WORAUF UNTERNEHMEN BEI DER AUSWAHL VON CLOUD-ANBIETERN ACHTEN SOLLTEN:

Fünf Tips für klare Sicht in der Cloud

Die Nutzung von Cloudservices ist für viele Unternehmen eine betriebliche Notwendigkeit geworden. Werden personenbezogene Daten in die Cloud ausgelagert, gelten bei der Auswahl eines Cloudanbieters jedoch besondere Vorgaben durch die DSGVO. Um die Vorgaben bestmöglich zu erfüllen, sollten Unternehmen einige wesentliche Punkte beachten ... *von Michael Scheffler*

Bild: Bitglass

Michael Scheffler, Regional Director Central and Eastern Europe, Bitglass

Für Cloudservices gilt das Modell der Shared Responsibility, das heißt, daß sowohl der Anbieter als auch das nutzende Unternehmen für die Datensicherheit verantwortlich sind. Während der Nutzer dafür zu sorgen hat, daß die Datennutzung in der Cloud sicher ist, hat der Cloud-Anbieter für die Sicherheit der bereitgestellten Infrastruktur zu garantieren. Werden für personenbezogene Daten Cloudservices genutzt, verlangt die DSGVO von den Nutzern, sich zu vergewissern, daß der Cloud-Anbieter seiner Verantwortung in ausreichendem Maße nachkommt. Unternehmen müssen also sicherstellen, daß das Datenschutzniveau, das sie ihren Kunden zusichern, auch jenseits ihrer eigenen Infrastruktur in der Cloud aufrechterhalten bleibt. Bei Einführung der DSGVO war vorgesehen, mit Hilfe von Gütesiegeln Unternehmen die Auswahl von Cloud-Anbietern zu erleichtern. Standards für Zertifizierer werden gegenwärtig allerdings erst vom Europäischen Datenschutzrat erarbeitet. Dennoch entbindet ein Gütesiegel die Unternehmen nicht von ihrer Verpflichtung zur gewissenhaften Überprüfung der Sicherheitsmaßnahmen des Cloud-Anbieters. Das dient dazu, klare Verantwortlichkeiten zu schaffen, damit im Ernstfall die Zuständigkeiten und daraus resultierenden Verpflichtungen geklärt sind.

Ein guter Anhaltspunkt, um eine erste Auswahl an geeigneten Cloud-Anbietern zu treffen, sind derzeit die ISO-Zertifizierungen 27001 und 27017, die sich am IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) orientieren. Um darüber hinaus ihrer Prüfpflicht nach DSGVO-Gesichtspunkten nachzukommen, müssen Unternehmen ihre eigenen Datenschutzrichtlinien mit denen der in Frage kommenden Cloud-Anbieter abgleichen. Dabei sollten insbesondere die folgenden Punkte beachtet werden:

Standort der Datenverarbeitung, -speicherung und -sicherung

Der Firmenstandort eines Anbieters sagt nicht zwangsläufig aus, daß eben dort auch der Cloudservice gehostet wird und somit die Verarbeitungstätigkeiten stattfinden. Nach DSGVO-Aspekten ist es in diesem Zusammenhang wichtig, zu ermitteln, ob die Daten im EU-Raum oder außerhalb davon verarbeitet, gespeichert und gesichert werden. Ist letzteres der Fall, muß der Cloud-Nutzer prüfen, ob die Möglichkeiten zur Durchsetzung ihrer Datenschutzrechte bei Kunden im entsprechenden Land dieselben sind wie innerhalb der EU. Für den Cloudanbieter gibt es diesbezüglich verschiedene Möglichkeiten, dies nachzuweisen, beispielsweise durch eine entsprechende von der EU genehmigte Zertifizierung oder eine offizielle Stellungnahme der zuständigen Aufsichtsbehörden.

Aktueller Malware-Schutz

Der Cloud-Anbieter sollte nachweisen können, daß er über einen geeigneten Virenschutz verfügt, der auch die Blockierung und Entfernung von noch unbekannter Malware ermöglicht – also idealerweise verhaltensbasiert arbeitet. Überaus fortschrittlich wäre es, wenn der Cloudprovider auch Malware-Schutzfunktionen für Daten in der Cloud und während des Uploads bieten kann. Weiterhin sollte mit dem Hersteller der Software eine mindestens tägliche Aktualisierung vereinbart sein.

