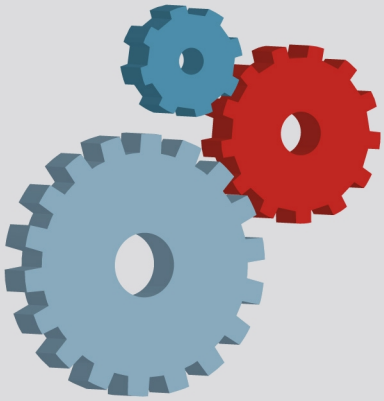
Bundesamt
für Sicherheit in der
Informationstechnik

Überblickspapier Online-Speicher



IT-Grundschutz aktuell

Was sind Online-Speicher?

Die Nutzung von Online-Speicher, oft auch Online Storage, Cloud Speicher oder Cloud Storage genannt, bietet Anwendern die Möglichkeit, Daten im Internet bzw. in einer sogenannten Cloud aufzubewahren und unabhängig von ihrem Aufenthaltsort darauf zuzugreifen.

Online-Speicher-Dienste wie z. B. Dropbox, Wuala, CloudMe, TeamDrive, Telekom Mediencenter, Microsoft Skydrive oder Google Drive erfreuen sich in den letzten Jahren, auch in Deutschland, wachsender Beliebtheit. Die Gründe für den zu beobachtenden Anstieg der Nutzerzahlen sind dabei vielfältig. Waren Online-Speicher bis vor Kurzem meist nur in den USA beheimatet, ausschließlich in englischer Sprache verfügbar oder mit hohen Kosten verbunden, existieren nunmehr auch deutschsprachige und erheblich günstigere Angebote. Die steigende Zahl der Online-Speicher-Anbieter, die ihre Dienste speziell auf Kunden im geschäftlichen Umfeld zuschneiden, lässt bereits die wachsende Bedeutung von Online-Speichern für Unternehmen und Behörden auch in der näheren Zukunft erahnen.

Die gängigen Online-Speicher-Dienste bieten in der Regel sowohl ein Programm zur Installation auf dem Rechner des Mitarbeiters als auch ein Webportal an, um direkt über das Internet auf die Daten zugreifen zu können. Die Client-Software legt dabei zumeist einen Ordner im Dateisystem des Benutzers an. Die darin befindlichen Daten werden automatisch oder manuell in den Online-Speicher übertragen. Bei weiteren Lösungen ist es dem Nutzer beispielsweise möglich, die zu übertragenden Daten einfach über den Dateimanager auszuwählen und anschließend zur Online-Speicherung freizugeben. Neben einer Client-Software und dem Zugriff über ein Web-Portal werden oftmals auch Applikationen, sogenannte Apps, für den Einsatz mit mobilen Endgeräten, wie etwa Smartphones oder Tablet-PCs, angeboten.

Wozu wird Online-Speicher genutzt?

Bei der Nutzung von Online-Speicher-Diensten kann zwischen verschiedenen Varianten unterschieden werden. Das Online-Backup, bei dem Daten einmalig oder in regelmäßigen Abständen über das Internet gespeichert werden, um nach einem Datenverlust wieder abgerufen werden zu können, stellt dabei die einfachste Form der Nutzung dar. Bei der Online-Festplatte stehen je nach Anbieter neben der reinen Datenspeicherung, meist in Form einer automatischen oder manuellen Synchronisation festgelegter Dateiordner, auch zusätzliche Funktionen zur Verfügung. Das Teilen von Daten mit Kollegen oder Geschäftspartnern, die gemeinsame Arbeit an Dokumenten sowie die Synchronisation verschiedener Endgeräte sind dabei zunehmend auch in Behörden und Unternehmen von Interesse.

Was wird in diesem Papier betrachtet?

Das vorliegende Überblickspapier richtet sich vornehmlich an Anwender von Online-Speicher-Lösungen im Behörden- und Unternehmensumfeld. In diesem Zusammenhang werden exemplarisch einige repräsentative Typen von Online-Speicher-Diensten betrachtet und hinsichtlich ihres Funktionsumfangs sowie verschiedener Sicherheitsaspekte untersucht. Zunächst werden einige allgemeine Gefährdungen betrachtet, die unabhängig vom tatsächlichen Einsatzszenario des Online-Speicher-Dienstes als relevant betrachtet werden. Um diesen Gefährdungen vorzubeugen, werden Sicherheitsmaßnahmen empfohlen, die einen möglichst sicheren Einsatz der Online-Speicher-Dienste gewährleisten sollen. Jede Institution muss jedoch auf strategischer Ebene entscheiden, ob die bestehenden Risiken bei der Nutzung von Online-Speicher-Diensten tragbar sind oder nicht. Einige Online-Speicher-Dienste bieten ein breites Spektrum an Funktionalitäten, die im Behörden- und Unternehmensumfeld eine Vielzahl von Anwendungsszenarien denkbar machen. Mit der Nutzung dieser Funktionalitäten gehen unter Umständen weitere Gefährdungen einher, die über die betrachteten allgemeinen Gefährdungen hinaus gehen. Anhand einiger typischer Einsatzszenarien werden daher zusätzliche Gefahrenpotenziale dargestellt und entsprechende Sicherheitsmaßnahmen empfohlen.

