Bundesamt
für Sicherheit in der
Informationstechnik

BSI FÜR BÜRGER

INS INTERNET - MIT SICHERHEIT

In die Cloud – aber sicher!

Basisschutz leicht gemacht

Tipps und Hinweise zu
Cloud Computing

www.bsi-fuer-buerger.de ▪ www.facebook.com/bsi.fuer.buerger

In die Cloud – aber sicher

Eine Cloud ist ein Online-Dienst. Sie speichern Ihre Daten auf Rechnern, auf die Sie über das Internet jederzeit zugreifen können. Daten in der Cloud zu hinterlegen ist zwar praktisch, birgt aber auch Risiken. Wir haben für Sie Informationen und hilfreiche Tipps rund um das Cloud Computing zusammengestellt, die wir Ihnen auf unserer Web-Seite

www.bsi-fuer-buerger.de/BSIFB/Cloud

anbieten.

2 Was bedeutet Cloud Computing eigentlich?

Cloud Computing kann als „Rechenleistung aus der Wolke“ verstanden werden, wobei die Wolke ein bildlicher Ausdruck für viele vernetzte Rechner ist. Beim Cloud Computing greifen Sie somit nicht mehr auf die Rechenleistung oder den Speicher Ihres eigenen PCs zurück, sondern nutzen die Rechenleistung eines Cloud-Anbieters. Da er mit dem Internet verbunden ist, sind Ihre Daten mit Ihrem PC, Smartphone oder Tablet stets abrufbar. Neben dem Speichern von Daten bieten viele Cloud-Anbieter auch Software-Anwendungen an.

3 Wo werden Cloud-Dienste eingesetzt?

Ein klassisches Beispiel für einen Cloud-Dienst ist Web-Mail. Anbieter stellen Ihnen online ein Postfach für Ihre E-Mails zur Verfügung. Die Nachrichten Ihres Online-Postfachs befinden sich auf dem Server des Anbieters. Sie können von jedem Ort aus und mit jedem internetfähigen Gerät auf Ihre E-Mails zugreifen. Ein weiterer beliebter Cloud-Dienst sind Online-Speicher, bei denen Sie Daten hinterlegen und mit anderen Nutzern teilen können.

Einige Anbieter ermöglichen es, Ihre Daten auch mit online ausführbaren Anwendungen zu bearbeiten, etwa mit Programmen zur Text- oder Grafikbearbeitung. Die Anwendung muss dafür nicht auf Ihrem Rechner installiert sein. Die gespeicherten Dateien können über einen Browser direkt in der Cloud bearbeitet werden.

4 Vorteile der Cloud

Flexibilität und Verfügbarkeit
Der Zugriff auf die in der Cloud gespeicherten Daten ist für Sie jederzeit und von überall her mit einem internetfähigen Gerät möglich. Der Cloud-Anbieter ist verantwortlich für ausreichend Rechenleistung und Speicherplatz.

Nutzerfreundlichkeit
Cloud-Dienste werden über den Browser oder über Apps aufgerufen. Ohne großen Aufwand können Sie in der Cloud Ihre Daten mit anderen teilen. Dazu müssen Sie die Daten lediglich einmal in die Cloud hochladen. Mit einer entsprechenden Berechtigung können diese dann mit anderen geteilt werden.

Kostenersparnis
Wenn Sie einen Cloud-Dienst nutzen, ersparen Sie sich den Kauf und die Aktualisierung von Hard- und Software, die notwendig wären, um dieselben Anwendungen auf Ihrem Rechner zu nutzen. Viele Anbieter stellen Privatanwendern kostenlose Basis-Leistungen zur Verfügung. Benötigen Sie mehr, werden Preise nach Umfang gestaffelt.

Daten-Backup und Sicherheit
Grundsätzlich ist der Cloud-Anbieter für die Sicherheit der in der Cloud gespeicherten Daten verantwortlich. Er übernimmt das Einspielen von Softwareupdates, die Aktualisierung des Virenschutzes oder die Durchführung einer Datensicherung. Als Nutzer sollten Sie zudem die Tipps beachten, die wir Ihnen im Folgenden zusammengestellt haben.

