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

1 In die Cloud – aber sicher

Ein Cloud-Dienst ist ein Online-Dienst, auf den Sie über das Internet jederzeit zugreifen können. Beispielsweise können Sie Daten in der Cloud hinterlegen, sie mit anderen teilen oder gemeinsam bearbeiten. Das ist praktisch, birgt aber auch Risiken. Wir haben für Sie Informationen und hilfreiche Tipps rund um das Cloud Computing zusammengestellt, die wir Ihnen auf unserer Webseite anbieten:

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

2 Was bedeutet Cloud Computing eigentlich?

Cloud Computing kann als „Rechenleistung aus der Wolke“ verstanden werden. Die Wolke ist dabei ein bildlicher Ausdruck für Rechenzentren, die mit dem Internet verbunden sind. Er macht zudem deutlich, dass das Innere der Wolke unbekannt und von außen nicht einsehbar ist. Beim Cloud Computing greifen Sie somit nicht mehr auf die Rechenleistung oder den Speicher Ihres eigenen PCs, Smartphones oder Tablets zurück, sondern nutzen die Rechenleistung eines Cloud-Anbieters. Da die Cloud mit dem Internet verbunden ist, sind Ihre Daten mit unterschiedlichen Endgeräten stets abrufbar. Neben dem Speichern von Daten bieten viele Cloud-Anbieter auch Software-Anwendungen an, beispielsweise zum Bearbeiten von Dokumenten.

3 Wo werden Cloud-Dienste eingesetzt?

Unterschiedliche Cloud-Dienste haben gemeinsam, dass Anbieter einen Dienst mit spezifischer Funktionalität zur Verfügung stellen. Die genaue technische Umsetzung des Dienstes ist dabei in der Regel nicht bekannt.

Ein beliebter Cloud-Dienst sind Online-Speicher, bei denen Sie Daten hinterlegen und diese von verschiedenen Endgeräten aufrufen oder sie 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.

Ein weiteres Beispiel für einen Cloud-Dienst ist die Web-Mail. Anbieter stellen Ihnen online ein Postfach für Ihre E-Mails zur Verfügung. Die Nachrichten Ihres Online-Postfachs befinden sich dabei auf dem Server des Anbieters. Sie können von jedem Ort aus und mit jedem internetfähigen Gerät auf Ihre E-Mails zugreifen.

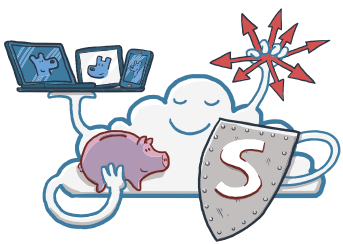
Geräte wie Smartwatches oder Fitnesstracker synchronisieren ihre Aufzeichnungen je nach Einstellung mit cloudbasierten Online-Diensten. Diese können die Daten automatisiert nach bestimmten Kriterien auswerten.

Auch die beliebten Video- oder Musik-Streaming-Plattformen sind Cloud-Dienste. Der Anbieter eines Streaming-Dienstes hat über die Analyse des jeweiligen Nutzerverhaltens die Möglichkeit, Auswertungen zu erstellen und so zum Beispiel zielgerichtet Werbung einzublenden.

4 Vorteile der Cloud

Flexibilität und Verfügbarkeit
Der Zugriff auf die in der Cloud gespeicherten Daten ist für Sie jederzeit und von überall mit einem internetfähigen Gerät möglich. Der Cloud-Anbieter ist grundsätzlich verantwortlich für ausreichend Rechenleistung und Speicherplatz. Wie groß diese konkret sind, hängt vom jeweiligen Nutzungsvertrag ab.

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 andere dann auf diese zugreifen.



Aktualität
Software-Anbieter, die ihre Software über die Cloud bereitstellen, halten diese in der Regel auf dem neusten Stand. Cloud-Nutzer müssen sich entsprechend nicht um Software-Updates kümmern oder gar eine neue Version erwerben. Sie mieten den Dienst und der Anbieter sorgt für die Bereitstellung der Funktion.

Daten-Backup und Sicherheit
Grundsätzlich ist der Cloud-Anbieter für die Sicherheit der in der Cloud gespeicherten Daten verantwortlich. Regelmäßige Daten-Backups, also das Anlegen einer aktuellen Datensicherung, werden automatisch erstellt. Weitere Sicherheitsaspekte werden ebenso zentral bewerkstelligt, beispielsweise das Einspielen von Sicherheitsupdates für die bereitgestellte Software sowie die Aktualisierung des Virenschutzes. So wird verhindert, dass Angreifer Sicherheitslücken in Software ausnutzen können.

Als Nutzer sollten Sie jedoch 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 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 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 Webseite *www.bsi-fuer-buerger.de/SicherSurfen*.

Zugang zu Cloud-Diensten

Schützen Sie den Zugang zu Ihrem Cloud-Dienst. Eine einfache Kombination aus Benutzername und starkem Passwort schützt nicht optimal. Inzwischen bieten immer mehr Cloud-Anbieter eine Zwei-Faktor-Authentisierung an, wie sie beispielsweise beim Onlinebanking eingesetzt wird. Zusätzlich zu Benutzername und einem starken Passwort (erster Faktor) wird hier ein weiteres Merkmal eingesetzt, um den rechtmäßigen Nutzer zweifelsfrei zu authentisieren. Als zweiter Faktor kommt beispielsweise ein Sicherheitstoken, also eine Hardware-Komponente wie ein Schlüssel, eine Chipkarte oder ein spezieller USB-Stick, zum Einsatz. Auch eine vom Anbieter versendete SMS kann genutzt werden.

