Der monatliche Security Awareness Newsletter für Computeranwender

OUCH!

IN DIESER AUSGABE...

- Überblick
- Auswahl eines Cloud Anbieters
- Schutz Ihrer Daten

Sichere Nutzung von Cloud-Diensten

Überblick

“Die Cloud” ist eine sehr mächtige Technologie, die binnen kurzer Zeit sowohl bei Privatnutzern wie auch bei Unternehmen einen hohen Stellenwert einnahm. “Cloud” hat hierbei häufig mehrere Bedeutungen, beschreibt im Allgemeinen aber die Nutzung eines Diensteanbieters im Internet zur Verarbeitung und Speicherung Ihrer Daten. Vorteil der „Cloud“ ist nicht nur, dass Sie jederzeit von überall her Ihre Daten von all Ihren Geräten erreichen und diese abgleichen können, sondern dass Sie Daten auch mit jedermann teilen können. Der Grund warum diese Dienste als “Cloud”, zu Deutsch “Wolke”, bezeichnet werden, ist dass man gewöhnlich gar nicht genau weiß, wo die Daten physikalisch gespeichert sind. Beispiele für das sogenannte „Cloud Computing“ sind das Bearbeiten von Dokumenten mittels Google Docs, das Speichern und Teilen von Dateien in der Dropbox, der Betrieb eines eigenen Servers in der Amazon Cloud, oder das Speichern von Musik in Apple‘s iCloud. Diese Onlinedienste haben das Potential, Ihnen tagtäglich die Arbeit bedeutend zu erleichtern, sie bergen jedoch auch ihre ganz eigenen Risiken. In diesem Newsletter beschreiben wir daher die sichere Nutzung der Cloud.

Gastautor

James und Kelli Tarala (@isaudit / @kellitarala) sind leitende Berater bei Enclave Security und haben vielfältige SANS Trainingsprogramme erstellt, darunter SANS Audit 566: Implementing and Auditing the Twenty Critical Security Controls und MGT 415: A Practical Introduction to Risk Assessments.

Auswahl eines Cloud Anbieters

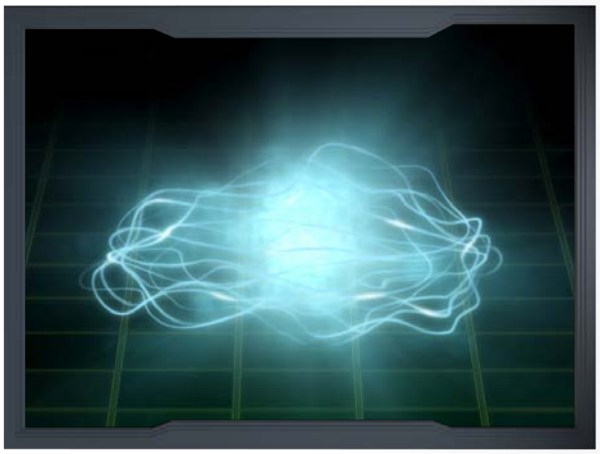
Die Cloud ist weder gut noch böse, sie ist schlicht ein Werkzeug um Dinge zu erledigen, sowohl privat als auch im Job. Wenn Sie diese Dienste nutzen, geben Sie jedoch Ihre eigenen, schützenswerten Daten in die Hände Fremder, von denen Sie annehmen, dass sie Ihre Daten schützen und dauerhaft verfügbar halten. Daher sollten Sie den geeigneten Anbieter gewissenhaft auswählen. Für Ihren beruflich genutzten Computer bzw. Unternehmensdaten sollten Sie die Nutzung von Cloud-Diensten mit Ihren Vorgesetzten besprechen. Wenn die Nutzung von Cloud-Diensten erlaubt ist, sollten Sie zudem klären welche Dienste genau erlaubt sind, und welchen Auflagen die Nutzung unterliegt. Wenn Sie einen Cloud-Anbieter für Ihren persönlichen Bedarf suchen, bedenken Sie die folgenden Punkte:

1. **Unterstützung**: Wie leicht ist es, Hilfe oder eine Antwort auf eine Frage zu bekommen? Gibt es eine Telefonnummer oder E-Mail-Adresse, die Sie kontaktieren können? Gibt es weitere Möglichkeiten wie z.B. öffentliche Foren oder FAQ Bereiche auf der Webseite des Anbieters?
2. **Einfachheit**: Wie einfach ist es, den Dienst zu nutzen? Je komplexer die Benutzung ist, desto eher besteht

Sichere Nutzung von Cloud-Diensten

die Gefahr einer Fehlbedienung, die womöglich zu Verlust oder Veröffentlichung Ihrer privaten Daten führt. Nutzen Sie einen Cloud-Anbieter, dessen Bedienung verständlich ist und dessen Konfiguration Sie überblicken können.

3. **Sicherheit**: Wie gelangen Ihre Daten von Ihrem Computer in die Cloud, ist die Verbindung sicher verschlüsselt? Wie werden Ihre Daten beim Anbieter gespeichert, sind sie verschlüsselt und wer kann sie ggfs. entschlüsseln?
4. **Nutzungsbedingungen**: Nehmen Sie sich die Zeit, die Nutzungsbedingungen zu lesen (sie sind oft überraschend einfach zu lesen). Prüfen Sie, wer Zugriff auf Ihre Daten hat, und welche Zugriffsrechte diese Personen haben.