Das Überblickspapier gibt keine Empfehlungen zu Entscheidungen, deren Umsetzung tief greifenden Einfluss auf die strategische Ausrichtung der IT einer Institutionen hätte, wie dies beispielsweise beim Thema Microsoft Office 365 oder Google Docs der Fall wäre. Es kann jedoch als Hilfsmittel für solche strategischen Entscheidungen dienen.

Allgemeine Gefährdungsübersicht

Institutionen, die sich für die Nutzung von Online-Speicher-Diensten interessieren, sollten sich im Vorfeld dieser - zumeist strategischen - Entscheidung mit den möglichen Risiken auseinandersetzen, die damit einhergehen. In diesem Zusammenhang ist die wichtige Frage zu klären, welche Daten in einen Online-Speicher übertragen werden sollen bzw. dürfen und welchen Schutzbedarf diese Daten haben.

Aus dem Einsatz von Online-Speicher-Diensten kann sich für Behörden und Unternehmen eine Vielzahl von Gefährdungen ergeben. An dieser Stelle werden zunächst einige davon betrachtet, die ganz unabhängig von konkreten Anwendungsfällen auftreten können. Sie behalten ihre Relevanz auch bei der späteren Betrachtung spezifischer Einsatzszenarien.

Datenverlust

Die Geschäftsprozesse in Institutionen sind heutzutage größtenteils von Informationstechnik durchdrungen. Kommunikationsdaten, Verträge, Werbematerialien oder Konstruktionspläne liegen in vielen Fällen ausschließlich in digitaler Form vor. Für Unternehmen und Behörden sind diese Daten oftmals von großer Bedeutung. Datenverlust kann neben erheblichen finanziellen Belastungen, bis hin zur Bedrohung der Existenz, auch rechtliche Konsequenzen nach sich ziehen, wenn dadurch beispielsweise die gesetzliche Aufbewahrungsfrist für geschäftsrelevante Unterlagen nicht eingehalten wird.

Nicht-Verfügbarkeit / Diensteausfall

Ist der Zugriff auf die Daten der Institution nicht möglich, da der Online-Speicher-Dienst aufgrund eines Ausfalls des Providers oder der Internetverbindung nicht zur Verfügung steht, kann dies die Geschäftsprozesse innerhalb der Institution stören oder ganz stoppen. Wichtig sind in diesem Zusammenhang insbesondere die Verfügbarkeitsanforderungen an die betroffenen Daten. Sofern die Institution auf eine hohe Verfügbarkeit angewiesen ist, drohen bei längeren Ausfallzeiten des Anbieters finanzielle Verluste und Imageschädigungen.

Verlust der Vertraulichkeit der Daten

Neben der Verfügbarkeit des Online-Speichers und der darin abgelegten Daten hat für Unternehmen und Behörden vor allem auch die Vertraulichkeit der Informationen einen hohen Stellenwert. Gelingt es Angreifern beispielsweise, Zugang zu sensiblen Daten der Institution zu erlangen und diese z. B. einem breiteren Personenkreis zugänglich zu machen, drohen neben erheblichem Imageverlust auch rechtliche Konsequenzen und finanzielle Einbußen.

Verlust der Integrität der Daten

Bei der Übertragung von Daten, deren Bearbeitung über das Netz oder deren abschließender Speicherung können Integritätsprobleme auftreten, die bis hin zum Totalverlust führen können. Dies gilt auch für verschlüsselte Daten. Die Auswirkungen für die Institution sind ähnlich wie beim Verlust der Vertraulichkeit.

Verstoß gegen Datenschutzbestimmungen

Rechtliche Aspekte spielen für Unternehmen zudem immer dann eine Rolle, wenn personenbezogene Daten im Sinne des §3 Absatz 1 Bundesdatenschutzgesetz (BDSG) an einen Online-Speicher-Dienst übergeben werden. Eine solche Auftragsdatenverarbeitung ist, in Abhängigkeit vom tatsächlichen Speicherort der Daten, laut §11 BDSG nur unter bestimmten Voraussetzungen möglich und zudem an die Erteilung eines schriftlichen Auftrages gebunden. Bei einer Zuwiderhandlung gehen Institutionen das Risiko ein, gegen bestehendes Recht zu verstoßen und damit nicht nur ihren Ruf zu schädigen, sondern sich auch Schadenersatzansprüchen oder Bußgeldern gegenüberzusehen.

Insolvenz des Cloud Service Providers

Derzeit ändern sich die Geschäftsmodelle beim Cloud Computing rasant und auch die Anbieter wechseln. Falls ein Online-Speicher-Anbieter insolvent wird oder aus einem anderen Grund die Geschäftstätigkeit einstellt, kann dies dazu führen, dass die dort gespeicherten Daten für die Kunden ganz oder zumindest zeitweise nicht verfügbar sind und damit Geschäftsprozesse gestört werden oder ausfallen.

Unsicheres Löschen

Werden bei Vertragsende die Daten der Institution durch den Online-Speicher-Provider nicht ordnungsgemäß gelöscht, besteht die Gefahr, dass Unbefugte Zugriff auf die Daten erhalten.

Unsichere Client-Software

Sofern die Client-Software des Online-Speicher-Anbieters Schwachstellen aufweist, ist auf diesem Weg ebenfalls der Zugriff Unbefugter auf die Daten der Institution möglich.

Wie kann diesen Risiken begegnet werden?

