FILESHARING

Sicherheit geht vor

Datenaustausch-Dienste im Betrieb: Risiken im Blick behalten und professionelle Anwendungen nutzen.

Von Markus Vollmuth

Foto: Bawolxel/GettyImages.de

In Zeiten von Homeoffice und zunehmend mobilen Arbeitswelten erfreuen sich Filesharing-Dienste wie Dropbox oder Wetransfer auch bei Unternehmen steigender Beliebtheit. Denn die Mitarbeiter arbeiten vielfach mit Grafiken, Videos, Audios, Präsentationsdokumenten und Tabellenkalkulationen, die oft sehr groß sind. Das Versenden per E-Mail-Anhang kann deshalb aufgrund der begrenzten Speicherkapazitäten der Postfächer schnell zum Problem werden. Viele Beschäftigte nutzen deshalb vermehrt die Filesharing-Dienste, die allerdings oft ausschließlich für den Privatgebrauch gedacht sind – jenseits jeglicher Kontrollen und Schutzmaßnahmen der IT-Abteilung. Damit wächst die Gefahr, dass Informationen in falsche Hände gelangen. Wenn zudem personenbezogene Daten betroffen sind, bringt das zusätzlich Herausforderungen beim Datenschutz mit sich. Zu diesen Daten gehören alle Informationen, die sich auf eine natürliche Person beziehen oder zumindest beziehbar sind und so Rückschlüsse auf deren Persönlichkeit erlauben, auch wenn diese verschlüsselt übertragen bzw. gespeichert werden.

Möchten Unternehmen einen solchen Datenaustausch-Dienst nutzen, ist es erforderlich, mit diesem einen Datenschutzvertrag abzuschließen, genauer gesagt einen Auftragsverarbeitungsvertrag. Versäumt man das, kann das ein Bußgeld nach sich ziehen. Auch kann eine Übermittlung von personenbezogenen Daten an einen nicht freigegebenen Dienst eine Datenpanne darstellen. Falls es dann beim Filesharing-Dienstleister zu einem Datenleck kommen sollte, durch das personenbezogene Daten öffentlich werden, fällt das auf das Unternehmen zurück. Bei der Nutzung eines nicht in der EU ansässigen Dienstleisters darf man zudem nicht vergessen, dass es sich dabei um eine Übermittlung personenbezogener Daten in ein Drittland ohne Vertragsgrundlage handeln kann. Der Europäische Gerichtshof (EuGH) veränderte im

Sommer 2020 mit dem Schrems-II-Urteil und dem damit verbundenen Wegfall der Datenschutzvereinbarung „Privacy Shield" die Rechtsgrundlagen für den Austausch personenbezogener Daten mit den USA. Das bedeutet: Personenbezogene Daten dürfen nicht mehr ohne geeignete Garantien, die den Datenschutz sicherstellen sollen, in die USA übermittelt werden.

Probleme bei der Nutzung

Die Nutzung von externen Filesharing-Plattformen stellt aus Sicht der Informationssicherheit immer eine potenzielle Verletzung der Schutzziele „Vertraulichkeit", „Verfügbarkeit" und „Integrität" dar. Das ist beispielsweise der Fall, wenn Dienste eingesetzt werden, bei denen die Sicherheit der Datenverarbeitung unklar und teilweise zweifelhaft ist. So kann es passieren, dass Firmendaten auf beliebige Server transferiert werden, sodass eine Kontrolle durch das Unternehmen nicht mehr möglich ist. Ein weiteres Problem ist die Wiederherstellbarkeit: Filesharing-Dienste sind nicht Teil des unternehmensinternen Datensicherungskonzepts, ein Verlust von Daten kann deshalb im Regelfall nicht ausgeglichen werden. Zudem erfolgt keine zentrale Datenhaltung, sodass es zu doppelter Datenhaltung und Inkonsistenzen von Dateiversionen kommen kann.