Die Cloud kann Ihre Informationen leichter verfügbar machen und einen Produktivitätsgewinn bedeuten, bedingt aber große Sorgfalt beim Speichern und Teilen von Daten.

Schutz Ihrer Daten

Sobald Sie einen Cloud-Anbieter ausgewählt haben ist der nächste Schritt sicherzustellen, dass Sie den Dienst korrekt benutzen. Wie Sie auf Ihre Daten zugreifen und diese teilen, kann oft weit größere Auswirkungen auf die Sicherheit Ihrer Dateien haben als alles andere. Einige Schlüsselpunkte hierfür sind:

1. **Anmeldung**: Nutzen Sie ein starkes, einzigartiges Passwort zur Anmeldung an Ihrem Cloud-Konto. Einige Anbieter ermöglichen eine Zwei-Wege-Authentifizierung, wovon Sie wann immer möglich Gebrauch machen sollten.
2. **Teilen von Dateien / Ordnern**: Die Cloud macht es sehr leicht, Daten zu teilen, manchmal sogar zu leicht. Im schlimmsten Fall stellen Sie vielleicht sogar Ihre Dateien oder ganze Ordner unabsichtlich öffentlich ins Internet. Der beste Schutz dagegen ist natürlich, zunächst keinerlei Dateien mit irgendwem zu teilen. Zugriff auf einzelne Dateien oder Ordner sollten dann nur genau benannte Personen oder Gruppen erhalten, und jeder nur auf das worauf er Zugriff benötigt. Sobald eine berechtigte Personen keinen Zugriff auf von Ihnen freigegebene Daten mehr benötigt, entfernen Sie die Berechtigung umgehend. Ihr Cloud-Anbieter sollte einen einfachen Weg bereitstellen, die eingestellten Zugriffsmöglichkeiten auf Ihre Daten zu überprüfen und zu verwalten.
3. **Teilen von Dateien / Ordnern mittels Links**: Ein gängiges Merkmal von Cloud-Diensten ist die Möglichkeit, einen Link zu erzeugen der auf freigegebene Dateien oder Ordner zeigt. Damit können Sie jedermann einfach Zugriff auf die Daten verschaffen, ohne dass der Empfänger ein eigenes Konto bei dem Cloud-Anbieter benötigt. Dieser Ansatz bietet jedoch nur sehr geringe Sicherheit, denn jeder der diesen Link kennt oder errät hat Zugriff auf die Daten. Wenn Sie den Link nur einer einzigen Person senden, kann diese ihn wiederum beliebig an Dritte weitergeben, ja er könnte sogar im Ergebnis von Suchmaschinen wie Google zu finden sein. Stellen Sie daher

Sichere Nutzung von Cloud-Diensten

sicher, den Link wieder zu deaktivieren, sobald er nicht mehr benötigt wird, oder schützen Sie ihn zusätzlich mit einem Passwort.

4. **Einstellungen**: Stellen Sie sicher, dass Sie die Bedeutung der verschiedenen Einstellungen Ihres Cloud-Anbieters verstehen. Wenn Sie z.B. Daten mit jemandem teilen, kann dieser wiederum selbst die Daten ohne Ihr Wissen mit Dritten teilen?
5. **Virenschutz**: Stellen Sie sicher, dass auf Ihrem Computer und allen weiteren, die auf Ihre Daten zugreifen, ein aktuelles Virenschutzprogramm installiert ist. Wenn eine Ihrer Dateien, die bei Ihrem Cloud-Anbieter lagert, auf einem Computer infiziert wird verteilt sich diese Datei auch auf alle anderen zugreifenden Systeme.
6. **Datensicherung**: Auch wenn Ihr Cloud-Anbieter eine Sicherung Ihrer Daten vornimmt, sollten Sie regelmäßig selbst ein solches Backup erstellen. Sie stellen damit nicht nur sicher, weiterhin Zugriff auf Ihre Daten zu haben wenn Ihr Anbieter sein Geschäft einstellt oder die Daten aus irgend einem anderen Grund dort nicht mehr verfügbar sind, sondern können auch einfacher größere Datenmengen aus Ihrer eigenen Sicherung wiederherstellen anstatt diese aus der Cloud zu laden. Prüfen Sie zudem wie oft Ihr Anbieter eine Sicherung vornimmt, ob er Ihnen die Möglichkeit bietet ältere Versionen von Dateien wiederherzustellen und wie lange ältere Sicherungen vorgehalten werden.

Weiterführende Informationen

OUCH! Starke Passwörter:	http://www.securingthehuman.org/resources/newsletters/ouch/2013#may2013
OUCH! Passwortverwaltungsprogramme:	http://www.securingthehuman.org/resources/newsletters/ouch/2013#october2013
OUCH! Datensicherung:	http://www.securingthehuman.org/resources/newsletters/ouch/2013#september2013
Gängige Begriffe der IT Sicherheit:	https://www.bsi-fuer-buerger.de/BSIFB/DE/Wissenswertes_Hilfreiches/Service/Glossar/glossar_node.html

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

OUCH! wurde aus dem Englischen übersetzt von Marek Kreul und René Wiedewilt. Beide arbeiten für das CERT eines deutschen IT-Dienstleisters 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