5 Tipps rund um Cloud Computing

Basisschutz
Der beste Schutz Ihrer Daten beim Cloud-Anbieter nützt wenig, wenn Ihr Endgerät nicht geschützt ist. Ein guter Basisschutz (siehe Infokasten) ist daher unumgänglich. Schadsoftware auf Ihrem Zugangsgerät kann auch Ihre Daten in der Cloud angreifen. Der Zugriff auf Cloud-Dienste ist oft nur über Benutzername und Passwort geschützt. Sobald jemand anderes diese Zugangsdaten kennt, kann er ungehindert, jederzeit und von überall her auf Ihre Daten zugreifen. Der Zugriff über unsichere Netze – etwa ungesicherte WLAN-Hotspots – stellt ein Risiko dar. In diesen Netzen können Angreifer Zugangsdaten mitlesen und missbrauchen.

Info

Weitere Tipps zum Basisschutz erhalten Sie in unserer Broschüre „Surfen – aber sicher“ und auf unserer Web-Seite *www.bsi-fuer-buerger.de/Smartphones.*

Mobile Endgeräte

Nicht nur Sie haben über eine auf dem Smartphone installierte App leichten Zugriff auf die Daten in der Cloud, sondern auch mögliche Angreifer. Viele Anwender speichern die Zugangsdaten in der App des Cloud-Anbieters. Dann genügt ein Aufruf der App, um auf die Daten zuzugreifen. Gerät das Smartphone in falsche Hände, sind die Daten in der Cloud nur so sicher, wie das Smartphone vor unerlaubtem Zugriff geschützt ist.

Info

Weitere Tipps zum Umgang mit den mobilen Endgeräten erhalten Sie in unserer Broschüre „Mobilkommunikation“ und auf unserer Web-Seite *www.bsi-fuer-buerger.de*.

Nutzungsbedingungen und Datenschutzbestimmungen

Jeder Cloud-Anbieter kann seine eigenen Nutzungsbedingungen aufstellen, solange er damit keine Gesetze bricht. Dasselbe gilt für den Datenschutz. Möglicherweise räumen Sie dem Anbieter Zugriffs- und Nutzungsrechte für Ihre gespeicherten Dateien ein. Überprüfen sie hier genau, welche Rechte Sie Ihrem Dienstleister einräumen.

Haftungsfragen und Anbieterwechsel

Informieren Sie sich sorgfältig über Haftungsfragen im Falle eines Datenverlustes, einer Anbieterinsolvenz oder eines Eigentümerwechsels. Auch für den Fall eines Anbieterwechsels müssen Sie sich bereits im Vorfeld darüber informieren, ob eine problemlose Datenmigration möglich ist.

Weitergabe von Daten an Dritte

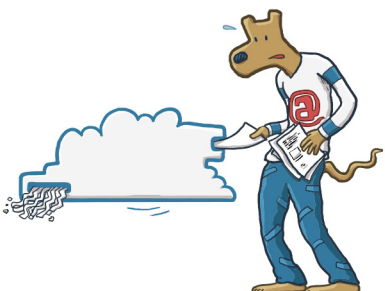
Besonders bei kostenlosen Cloud-Diensten besteht die Möglichkeit, dass der Anbieter Daten an Dritte zu kommerziellen Zwecken verkauft oder selbst nutzt. Ein Blick in die allgemeinen Geschäftsbedingungen (AGB) gibt Auskunft darüber, welche Rechte Sie Ihrem Anbieter einräumen.

Standorte des Cloud-Anbieters und der Cloud-Rechenzentren

Es ist häufig nicht ersichtlich, in welchem Land der Cloud-Anbieter seinen Sitz hat oder wo sich die von ihm genutzten Rechenzentren befinden. Auch ein in Deutschland ansässiges Unternehmen kann durchaus Server im Ausland betreiben. Daher ist es für den Anwender in der Regel nicht nachvollziehbar, an welchem Ort der Welt seine Daten gespeichert werden und welchen rechtlichen Bestimmungen die Daten damit unterliegen.

