Der monatliche Security Awareness Newsletter für Jedermann

OUCH!

IN DIESER AUSGABE...

- Überblick
- Auswahl eines Cloud Anbieters
- Absicherung Ihrer Daten

Sichere Nutzung der Cloud

Überblick

“Die Cloud” kann für verschiedene Menschen unterschiedliches bedeuten, meist bezeichnet man damit aber die Angebote von Dienstleistern im Internet zur Verwaltung Ihrer Computersysteme und/oder Speicherung Ihrer Daten. Ein Vorteil der Cloud ist die einfache Erreichbarkeit und Synchronisierung Ihrer Daten auf mehreren Geräten überall auf der Welt, und die Möglichkeit leicht Daten mit beliebigen anderen Personen zu teilen. Der Begriff „Cloud“, zu deutsch „Wolke“, ist treffend gewählt, denn oft weiß man als Kunde nicht wo die Daten physisch gespeichert sind. Beispiele für das sog. Cloud-Computing sind das Erstellen von Dokumenten mittels Google Docs, das Teilen von Daten mittels Dropbox, das Betreiben eines eigenen Servers in der Amazon Cloud, das Speichern von Kundendaten in Salesforce oder das Archivieren Ihrer Bilder und Musiktitel in Apple’s iCloud. Diese Online-Dienste können Ihre Produktivität sehr erhöhen, bergen aber auch ganz eigene Risiken. In diesem Newsletter erklären wir Ihnen daher, wie Sie auf sichere Art die Cloud zu Ihrem Vorteil nutzen können.

Gastautor

Dave Shackleford (**@daveshackleford**) ist IT Berater, Besitzer des Unternehmens Voodoo Security und Autor zahlreicher SANS Kurse, einschließlich SANS Security 579: Virtualization and Private Cloud Security und Security 524: Cloud Security Fundamentals.

Auswahl eines Cloud Anbieters

Die Cloud ist weder gut noch schlecht, es ist ein Werkzeug um Dinge zu erledigen – sowohl privat wie auch beruflich. Wenn Sie diese Dienste nutzen, händigen Sie jedoch private bzw. vertrauliche Daten an Dritte aus und müssen darauf vertrauen, dass der Dienstleister sie sicher und jederzeit für Sie zugänglich verwahrt. Daher kommt der Auswahl eines Cloud-Anbieters eine hohe Bedeutung zu. Für berufliche Nutzung sollten Sie Ihre Vorgesetzten ansprechen um zu erfahren, ob und ggf. welche Cloud-Dienste Sie nutzen dürfen, und welchen Richtlinien die Nutzung unterliegt. Wenn Sie einen Cloud Dienst für private Nutzung in Betracht ziehen, beachten Sie folgendes:

1. **Unterstützung**: Wie leicht ist es Hilfe zu bekommen oder Antwort auf eine Frage? Gibt es eine E-Mail-Adresse die Sie kontaktieren, oder ein öffentliches Forum in dem Sie Ihre Fragen stellen können? Gibt es eine Sektion für häufig gestellte Fragen (FAQ) auf der Webseite?
2. **Einfachheit**: Wie leicht ist der Dienst zu nutzen? Je komplexer der Dienst ist, umso wahrscheinlicher werden

Sichere Nutzung der Cloud

Sie Fehler machen und versehentlich Daten verlieren oder veröffentlichen. Wählen Sie einen Cloud-Anbieter, dessen Dienste Sie leicht verständlich, einfach zu konfigurieren und zu nutzen finden.

3. **Sicherheit**: Welche Daten werden von Ihnen ggf. gesammelt? Wie gelangen Ihre Daten von Ihrem Computer zum Cloud-Dienst, und wie werden Sie dort übertragen? Sind sie verschlüsselt – und wer kann sie wieder entschlüsseln?
4. **Nutzungsbedingungen**: Nehmen Sie sich einen Moment Zeit, um die Nutzungsbedingungen durchzulesen (diese sind oft überraschend leicht zu lesen). Prüfen Sie wer Zugriff auf Ihre Daten erhalten kann, was ihre Rechte sind und welche Verpflichtungen zum Schutz der Daten der Anbieter in Ihrer Zuständigkeit sieht.

