AUSGABE...

- Datensicherung: Was, Wann und Wie
- Wiederherstellung
- Kernpunkte

Datensicherung & Wiederherstellung

Überblick

Wenn Sie einen Computer oder ein Mobilgerät nur lange genug verwenden, wird früher oder später etwas schief gehen (z.B. kann es zum Verlust von persönlichen Daten, Unterlagen oder Fotos kommen). Sie löschen vielleicht aus Versehen die falschen Dateien, Ihre Festplatte ist defekt, Sie verlieren ein Gerät oder werden mit einem Virus oder einem Verschlüsselungsprogramm infiziert. In diesen Situationen sind regelmäßig angefertigte Datensicherungen oft die einzige Möglichkeit zur Rettung Ihrer digitalen Daten. In diesem Newsletter erläutern wir, was Datensicherung ist, wie Sie Ihre Daten richtig sichern und entwerfen eine einfache, zu Ihnen passende Sicherungsstrategie.

Gastautor

Keith Palmgren ist im Bereich Cybersicherheit tätig und besitzt eine mehr als dreißigjährige Erfahrung auf dem Gebiet der IT Sicherheit. Er ist leitender SANS Ausbilder und der Autor des Kurses SANS SEC301, “Introduction to Information Security”. Keith führt ein erfolgreiches IT Sicherheit Beratungsunternehmen und ist auf Twitter zu finden: **@kpalmgren**

Datensicherung: Was, Wann und Wie

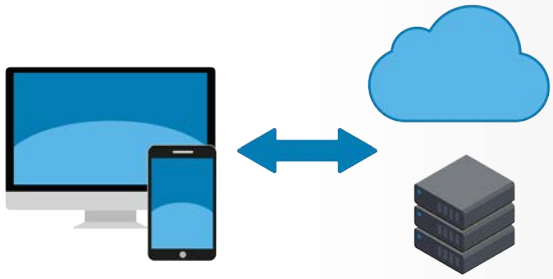
Datensicherungen, engl. „Backups“, sind Kopien Ihrer Daten die anderswo als auf Ihrem Computer oder Mobilgerät gespeichert sind. Wenn Sie wertvolle Daten verlieren, können Sie sie aus diesen Backups wiederherstellen. Leider erstellen viele Menschen viel zu selten Backups, obwohl das eine einfache und sehr kostengünstige Maßnahme ist. Der erste Schritt besteht darin, zu entscheiden was Sie sichern wollen. Es gibt prinzipiell zwei Ansätze: (1) ausgewählte Daten die Ihnen wichtig sind; oder (2) alles, einschließlich des Betriebssystems. Viele Backuplösungen sichern in der Standardeinstellung gemäß des ersten Ansatzes, sie sichern Daten aus den üblicherweise verwendeten Ordnern. In vielen Fällen ist das schon alles, was sie brauchen. Wenn Sie aber nicht sicher sind, was Sie sichern sollten, oder auf Nummer sicher gehen wollen, sichern Sie besser alles.

Im zweiten Schritt müssen Sie entscheiden, wie oft Sie sichern wollen. Eingebaute Sicherungsprogramme wie “Apple Time Machine” oder “Microsoft Windows Sichern und Wiederherstellen” ermöglichen Ihnen einen automatischen „einmal einstellen und nie wieder daran denken müssen“ Zeitplan. Übliche Optionen sind stündliche, tägliche, wöchentliche usw. Intervalle. Andere Lösungen bieten sogar „kontinuierlichen Schutz“, indem sie neue oder veränderte Daten sofort nach dem Speichern nochmal sichern. Wir empfehlen mindestens tägliche Datensicherungen.

Nun müssen Sie noch festlegen, wie die Datensicherung erfolgen soll. Wir unterscheiden hier zwei verschiedene Ansätze: physische Medien oder cloud-basierten Speicher. Jeder Ansatz hat seine eigenen Vor- und Nachteile. Wenn Sie nicht

Datensicherung & Wiederherstellung

sicher sind welcher Ansatz der geeignetere ist, können Sie einfach beide kombinieren. Physische Medien sind Geräte die Sie kontrollieren, z.B. externe USB Festplatten oder Netzwerk-Speichersysteme. Der Vorteil bei der Benutzung eigener physischer Medien ist, dass Sie so auch große Datenmengen schnell sichern und wiederherstellen können. Der Nachteil dieses Ansatzes ist, dass eine Infektion mit z.B. Ransomware möglicherweise auch Ihre Datensicherung gefährdet. Eine größere Katastrophe wie ein Diebstahl oder ein Brand kann dazu führen, dass Sie nicht nur Ihren Computer, sondern auch alle Datensicherungen verlieren. Solche externen Datenträger sollten Sie möglichst an einem anderen, sicheren Ort lagern. Achten Sie dabei unbedingt auf eine aussagekräftige Beschriftung.