Verfügbarkeit und Integrität der Daten
Sollten Sie über keine Internetverbindung verfügen, können Sie nicht auf die Daten in der Cloud zugreifen. Das Gleiche gilt, wenn die Internetanbindung oder das Rechenzentrum des Cloud-Anbieters ausfällt. Erkundigen Sie sich bei Ihrem potenziellen Cloud-Anbieter über dessen IT-Infrastruktur und achten Sie darauf, dass er über ein sicheres Rechenzentrum, eine redundante Internetanbindung und einen räumlich entfernten Ausweichstandort verfügt.

Dies ist vor allem dann angeraten, wenn Sie besonders wichtige Daten in der Cloud speichern, wie beispielsweise Gesundheitsdaten oder die Steuererklärung. Informieren Sie sich über die Sicherheitszusagen des Cloud-Anbieters. Zertifikate können hier Vertrauen schaffen.



Zugang zu Cloud-Diensten
Eine einfache Kombination aus Benutzername und Passwort schützt nicht optimal. Inzwischen bieten immer mehr Cloud-Anbieter eine Zwei-Faktor-Authentisierung an, wie sie beispielsweise beim Online-Banking eingesetzt wird. Zusätzlich zu Benutzername und Passwort wird hier ein einmalig gültiger temporärer Zugangscode generiert, um den rechtmäßigen Nutzer zweifelsfrei zu authentisieren.

Verschlüsselung der Datenübertragung
Der gesamte Datenverkehr mit der Cloud kann verschlüsselt oder unverschlüsselt erfolgen. Werden die Daten unverschlüsselt übertragen, sind diese für Unbefugte einsehbar, die sich zum Beispiel über einen Man-In-The-Middle-Angriff[1] in Ihre Datenübertragung einklinken. Achten Sie bei der Auswahl Ihres Cloud-Anbieters unbedingt darauf, dass die Übertragung über eine sichere Verbindung wie https erfolgt.

1 Zwischen Sender und Empfänger werden die Daten „in der Mitte“ abgegriffen.

Datenverschlüsselung

Wichtige und sensible Daten sollten nur verschlüsselt in der Cloud gespeichert werden. Viele Cloud-Anbieter bieten eine Verschlüsselung der Daten in der Cloud bereits an. Allerdings können Sie die Umsetzung und tatsächliche Sicherheit dieser Maßnahmen nicht überprüfen, wenn der Schlüssel zum Entschlüsseln beim Cloud-Anbieter liegt. Eventuell werden die Anbieter von Behörden aufgefordert, Ihre Daten zu entschlüsseln. Die derzeit sicherste Variante ist daher, die Daten selbst zu verschlüsseln und anschließend in die Cloud zu übertragen. So können Sie sichergehen, dass nur Sie Zugriff auf Ihre Inhalte haben. Das bedeutet jedoch auch, dass Sie Ihre Daten bei sich abspeichern und entschlüsseln müssen, um mit ihnen arbeiten zu können. Dazu ist es notwendig, dass auf jedem Gerät, mit dem Sie auf Ihre Inhalte zugreifen möchten, Ihr privater Schlüssel und die Verschlüsselungssoftware vorhanden ist.

Datenlöschung

Bevor Sie Ihre Daten einem Cloud-Anbieter anvertrauen, sollten Sie prüfen, wie aufwendig es ist, die Daten wieder aus der Cloud zu entfernen. Das endgültige Löschen von Daten in der Cloud gestaltet sich schwieriger als auf dem eigenen Rechner zu Hause. Cloud-Anbieter speichern zur Sicherheit oft mehrere Kopien der Dateien in verschiedenen Rechenzentren. Vereinzelt werden Daten auch nicht gelöscht, sondern sind nur nicht mehr für Sie sichtbar. So kann der Cloud-Anbieter weiter die Daten nutzen, um beispielsweise Profile zu erstellen.

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik – BSI

Bezugsquelle
Bundesamt für Sicherheit in der Informationstechnik – BSI
Godesberger Allee 185-189, 53175 Bonn
E-Mail: mail@bsi-fuer-buerger.de
Internet: www.bsi.bund.de
www.bsi-fuer-buerger.de
www.facebook.com/bsi.fuer.buerger
Telefon +49 (0) 22899 9582-0
Service-Center +49 (0) 800 274 1000

Stand
August 2016

Illustrationen
Leo Leowald

Artikelnummer
BSI-IFB 16/253