Institutionen, die eine strategische Entscheidung für die geschäftliche Nutzung von Online-Speichern treffen, sollten ihr Augenmerk bei der Auswahl eines geeigneten Anbieters daher auf einige wichtige Punkte richten, da die Sicherheitsfunktionen von Anbieter zu Anbieter verschieden ausgestaltet sind.

Ort der Datenspeicherung

Idealerweise setzt der Anbieter des Online-Speichers seine Kunden darüber in Kenntnis, wo deren Daten tatsächlich gespeichert werden, an welchem Standort also die entsprechenden Server angesiedelt sind. Verfügt der Online-Speicher-Dienst über Standorte in unterschiedlichen Ländern, sollte es dem Kunden möglich sein, bestimmte Standorte fest auszuwählen oder auszuschließen.

Gestaltung des Vertrags

Der Vertrag zwischen dem Anbieter des Online-Speichers auf der einen Seite und der Institution auf der anderen Seite muss sich an den Anforderungen nach §11 BDSG orientieren, wenn personenbezogene Daten verarbeitet werden. Aber auch in anderen Fällen gibt diese Aufstellung eine sinnvolle Hilfestellung. Darüber hinaus sollte die Institution Wert auf eine ordentliche Verwaltung der Geschäftsbeziehung legen. Berücksichtigt man dies, wird das Risiko des Verstoßes gegen geltendes Recht bereits erheblich reduziert. Insbesondere beim Umgang mit personenbezogenen Daten empfiehlt sich jedoch zusätzlich eine genaue rechtliche Prüfung.

Vereinbarungen zur Dienstgüte (SLA)

Für Kunden, die Online-Speicher nutzen, um Unternehmens- oder Behördendaten zu speichern, sind sowohl die Verfügbarkeit des gewählten Dienstes als auch der Schutz der eigenen Daten vor Verlust, Veränderung oder Offenlegung wichtige Kriterien bei der Suche nach einem geeigneten Anbieter. Im Zusammenhang mit der Bereitstellung von IT-Dienstleistungen ist die Vereinbarung sogenannter Service Level Agreements (SLA) zwischen den Vertragspartnern eine gängige Vorgehensweise zur Sicherstellung des gewünschten Grades der Dienstgüte. Diese Praxis scheint bisher jedoch im Umfeld von Online-Speicher-Diensten noch nicht bzw. nur in wenigen Ausnahmefällen etabliert zu sein, entsprechend ist die Aushandlung von Strafzahlungen bei Nicht-Verfügbarkeiten kaum möglich. Institutionen fällt es daher schwer, sich ein Urteil darüber zu bilden, wie zuverlässig ein Online-Speicher-Dienst auf diesem Gebiet einzuordnen ist. Recherchen über die Geschäftszahlen des Anbieters, die Dauer seiner bisherigen Geschäftstätigkeit oder entsprechende Testberichte können hier beispielsweise als Anhaltspunkte herangezogen werden.

Geeignete Authentisierungsmethoden

Die Nutzung von Online-Speicher-Diensten geht in der Regel damit einher, einem Anbieter, mit dem bis zu diesem Zeitpunkt noch keine Geschäftsbeziehungen bestehen, interne Daten anzuvertrauen. Entsprechend kritisch sollten Institutionen in diesem Zusammenhang die Vertraulichkeit und Integrität der übertragenen Daten sehen und auf die Umsetzung entsprechender Schutzmaßnahmen beim gewählten Anbieter achten. Eine notwendige Sicherheitsmaßnahme, um Vertraulichkeit, Verfügbarkeit und Integrität gespeicherter Daten gewährleisten zu können, besteht in der Umsetzung geeigneter Zugangskontrollmechanismen. Bereits zu dem Zeitpunkt, wenn sich ein Kunde bei einem Online-Speicher-Dienst registriert, sollte der Anbieter hier für ein angemessenes Sicherheitsniveau Sorge tragen, indem er beispielsweise die Existenz und den Zugriff des Kunden auf die angegebene E-Mail-Adresse, die für die Registrierung verwendet wird, validiert. Außerdem sollte ein Anbieter generell dem Schutzbedarf der Kundendaten angemessene Authentisierungsmechanismen anbieten, beispielsweise Zwei-Faktor-Authentisierung. Bei Passwort-basierten Verfahren sollte unter anderem die Passwortgüte angezeigt werden und nur ausreichend starke Passwörter zugelassen werden. Der Anbieter sollte ebenfalls ein geeignetes Verfahren zum Umgang mit fehlgeschlagenen Anmeldeversuchen bzw. zur Rücksetzung von Benutzerpasswörtern im Einsatz haben. Hier bietet sich beispielsweise eine Time-Out-Funktionalität an, die einen erneuten Anmeldeversuch erst nach Ablauf einer festgelegten Zeitspanne erlaubt. Auf diesem Weg kann Angriffen entgegenwirkt werden, die auf dem Erraten des Passwortes durch Ausprobieren unterschiedlicher Varianten basieren.