Nicht zuletzt werden durch die Nutzung dieser Dienste Einfallstore für Phishing und Malware geöffnet. So haben IT-Sicherheitsforscher eine neue Windows-Malware, die auf den Namen „Crutch" getauft wurde, entdeckt und analysiert: „Crutch" ist eine ganze Tool-Sammlung, die dazu dient, vertrauliche Informationen von betroffenen Systemen zu kopieren und an die Cyber-Kriminellen zu schicken. Diese Informationen werden – unter Verwendung der offiziellen Dropbox-Programmierschnittstelle – an hinterlegte Dropbox-Accounts der Cyber-Kriminellen gesendet. Der hauptsächliche Grund, warum Cyberkriminelle die Dropbox-Schnittstelle nutzen, ist laut der IT-Sicherheitsforscher, dass „Crutch" durch die Nutzung freigegebener und schon verwendeter Infrastrukturen mehrere Sicherheitsmaßnahmen umgeht. Der Dropbox-Verkehr fügt sich unauffällig in den regulären Netzwerkverkehr ein und erregt dadurch relativ wenig Aufmerksamkeit.

Auf professionelle Lösungen setzen

Um Informationssicherheitsvorfälle und Datenpannen zu verhindern, muss man auf professionelle, speziell für Unternehmen konzipierte Filesharing-Lösungen zurückgreifen, denn die Nutzung externer Dienste ohne Managementfunktionen und Berechtigungskonzepte ist mit Risiken verbunden. Bei der Auswahl einer Datenaustausch-Plattform gibt es eine Reihe sicherheitsrelevanter Aspekte zu beachten. So ist eine verschlüsselte Datenübertragung und -speicherung („Data in transit" und „Data at rest") unverzichtbar. Mit Blick auf den Server-Standort ist es wichtig, dass sich dieser innerhalb von Deutschland bzw. der EU befindet. Außerdem muss man darauf achten, dass der Cloud-Dienst Möglichkeiten zur Datensicherung und -wiederherstellung anbietet. Falls die genutzte Datenaustausch-Plattform kleine solche Lösungen bereitstellt, sind zusätzlich alternative Speicher gefragt, um die Verfügbarkeit der Informationen sicherzustellen. Verschiedene Cloud-Anbieter wurden nach international anerkannten Standards zertifiziert, die einerseits allgemeine Sicherheits- und Datenschutzstandards festlegen und andererseits die Verarbeitung personenbezogener Daten in der Cloud regeln. Mit Hilfe der ISO 27017 belegen Anbieter die Sicherheit ihrer Dienstleistungen gegenüber ihren Nutzern, während sich die Zertifizierung ISO 27018 mit der sicheren Verarbeitung personenbezogener Daten befasst.

Zudem empfiehlt es sich, mit Hilfe einer Richtlinie im Betrieb festzulegen, welche Informationen durch die Nutzer wie verarbeitet bzw. freigegeben werden dürfen. Hier sind auch die externen Dienste zu benennen, die in der Firma zur Nutzung freigegeben sind. Das Unternehmen muss anschließend sicherstellen, dass diese Richtlinie auch allen Nutzern bekannt ist und dass deren Regelungen befolgt werden.

Markus Vollmuth ist Informationssicherheitsberater bei der Atarax Unternehmensgruppe in Herzogenaurach, einem Dienstleister für strategische Unternehmenssicherheit und Haftungsmanagement (www.atarax.de).

Infos zum sicheren Cloud-Computing

Einen thematischen Überblick zum Thema Cloud-Computing bietet die **„Orientierungshilfe Cloud-Computing"**, die von den Arbeitskreisen „Technik" und „Medien" der Datenschutzkonferenz erarbeitet wurde. Die rechtlichen Anforderungen und Bezüge der Orientierungshilfe entsprechen jedoch noch dem alten Datenschutzrecht, das bis 24. Mai 2018 galt (www.datenschutzkonferenz-online.de/orientierungshilfen.html, Abschnitt „2014"). Eine neue Orientierungshilfe, die die Anforderungen der Datenschutzgrundverordnung (DSGVO), insbesondere die Vorschriften zur Auftragsdatenverarbeitung (Art. 28), berücksichtigt, wird derzeit von den deutschen Datenschutzaufsichtsbehörden erarbeitet.

Zur Informationssicherheit beim Thema Cloud-Computing hat das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** ein Dossier für Anwender herausgegeben (www.bsi.bund.de, Suchbegriff „Dossier Anwender-Management"). Darüber hinaus informiert das BSI auf seiner Webseite auch allgemein zum Thema Cloud-Computing (www.bsi.bund.de/cloud).