Tipps zu starken Passwörtern erhalten Sie auf unserer Webseite *www.bsi-fuer-buerger.de/Passwoerter.*

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. Gelangt das Smartphone in falsche Hände, sind die Daten in der Cloud nur so sicher, wie das Smartphone vor unerlaubtem Zugriff geschützt ist.

Info

Tipps zum sicheren Umgang mit mobilen Endgeräten erhalten Sie in unserer Broschüre „Sicher unterwegs mit Smartphone, Tablet & Co“ und auf unserer Webseite *www.bsi-fuer-buerger.de/Smartphones.*

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 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 Datenübertragung 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, Vertraulichkeit 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. Informieren Sie sich über die Sicherheitszusagen des Cloud-Anbieters. Wie gewährleistet er die Verfügbarkeit der Daten? Sind diese seitens des Anbieters vor unbefugtem Zugriff geschützt? Kann ihre Unversehrtheit sichergestellt werden? Über verschiedene, durch unabhängige Institutionen vergebene Sicherheitskennzeichen wie Zertifikate und Testate können Sie nachvollziehen, ob ein Cloud-Anbieter festgelegte Sicherheitsstandards erfüllt oder mit den jeweiligen gesetzlichen Regelungen des Staates übereinstimmt. Sie geben Orientierung bei der Auswahl eines Anbieters.

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.

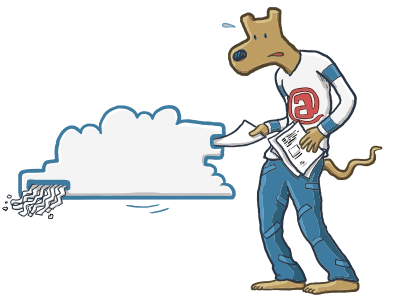
Datenverschlüsselung
Wichtige und sensible Daten sollten nur verschlüsselt in der Cloud gespeichert werden. Viele Cloud-Anbieter bieten eine Verschlüsselung der Daten in der Cloud bereits an. Allerdings können Sie die Umsetzung und tatsächliche Sicherheit dieser Maßnahmen nicht überprüfen, wenn der Schlüssel zum Entschlüsseln beim Cloud-Anbieter liegt. 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 auf Ihrem Gerät ablegen 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.

Freigabe von Daten

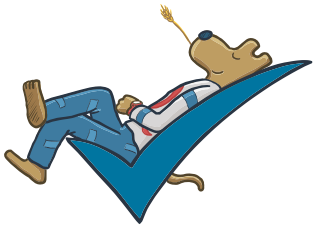
Wenn Sie Daten in der Cloud mit anderen Personen teilen möchten, wird hierzu häufig eine Freigabe per Link eingerichtet. Dabei ist zu beachten, dass jede Person, die den Link kennt, Zugriff auf die freigegebenen Daten hat. Aus diesem Grund empfiehlt es sich, Freigaben möglichst zeitlich zu begrenzen. Außerdem sollten sie immer spezifisch und restriktiv angewendet werden. Sie können beispielsweise nur die benötigte Datei freigeben und nicht den Ordner, in dem die Datei liegt. Prüfen Sie zudem die Standardeinstellungen Ihres Cloud-Dienstes und passen diese nach Ihren Bedürfnissen an. Eine gute Strategie ist es, zu Beginn möglichst defensive Einstellungen zu wählen, zum Beispiel indem Sie die Übermittlung von Daten an Dritte abschalten und nicht benötigte Funktionalitäten deaktivieren.

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. Manche Cloud-Anbieter behalten die Daten auch nach einer Kündigung oder dem Löschen noch für einige Zeit für den Fall, dass die Kündigung zurückgenommen oder ein Nutzerkonto wieder aktiviert wird. Informationen hierzu finden Sie in den AGB des Dienstleisters. Gleichzeitig kann der Anbieter endgültig gelöschte Daten in der Regel nicht wiederherstellen. Für solche Fälle können Sie sich mit einer lokalen Datensicherung absichern.



NOTIZEN



Das BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) verfolgt das Ziel, die Digitalisierung in Deutschland sicher zu gestalten. Im Sinne des digitalen Verbraucherschutzes sensibilisiert das BSI die Verbraucherinnen und Verbraucher für Sicherheitsrisiken im Cyber-Raum und die sichere Nutzung digitaler Technologien. Mit dem Informationsangebot „BSI für Bürger“ bietet es eine unabhängige und neutrale Anlaufstelle zu Fragen der Informations- und Cyber-Sicherheit.

Herausgeber
Bundesamt für Sicherheit in der Informationstechnik – BSI
53175 Bonn

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
Service-Center: +49 (0) 800 274 1000

Stand
Februar 2020

Illustrationen
Leo Leowald www.leowald.de

Artikelnummer
BSI-IFB 20/253