Verschlüsselung der Daten

Werden schützenswerte Daten über ungeschützte Netze übertragen, muss über den Einsatz zuverlässiger Verschlüsselungsverfahren intensiv nachgedacht werden. Wenn geschäftsrelevante Daten einer Institution in Online-Speichern gespeichert werden, sollten diese auch verschlüsselt werden. Die Verschlüsselung von Daten kann dabei

- ausschließlich auf dem Transportweg (Data-in-Motion),
- am eigentlichen Speicherort der Daten (Data-at-Rest) oder
- bereits auf dem Client des jeweiligen Benutzers (Data-at-Rest)

vorgenommen werden. Welche Variante sich für den Einsatz im institutionellen Umfeld am besten eignet, hängt unter anderem vom Schutzbedarf der übertragenden Daten ab. Vertrauliche Informationen sollten in einem Online-Speicher verschlüsselt abgelegt werden. Die Verschlüsselung innerhalb der eigenen Institution erfordert ein geeignetes Schlüsselmanagement.

Verschlüsselung auf dem Transportweg

Die Verschlüsselung der Daten auf dem Transportweg wird von der überwiegenden Zahl der untersuchten Online-Speicher-Anbieter standardmäßig angeboten, ohne dass hierfür zusätzliche Kosten oder zusätzlicher Arbeitsaufwand für die Kunden entstehen. Institutionen sollten daher bei der Auswahl eines Anbieters entsprechenden Wert auf die Gewährung einer angemessenen Transport-Sicherheit legen. Zu beachten ist hierbei, dass damit lediglich ein Schutz vor unerwünschtem Zugriff auf dem Weg zwischen Institution und Dienstanbieter gewährleistet ist.

Verschlüsselung am eigentlichen Speicherort

Eine Steigerung des Sicherheitsniveaus ist durch zusätzliche Verschlüsselung der Daten am Speicherort gegeben. Allerdings ist zu beachten, dass hierbei der Anbieter für das Schlüsselmanagement verantwortlich ist und somit potenziell in der Lage ist, die Daten zu entschlüsseln. Der Anbieter sollte nachprüfbar darlegen können, wie der Zugriffsschutz gewährleistet wird und welches Sicherheitsniveau das eingesetzte Schlüsselmanagement bietet.

Verschlüsselung auf dem Client der Benutzer

Die Verschlüsselung der extern gespeicherten Daten bereits auf dem Client des Benutzers stellt die sicherste Methode zur Gewährleistung der Vertraulichkeit dar. Hierbei werden dem Anbieter eines Online-Speichers ausschließlich verschlüsselte Daten übergeben. Damit ist der Umfang und die Qualität von zusätzlich angebotenen Sicherheitsmaßnahmen zum Schutz der Vertraulichkeit beim Anbieter weniger relevant. Um die Daten vor einer externen Speicherung lokal zu verschlüsseln, muss eine entsprechende Krypto-Applikation auf dem Client installiert sein. Einige Online-Speicher-Anbieter haben eine solche Verschlüsselungsfunktionalität bereits in ihre Client-Software integriert. Bei der lokalen Datenverschlüsselung ist zu beachten, dass ein geeignetes Schlüsselmanagement erforderlich ist, um beispielsweise einen Datenaustausch mit Dritten zu ermöglichen. Zudem müssen nicht nur die genutzten kryptografischen Schlüssel sicher archiviert werden, sondern auch das genutzte Programm.

Spezifische Anwendungsszenarien

Die bisher betrachteten Gefährdungspotenziale bestehen unabhängig vom tatsächlich genutzten Funktionsumfang der gewählten Online-Speicher-Lösung. Gleiches gilt für die vorgeschlagenen Maßnahmen. Darüber hinaus birgt die Nutzung von Online-Speicher-Diensten eine Vielzahl weiterer Risiken, deren Ausprägung vom Einsatzszenario in der jeweiligen Institution abhängt. Im Folgenden werden daher verschiedene Anwendungsfälle betrachtet, wie sie im institutionellen Umfeld häufig anzutreffen sind. Anhand der aufgeführten Szenarien lassen sich sowohl potenzielle Gefährdungen als auch angemessene Schutzmaßnahmen anschaulich herausarbeiten.

Szenario: Nutzung des Online-Speichers als Backup-Lösung

Die Sicherung von wichtigen Daten mit dem Ziel, diese im Fall eines möglichen Datenverlustes zu einem späteren Zeitpunkt wiederherstellen zu können, wird allgemein mit dem Begriff "Backup" bezeichnet. Die Erstellung eines solchen Backups mithilfe eines Online-Speicher-Dienstes wird in der Regel über eine entsprechende Anwendung auf dem Client eines Benutzers initiiert. Die zu sichernden Daten werden dabei über das Internet von einem Rechner innerhalb der Institution auf einen Server des Online-Speicher-Anbieters übertragen. In Abhängigkeit des gewählten Anbieters kann der Umgang mit den übertragenen Daten dabei variieren. Ein Großteil der Anbieter unterstützt beispielsweise die Speicherung und Wiederherstellung unterschiedlicher Versionen einer zu übertragenden Datei. Bietet der Online-Speicher-Anbieter hingegen keine Versionierung von Dateien an, wird die ältere Datei ohne zusätzliche Rückfrage überschrieben und steht damit nicht mehr für eine Rücksicherung zur Verfügung. In diesem Fall erfüllt der Online-Speicher jedoch nicht die Anforderungen, die an ein Backup im Unternehmens- oder Behördenumfeld gestellt werden. Institutionen sollten daher insbesondere auf die vorhandene Versionierung der Daten achten, um dem unerwünschten Löschen älterer Datenversionen vorzubeugen.