Verfahrensregelung bei Sicherheitsvorfällen

Ein überaus wichtiges Kapitel ist die Verfahrensregelung bei Sicherheitsvorfällen. Der Cloud-Anbieter

muß darlegen, innerhalb welcher Fristen und in welchem Umfang er Auskunft über potentielle Datenverluste geben kann und ob diese zeitgleich an Nutzer und Aufsichtsbehörden gegeben werden. Anhand dessen sollten Cloud-Nutzer ihre eigenen internen Prozesse überprüfen, um sicherzustellen, daß Kunden und gegebenenfalls Aufsichtsbehörden innerhalb der gesetzlichen Frist von 72 Stunden informiert werden. Sofern noch nicht vorhanden, sollte für Cloud-Sicherheitsvorfälle ein unternehmensinterner Ablaufplan ausgearbeitet werden, in welchem alle nötigen Schritte und die erforderlichen beteiligten Personen festgelegt werden.

Datensicherung und Wiederherstellungsmechanismen

Cloud-Nutzer müssen sich vergewissern, daß die Vorgaben, die sie in ihrer Datenschutzerklärung ihren Kunden zusichern, auch in dem Vertrag mit dem Cloud-Anbieter abgebildet sind. Dafür hat der Cloud-Anbieter alle organisatorischen und technischen Verfahren für regelmäßige Backups und die Wiederherstellung von Daten bereitzustellen, zu dokumentieren und regelmäßig zu kommunizieren. Dies gilt auch für die Seite des Cloudanbieters. Außerdem muß er bei Vertragsabschluß dem Nutzer gegenüber erklären, daß ausschließlich autorisiertes Personal Zugriff auf die Daten hat. Dabei sollten sich Nutzer auch darauf beschränken, dem Anbieter maximal lesenden Zugriff einzuräumen.

Cloud-Anbieter und Subunternehmer

Bei Vertragsabschluß sollten Cloud-Nutzer in Erfahrung bringen, ob der Anbieter für bestimmte Cloudinstanzen mit Subunternehmen zusammenarbeitet. Ist dies der Fall, ist weiterhin zunächst zu klären, ob diese im selben geographischen Gebiet operieren wie der beauftragte Anbieter. Falls dies nicht zutrifft, muß nachgewiesen werden, ob auch in der entsprechenden Lage dort sichergestellt ist, daß dasselbe Datenschutzniveau wie im EU-Raum herrscht. Weiterhin muß auch die Erklärung eingeholt werden, daß der Subunternehmer alle vertraglich betroffenen Vereinbarungen zwischen Anbieter und Nutzer einhält. Ist dies nicht gegeben, wäre der Vertragsabschluß hinfällig.

Für optimale Datensicherheit: Was Cloud-Nutzer tun können

Insgesamt müssen Cloud-Nutzer sicherstellen, daß die von ihnen erhobenen personenbezogenen Daten über den gesamten Verarbeitungszyklus hinweg gesichert sind. Damit auf beiden Seiten die Maßnahmen perfekt ineinandergreifen, sollten Unternehmen dafür sorgen, daß ihre Daten in der Cloud geschützt sind. Mit Verschlüsselungstools können sie dafür sorgen, daß diese nicht zur Beute unbefugter Dritter werden. Dies bietet einen weiteren Vorteil: Gehen Daten auf dem Weg in die Cloud verloren, ist nach derzeitiger Auslegung der DSGVO kein meldepflichtiger Vorfall entstanden, da erbeutete Daten in verschlüsselter Form für die Diebe wertlos sind – gesetzt den Fall, es wurden nicht auch noch die erforderlichen Schlüssel entwendet. Allerdings lautet die Empfehlung des Gesetzgebers, in regelmäßigen Abständen zu überprüfen, ob der verwendete Verschlüsselungsalgorithmus neuesten Anforderungen entspricht. Kommt es mit einem veralteten Algorithmus zu einer Sicherheitspanne mit Datenverlust, trifft den Cloud-Nutzer womöglich eine Mitschuld. Der gegenwärtig höchste Standard ist der AES-256 (Advanced Encryption-Standard). Dieser nutzt 256-Bit-Schlüssel für die Chiffrierung von Daten. Ein ebenso langer Initialisierungsvektor sorgt dafür, daß auch in umfangreichen Datenmengen ein ausreichendes Maß an Zufälligkeit herrscht und der Datensatz nicht geknackt werden kann. Darüber hinaus sollten die Schlüssel ausschließlich unternehmensintern, durch einen beschränkten Personenkreis generiert und verwaltet werden.

Da zahlreiche Angriffsversuche häufig Social Engineering-Taktiken am Endpoint anwenden, um Zugriff auf möglichst viele Anwendungen und Daten zu erhalten, ist es darüber hinaus sinnvoll, das Sicherheitsbewußtsein der Unternehmensmitarbeiter regelmäßig zu schulen. Auf diese Weise wird das Bewußtsein für die Sicherheit von Daten nach und nach ein Bestandteil der Unternehmenskultur, der sämtliche Ebenen durchdringt. Dies trägt langfristig mit dazu bei, die rechtlichen Pflichten nach DSGVO-Vorgaben mit geringem Aufwand einhalten zu können. <<