Die Cloud kann den Zugang zu Ihren Daten erleichtern und Ihre Produktivität erhöhen, seien Sie jedoch vorsichtig wie Sie auf die Daten zugreifen und sie mit anderen teilen.

Absicherung Ihrer Daten

Sobald Sie einen Cloud-Anbieter ausgewählt haben, besteht der nächste Schritt darin sicherzustellen, dass Sie den Dienst sachgemäß nutzen können. Wie Sie auf Ihre Daten zugreifen und diese teilen kann oft einen größeren Einfluss auf ihre Sicherheit haben als alles andere. Die wichtigsten Schritte hierbei sind:

1. **Authentisierung**: Nutzen Sie ein starkes, einzigartiges Passwort um sich an Ihrem Cloud-Konto anzumelden. Wenn Ihr Cloud-Anbieter Zwei-Faktor-Anmeldung anbietet, empfehlen wir Ihnen sehr dieses Verfahren zu nutzen. Das ist einer der wichtigsten Schritte zur Absicherung Ihres Cloud-Kontos!
2. **Dateien / Ordner teilen**: Die Cloud macht es sehr leicht Daten zu teilen, manchmal zu leicht. Im schlimmsten Fall denken Sie vielleicht, Sie teilen Daten nur mit einer Person, geben aber versehentlich Dateien oder gar ganze Ordner für das gesamte Internet frei. Der beste Weg zum Schutz Ihrer Daten ist, standardmäßig Daten für niemanden freizugeben. Gewähren Sie dann nur genau benannten Personen oder Gruppen Zugriff auf wenige, ausgewählte Dateien und Ordner, je nach deren Bedarf. Wenn jemand nicht länger Zugriff auf Ihre Dateien benötigt, entfernen Sie die Berechtigung wieder. Ihr Cloud-Anbieter sollte einen einfachen Weg anbieten um einzusehen, wer Zugriff auf welche Dateien und Ordner hat.
3. **Dateien / Ordner über Links teilen**: Eine gängige Funktion von Cloud-Diensten ist die Möglichkeit, einen Web-Link zu generieren der auf Ihre Dateien oder Ordner zeigt. Diese Funktion erlaubt das Teilen von Inhalten mit beliebigen Personen, einfach durch Weitergeben des Web-Links. Dieser Ansatz bietet jedoch nur sehr wenig Sicherheit, da jeder

Sichere Nutzung der Cloud

der den Link kennt Zugriff auf die Daten hat. Wenn Sie den Link nur an eine Person senden, kann diese Person ihn an beliebige andere weitergeben, oder er könnte sogar von Suchmaschinen gefunden werden. Wenn Sie Daten mittels eines Web-Links teilen, stellen Sie sicher, dass Sie den Link deaktivieren wenn er nicht länger benötigt wird, idealerweise durch Setzen eines Ablaufdatums. Sie können den Link auch mit einem zusätzlichen Passwort schützen.

4. **Einstellungen**: Beschäftigen Sie sich mit den Sicherheitseinstellungen, die Ihr Cloud-Anbieter bereitstellt. Kann z.B. jemand, dem Sie Daten freigegeben haben, diese wiederum ohne Ihr Wissen für andere freigeben? Vielleicht gibt es auch die Möglichkeit einzusehen, wer Ihre freigegebenen Daten angesehen hat, und wann das geschah. Können Sie Ihre Daten auch im „nur lesen“ Modus freigeben, alternativ zum Modus „lesen+schreiben“ in dem Personen die Inhalte auch verändern können?
5. **Antivirus**: Die aktuellste Version eines Virenschutzprodukts sollte auf Ihrem und jedem anderen Computer installiert sein, mit dem Sie Daten teilen. Wenn eine von Ihnen freigegebene Datei infiziert wird, könnten sonst auch andere Computer die darauf Zugriff haben infiziert werden.

Weiterführende Informationen

Zwei-Faktor-Authentifizierung:	https://securingthehuman.sans.org/ouch/2015#september2015
Starke Passwörter:	https://securingthehuman.sans.org/ouch/2015#april2015
Passwort-Manager:	https://securingthehuman.sans.org/ouch/2015#october2015
Schadprogramme:	https://securingthehuman.sans.org/ouch/2016#march2016
SEC524: Cloud Security Fundamentals:	https://sans.org/sec524

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: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis, Cheryl Conley