Grundsätzlich sollte immer die Frage im Vordergrund stehen, welchen Schutzbedarf die gesicherten Daten haben, welchen gesetzlichen Verpflichtungen hinsichtlich der geschäftsrelevanten Daten eine Institution unterliegt und welche Auswirkungen der Verlust der Daten, deren Verfälschung oder ein Zugriff durch Unbefugte mit sich bringen würde.

Viele Anbieter von Online-Speicher-Diensten sind sich der Tatsache durchaus bewusst, dass Institutionen großen Wert auf die Verfügbarkeit ihrer Daten legen, und halten die Daten ihrer Kunden aus diesem Grund redundant vor. Deshalb sollten die Daten an unterschiedlichen Standorten bzw. in räumlich voneinander getrennten Rechenzentren gespeichert werden. Kommt es zu Problemen in einem Rechenzentrum, stehen die Daten in diesem Fall dennoch weiterhin in einem anderen Rechenzentrum zur Verfügung.

Unternehmen und Behörden sollten nicht nur Wert auf die sichere Speicherung ihrer Daten legen, sondern darüber hinaus auch die Umsetzung der Zugriffsmöglichkeiten auf die angelegten Benutzerkonten hinterfragen. Im Unternehmens- und Behördenumfeld sind gezielte Angriffe vorstellbar, deren Absicht darin liegt, eine Sperrung des Benutzerkontos herbeizuführen und auf diesem Weg den Zugriff auf das Backup der Daten zu verhindern. Eine solche Denial-of-Service-Attacke bedient sich dabei in der Regel unterschiedlicher Schwachstellen wie beispielsweise einer Kombination aus der automatischen Sperrung eines Benutzerkontos bei fehlgeschlagenen Anmeldeversuchen und einer nicht validierten E-Mail-Adresse. Das in diesem Zusammenhang bereits als mögliche Schutzmaßnahmen vorgestellte Time-Out-Prinzip kann einem solchen gezielten Denial-of-Service-Angriff entgegenwirken. Dabei wird das Benutzerkonto nicht vollständig gesperrt, sondern lediglich ein erneuter Anmeldeversuch für einen vorgegebenen Zeitraum unterbunden.

Nicht nur Vollständigkeit und Verfügbarkeit ihrer gesicherten Daten interessieren Institutionen, vielmehr legen sie, unter anderem zur Vermeidung rechtlicher Konsequenzen oder eines Imageverlustes, auch großen Wert auf deren Vertraulichkeit und Integrität. Die bereits beschriebenen Maßnahmen im Zusammenhang mit der Registrierung bei einem Online-Speicher-Anbieter dienen auch dem Schutz der Vertraulichkeit und Integrität der Daten, sind jedoch nicht ausreichend, um dem Großteil der bekannten Sicherheitsrisiken zu begegnen. Viele Institutionen setzen daher Verschlüsselungsverfahren ein, um das Sicherheitsniveau bei der Übermittlung und der Datenspeicherung bei externen Dienstleistern zu erhöhen. Auf die Möglichkeit, Verschlüsselung auch im Umfeld von Online-Speicher-Lösungen einzusetzen, wurde bereits oben eingegangen. An dieser Stelle wird das Thema dennoch erneut aufgegriffen, um auf die konkreten Problemstellungen beim Umgang mit unterschiedlichen Verschlüsselungsvarianten einzugehen.

Viele Anbieter von Online-Speicher-Lösungen werben mit der erhöhten Sicherheit durch den Einsatz von Verschlüsselung. Hier muss jedoch genauer analysiert werden, wie die Verschlüsselung im Einzelnen umgesetzt ist. In der Regel erfolgt nämlich lediglich die eigentliche Übertragung der Daten verschlüsselt, etwa über den Aufbau einer https-Verbindung (Hyper Text Transfer Protocol Secure). Vor und nach dem Transport liegen die Daten jedoch unverschlüsselt im Klartext vor. Einige wenige Anbieter stellen ihren Kunden, unabhängig vom Transportweg der Daten, zusätzliche Verschlüsselungsmethoden zur Verfügung. Die Verschlüsselung der Daten auf den Servern des Anbieters bietet nur Schutz der Vertraulichkeit bei einem Diebstahl der Speichermedien oder anderen direkten, unberechtigten Zugriff auf die Daten. Die Institution kann aber nicht ausschließen, dass ein Innentäter, also ein Mitarbeiter des Online-Speicher-Anbieters, Kenntnis von den entsprechenden Schlüsseln erlangt und damit auch auf die verschlüsselten Informationen zugreifen, diese verfälschen oder veröffentlichen kann. Erlangt ein Angreifer Zugriff auf die Daten, indem er die Authentisierung kompromittiert, dann ist die Verschlüsselung beim Anbieter ebenfalls wirkungslos.

Sehen Institutionen ihre Daten also als besonders schützenswert an, sollten sie diese bereits auf ihren eigenen Systemen und damit vor dem eigentlichen Datentransfer verschlüsseln.

Das Bedürfnis nach einer sicheren Methode zur Nutzung von Online-Speicher-Lösungen, gerade im Behörden- oder Unternehmensumfeld, wird vom Markt jedoch zunehmend aufgegriffen. So hat sich mittlerweile eine Reihe von Verschlüsselungslösungen etabliert, die größtenteils speziell auf die Zusammenarbeit mit Online-Speicher-Diensten abgestimmt sind. Die Programme überprüfen bereits bei der Installation, ob ein passender Ordner eines Online-Speichers existiert, und erzeugen anschließend einen entsprechenden Unterordner, in dem die verschlüsselten Dateien abgelegt werden. Institutionen, die zusätzliche Verschlüsselungssoftware einsetzen, sollten darauf achten, dass für die Anwendung ein ausreichend starkes Passwort oder anderer Zugriffsschutz gewählt wird. Zudem sollte eine Kopie der eingesetzten Softwarelösung und der zugehörigen kryptographischen Schlüssel an einem sicheren Ort hinterlegt werden, um im Falle eines vollständigen Datenverlustes innerhalb der Institution noch auf die verschlüsselten Backup-Daten des Online-Speichers zugreifen zu können. Zu diesem Zweck kann die Verschlüsselungssoftware unverschlüsselt beim Online-Speicher-Dienst gesichert werden, der Schlüssel muss selbstverständlich anders gesichert werden. Auf diesem Weg ist die Institution unabhängig davon, ob die Verschlüsselungssoftware auch nach einem längeren Zeitraum noch in einer kompatiblen Version zur Verfügung steht.

Institutionen sollten sich zudem davon überzeugen, dass die Wiederherstellung der gespeicherten Daten vom Online-Speicher fehlerfrei funktioniert, und sollten dies darüber hinaus regelmäßig testen.

Szenario: Datensynchronisation auf unterschiedlichen Endgeräten

Während die Backup-Funktionalitäten der Online-Speicher-Lösungen in der Regel lediglich auf die Speicherung von Dateien mit dem Ziel einer anschließenden Wiederherstellung abzielen, stehen Institutionen noch eine Reihe weiterer Optionen bezüglich des Einsatzgebietes von Online-Speichern zur Verfügung. Viele Unternehmen und auch Behörden setzen mittlerweile vermehrt auf den Einsatz unterschiedlicher Endgeräte, um dem wachsenden Anspruch an Mobilität, sowohl aus Sicht der Kunden, als auch vonseiten der Mitarbeiter zu erfüllen. Gerade Mitarbeiter, deren Aufgabengebiet auch längere Reisetätigkeiten mit sich bringt, nutzen oftmals verschiedene Endgeräte wie Smartphones, Tablet-PCs oder Notebooks, um auch von unterwegs auf Daten in der Institution zugreifen zu können.

Im folgenden Beispiel wird Alice betrachtet, die bei einem Unternehmen in München angestellt ist. Für den nächsten Tag ist die Vorstellung ihres Unternehmens geplant, um in Frankfurt einen neuen Kunden zu gewinnen. Um rechtzeitig beim Kunden zu sein, reist Alice bereits am Vortag an. Alice hat sich vorgenommen, die Zeit im Zug zu nutzen, um ihrer Präsentation am Notebook den letzten Schliff zu geben. Am Vormittag hat Alice die Präsentation an ihrem Arbeitsplatzrechner im Büro erstellt und in dem Ordner abgelegt, der automatisch mit dem Online-Speicher-Dienst synchronisiert wird, mit dem der Arbeitgeber von Alice einen Vertrag geschlossen hat. Alice kann die Präsentation nun ganz bequem von unterwegs auf ihrem Notebook aufrufen und weiter daran arbeiten. Um verloren gegangene oder defekte USB-Speicher oder das versehentliche Kopieren einer veralteten Version der Präsentation muss sich Alice nun keine Gedanken mehr machen. Selbst wenn ihr Notebook beim Kunden vor Ort aufgrund fehlender Kompatibilität oder eines Defektes nicht eingesetzt werden kann, steht Alice die Präsentation über das Web-Portal des Online-Speicher-Dienstes zur Verfügung.

Die Vorteile von Online-Speicher-Diensten im Zusammenhang mit dem gezeigten Szenario liegen auf der Hand, doch ähnlich wie die Backup-Funktionalität birgt auch der Einsatz auf unterschiedlichen Endgeräten Risiken. Auf bestehende Gefährdungen und umzusetzende Schutzmaßnahmen beim Einsatz mobiler Endgeräte soll an dieser Stelle nicht ausführlich eingegangen werden. Am Beispiel von Smartphones wurden bereits Maßnahmen zur sicheren Nutzung im institutionellen Umfeld in einem anderen Überblickspapier beschrieben. Im Zusammenhang mit der Nutzung von Online-Speicher-Lösungen gilt es, neben der generellen Einsatzfähigkeit auf mobilen Plattformen noch einige weitere Aspekte zu beachten. So bieten beispielsweise nicht alle Anbieter von Online-Speichern ihre Applikationen bereits für alle verbreiteten Plattformen (unter anderem Windows, Mac OS, Linux, iOS, Android oder Windows Phone) an. Daher sollte bei der Auswahl eines Anbieters darauf geachtet werden, dass die Applikationen mit den in der Institution eingesetzten Geräten und Betriebssystemen kompatibel sind.

Mobile Endgeräte verfügen nicht in jedem Fall über die Möglichkeit, gespeicherte Daten zu verschlüsseln. Geht ein Gerät mit unverschlüsselten Daten verloren, besteht aber nicht nur die Gefahr, dass ein Unbefugter auf die auf dem Gerät gespeicherten Daten zugreift, sondern auch auf das zugehörige Konto beim Online-Speicher-Anbieter. Nicht selten erfolgt die Anmeldung beim Online-Speicher-Konto automatisch bei der Inbetriebnahme des Endgerätes, sodass der Besitzer auch ohne Eingabe von Anmeldeinformationen Zugriff auf die online hinterlegten Daten erlangt. Um dieser spezifischen Gefährdung entgegenzuwirken, sollten Institutionen bei der Auswahl des Online-Speicher-Dienstes darauf achten, dass Applikationen für mobile Endgeräte nicht zwangsläufig eine automatische Anmeldung beim Online-Speicher durchführen. Sollte dennoch eine solche Single-Sign-On fähige Lösung gewählt werden, ist diese lediglich in Kombination mit einer Zwei-Faktor-Authentisierung oder bei vollständiger Verschlüsselung der Daten auf dem Endgerät zu empfehlen. Eine bewusste Anmeldung des Mitarbeiters durch die Eingabe seiner Benutzerkennung und des zugehörigen Passwortes ist hier vorzuziehen. Daneben bieten einige Online-Speicher-Dienste die Option, zugelassene Geräte für eine Datensynchronisation mithilfe eines Webportals zu verwalten. Bei Verlust eines Gerätes kann auf diese Weise die weitere Nutzung des Online-Speichers von diesem Gerät aus unterbunden werden.

Neben den bereits genannten Schutzmaßnahmen kommt den Mitarbeitern eine besondere Verantwortung für die Sicherheit der Daten der Institution zu. Daher ist es wichtig, die Mitarbeiter regelmäßig für die erforderlichen Sicherheitsmaßnahmen zu sensibilisieren und sie immer wieder über aktuelle Risiken zu informieren.

Szenario: Teilen von Dateien

Die bisher betrachteten Anwendungsfälle basieren auf der Nutzung des Online-Speichers durch einen einzelnen Mitarbeiter bzw. mithilfe eines einzelnen Benutzerkontos. Die Mehrzahl der Online-Speicher-Dienste ermöglicht darüber hinaus allerdings auch den Zugriff mehrerer Benutzer auf zuvor hinterlegte Daten. Im folgenden Beispiel spielt es keine Rolle, ob die zusätzlichen Nutzer selbst über ein Konto beim Online-Speicher-Anbieter verfügen, da der Zugriff auf die entsprechenden Daten meist mithilfe eines zuvor generierten Links über das Internet erfolgt.

Zur Anwendung gelangt ein solches Szenario beispielsweise im Bereich der wissenschaftlichen Zusammenarbeit, wenn unterschiedlichen Benutzern große Datenmengen zur Verfügung gestellt werden sollen. Die Verfügbarkeit und die Integrität der Daten spielen dabei eine größere Rolle als deren Vertraulichkeit. Dementsprechend setzt der Zugriff auf die Daten keine starke Authentisierung des Nutzers voraus und auch die Nachvollziehbarkeit erfolgter Zugriffe, wie sie beispielsweise durch die Erzeugung von Log-Dateien gewährleistet werden kann, ist nicht zwingend erforderlich.

Dennoch sollten auch in diesem Anwendungsfall Sicherheitsaspekte beachtet werden. Um die Integrität der zur Verfügung gestellten Daten gewährleisten zu können, sollte zumindest sichergestellt sein, dass Dateien zwar mithilfe des übersandten Links online eingesehen, jedoch nicht verändert werden können. Sofern die Veränderung von Dateien notwendig ist, müssen diese zunächst heruntergeladen werden, um eine lokale Bearbeitung zu ermöglichen. Neben der Integrität der Daten spielt im dargestellten Beispiel vor allem deren Verfügbarkeit eine Rolle. Anders als beim Backup von Unternehmens- oder Behördendaten muss hier die Möglichkeit des Einsatzes unterschiedliche Betriebssysteme oder Internet-Browser berücksichtigt werden. Bei der Auswahl eines geeigneten Online-Speicher-Dienstes ist zu prüfen, ob der Zugriff auf Daten die Installation

einer Client-Software voraussetzt und inwiefern das eingesetzte Webportal an einen bestimmten Browser bzw. an eine bestimmte Version eines Browsers gekoppelt ist. Muss der Benutzer eine Software auf seinem Client installieren, muss geprüft werden, ob die Software mit den unterschiedlichen Betriebssystemen kompatibel ist.

Der Link, der den Benutzer zu einer geteilten Datei führt, wird typischerweise mittels E-Mail versendet. Fängt ein Angreifer diese E-Mail ab, erhält er unter Umständen nicht nur Zugriff auf die geteilte Datei, sondern auch auf den Benutzernamen des Versenders. Informationen über den registrierten Nutzer des Online-Speicher-Dienstes sollten daher nicht aus generierten Verweisen auf geteilte Dateien extrahiert werden können. Gleiches gilt für Fehlermeldungen, wie sie etwa beim Verweis auf eine nicht (mehr) existente Datei ausgegeben werden.

Szenario: Gemeinsames Arbeiten an Dateien

Die überwiegende Zahl der Online-Speicher-Dienste ermöglicht nicht nur das soeben beschriebene Teilen von Dateien, sondern darüber hinaus auch noch die Möglichkeit, gemeinsam an gespeicherten Dateien zu arbeiten. Von großem Nutzen ist diese Möglichkeit beispielsweise im Zusammenhang mit der projektbasierten Zusammenarbeit eines räumlich verteilten Teams.

Zur Veranschaulichung wird ein Szenario mit Alice und Bob betrachtet, die beide beim selben Unternehmen angestellt, jedoch an unterschiedlichen Standorten tätig sind. Für ein Projekt müssen beide gemeinsam einige Dokumente bearbeiten. Bisher haben Alice und Bob die Dateien per E-Mail ausgetauscht, sie lokal bearbeitet und anschließend die veränderte Version wieder versandt. Häufig traten in diesem Zusammenhang Probleme bei der gemeinsamen Bearbeitung und nachfolgenden Zusammenführung von Dateien auf, die durch den Einsatz eines geeigneten Online-Speicher-Dienstes hätte umgangen werden können. Durchgeführte Änderungen an einem Dokument werden automatisch synchronisiert und stehen dem anderen damit schnell zur Verfügung. Arbeiten mehrere Nutzer gleichzeitig an einer Datei, wird dies vom Online-Speicher erkannt und ein entsprechender Hinweis ausgegeben.

Um eine solche Form der Zusammenarbeit sicher gestalten zu können, sollte der gewählte Online-Speicher-Dienst einige Voraussetzungen erfüllen. Im Gegensatz zur im Vorfeld beschriebenen Kooperationsform kommt der Vertraulichkeit und Integrität der geteilten Informationen hier eine größere Bedeutung zu. Der Zugriff auf eine Datei darf daher nur nach einer vorherigen Anmeldung des Benutzers beim Online-Speicher-Dienst gewährt werden. Einige Anbieter stellen außerdem umfangreiche Möglichkeiten der Benutzerverwaltung und Rechtevergabe zur Verfügung. Institutionen können beispielsweise Mitarbeiter in Teams gruppieren und ihnen damit Zugriff auf bestimmte Daten ermöglichen oder ihnen individuelle Berechtigungen für den Zugriff auf online gespeicherte Informationen zuweisen. Sofern der Speicherbedarf einzelner Mitarbeitergruppen sich stark unterscheidet, sollten Institutionen darauf achten, Kapazitäten individuell zuweisen und überwachen zu können. Ein Großteil der Online-Speicher-Anbieter mit Lösungen, die auf Unternehmen oder Behörden ausgerichtet sind, bietet diese Möglichkeit bereits an. Die Nachverfolgung tatsächlich erfolgter Zugriffe mit Hilfe erzeugter Log-Dateien wird bisher jedoch noch nicht von den Online-Speicher-Diensten unterstützt.

Fazit

Daten einer Institution unterliegen einem anderen Schutzbedarf als Daten privater Anwender. Der Verfügbarkeit der Daten und deren Schutz vor Verlust der Integrität oder der Vertraulichkeit kommt somit eine viel größere Bedeutung zu. Die Entscheidung zum Einsatz von Online-Speicher-Lösungen in Unternehmen oder Behörden findet daher in der Regel auf strategischer Ebene statt.

Institutionen sollten ihre Entscheidungen im Zusammenhang mit Online-Speicher-Lösungen auch gegenüber ihren Mitarbeitern in geeigneter Form kommunizieren und ihnen somit die Möglichkeit geben, Kenntnis über die Rahmenbedingungen der Nutzung von Online-Speichern oder auch ein generelles Verbot solcher Dienste zu erlangen.

In diesem Papier wurden eine Reihe von denkbaren Anwendungsfällen für den Einsatz von Online-Speicher-Lösungen im Unternehmens- und Behördenumfeld aufgezeigt. Die Einbindung unterschiedlicher Endgeräte und der damit verbundene schnelle und ortsunabhängige Zugriff auf die Daten einer Institution sowie sinkende Preise und eine breitere Palette von Angeboten lassen diese dabei zunehmend attraktiver werden.

Doch bei alle gegebenen Vorteilen sollten Unternehmen und Behörden auch die wichtigen Aspekte der Sicherheit ihrer Daten nicht aus den Augen verlieren. Gerade die Einfachheit und Unauffälligkeit, mit der sich Online-Speicher-Dienste in die IT-Systeme der Mitarbeiter integrieren, bergen die Gefahr, dass diese die notwendige Sorgfalt beim Umgang mit schützenswerten Daten außer Acht lassen. Zudem sollten sich die Verantwortlichen einer Institution immer vor Augen halten, dass sie ihre Daten einem Dritten übergeben, zu dem ein gewisses Vertrauensverhältnis existieren sollte.

An das BSI werden häufig Wünsche für IT-Grundschutz-Bausteine herangetragen, die aus verschiedenen Gründen nicht zeitnah realisierbar sind. Meist werden zu aktuellen neuen Vorgehensweisen, Technologien oder Anwendungen spezifische Sicherheitsempfehlungen benötigt, mit denen auf IT-Grundschutz basierende Sicherheitskonzepte schnell und flexibel erweitert werden können. Mit den Überblickspapieren sollen zeitnah zu aktuellen Themen Lösungsansätze präsentiert werden. Kommentare und Hinweise richten Sie bitte an: grundschutz@bsi.bund.de