Automatisierte, verlässliche Backups sind oft die letzte Möglichkeit zur Rettung Ihrer Daten.

Cloud-basierte Lösungen sind Onlinedienste, die Ihre Daten im Internet speichern. Hierfür installieren Sie gewöhnlich eine spezielle Anwendung auf Ihrem Computer. Diese Anwendung überträgt automatisch Ihre Daten basierend auf einem Zeitplan oder bei Erstellung und Veränderung. Ein Vorteil dieser Cloud-Lösung ist ihre Einfachheit, sie arbeitet meist vollautomatisch und Sie haben von überall Zugriff auf Ihre Daten. Häusliche Vorfälle wie Feuer und Diebstahl können Ihrer Cloud-Datensicherung zudem nichts anhaben. Durch die Versionierung der Backups in der Cloud können Sie sogar im Falle eines Malwarebefalls, wie z.B. durch Ransomware, eine nicht infizierte Version des Backups wiederherstellen. Leider dauert die Sicherung und Wiederherstellung signifikant länger als bei physischen Medien. Privatsphäre und Sicherheit kommt zudem eine große Bedeutung zu. Bietet der Backup-Dienstleister starke Sicherheitsmechanismen wie Datenverschlüsselung und 2-Faktor-Authentisierung?

Vergessen Sie auch Ihre Mobilgeräte nicht. Hier ist ein Großteil Ihrer Daten, beispielsweise Kalender und Kontakte, oft bereits in der Cloud gespeichert. Die Einstellungen der Apps und des System, kürzlich aufgenommene Fotos und Chat-Nachrichten sind oft aber nicht enthalten. Indem Sie ein Backup des Mobilgeräts anfertigen, schützen Sie nicht nur diese Daten, es ist auch einfacher sie auf ein neues Gerät zu übertragen wenn Sie wechseln. Ein iPhone oder iPad kann automatisch zu Apple iCloud sichern; bei Android und anderen Mobilgeräten ist es vom Hersteller oder Dienstanbieter abhängig. Es kann sein, dass Sie eine App speziell zur Datensicherung kaufen müssen.

Wiederherstellung

Das Sichern der Daten ist nur die halbe Miete; Sie müssen auch sicher sein, die Daten jederzeit wiederherstellen zu können. Prüfen Sie regelmäßig, dass die Backups funktionieren, indem Sie eine beliebige Datei daraus wiederherstellen und sie mit dem Original vergleichen. Erstellen Sie zudem vor jeder großen Änderung, wie einem Betriebssystemupdate

Datensicherung & Wiederherstellung

oder Umzug auf einen neuen Computer, eine vollständige Datensicherung, ebenso bevor Sie ein Gerät reparieren lassen (z.B. defekte Festplatte austauschen), und stellen Sie sicher, dass diese Daten wiederherstellbar sind.

Kernpunkte

- Unabhängig von der konkreten Lösung zur Sicherung Ihrer Daten sollten Sie die Backups automatisieren und regelmäßig überprüfen.
- Wenn Sie ein System von einer Datensicherung wiederherstellen, stellen Sie sicher vorher die neuesten Sicherheitspatches und Aktualisierungen einzuspielen.
- Veraltete Datensicherungen, die nicht länger benötigt werden, sind eine Bürde – löschen Sie sie, um sie vor unberechtigtem Zugriff zu schützen.
- Wenn Sie eine Cloud Lösung nutzen, prüfen Sie die Richtlinien und den Ruf des Dienstanbieters, und stellen Sie sicher, dass beides Ihren Anspruch erfüllt. Werden Ihre Daten verschlüsselt? Gibt es ein starkes Anmeldeverfahren, z.B. mittels 2-Faktor-Authentisierung?

Weiterführende Informationen

Passphrasen:	https://securingthehuman.sans.org/ouch/2017#april2017
2-Faktor-Authentisierung:	https://securingthehuman.sans.org/ouch/2015#september2015
Cloud-Sicherheit:	https://securingthehuman.sans.org/ouch/2016#november2016
Verschlüsselung:	https://securingthehuman.sans.org/ouch/2016#june2016
Ransomware:	https://securingthehuman.sans.org/ouch/2016#august2016

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 securingthehuman.sans.org/ouch/archives.

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: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley