Cloud-Dienste: Die richtige Verschlüsselung ist entscheidend

Früher wurden Daten primär in der IT-Umgebung des eigenen Unternehmens verarbeitet, gehalten und gesichert. Heute liegt die Lösung für viele IT-Bedürfnisse in der Cloud – die Datenhaltung ist einfach, leicht zugänglich, skalierbar, günstig und überall verfügbar. Mit der Auslagerung der Daten in die Cloud vertraut man jedoch gleichzeitig einem Dritten die wichtigsten Informationen des Unternehmens an. Um diese zu schützen, bieten sich Verschlüsselungssysteme an.

Bei der Nutzung einer Cloud besteht (ähnlich wie bei der eigenen IT-Infrastruktur) die Gefahr, dass sich Dritte unbefugten Zugriff auf die Daten in der Cloud beschaffen. Zum anderen birgt aber auch der Cloudanbieter selbst ein gewisses Risiko in sich.

Dieses Risiko muss sich dabei nicht zwangsläufig aus einem vorsätzlichen und delinquenten Verhalten ergeben (z. B. Entwendung und Verkauf der Daten an Wettbewerber), sondern kann sich auch aus gesetzlichen Bestimmungen entwickeln. Beispielsweise erwähnt sei hier der Clarifying Lawful Overseas Use of Data Act, kurz „CLOUD Act" oder grob ins Deutsche übertragen „Gesetz über die rechtmäßige Nutzung von Daten im Ausland". Als US-amerikanisches Gesetz ist es oft nur Experten bekannt, obwohl es eine extraterritoriale Auswirkung entfaltet und demnach auch für Europa und die DACH-Region von Interesse ist. Der „Cloud Act" räumt den US-Behörden unter bestimmten Voraussetzungen die Möglichkeit ein, dass amerikanische IT-Dienstleister ihnen einen Zugriff auf gespeicherte Daten geben müssen, auch wenn die Speicherung der Daten nicht in den USA erfolgt. Durch die bestehenden europäischen oder auch nationalen Datenschutzregelungen wäre die Übermittlung von Daten, die in der EU gespeichert wurden, an die USA nicht DSGVO-konform und rechtswidrig. Dennoch gibt es Fälle, in denen die US-Regierung die Herausgabe von Daten forderte und die Herausgabe auch erfolgt ist.

Oft sind sich die Nutzer der Cloud gar nicht im Klaren darüber, dass sie personenbezogene Daten oder streng vertrauliche Sachinformationen einem Dritten zur Aufbewahrung in der Cloud übergeben. Die Cloud ist von außen vor dem unbefugten Zugriff geschützt, aber was ist eigentlich mit dem Anbieter der Cloud? Dieser hat den passenden Schlüssel, um auf die Daten zuzugreifen. Das ist in etwa so, wie wenn Sie Ihr abgeschlossenes Tagebuch einem Fremden zur Aufbewahrung überlassen und ihm nicht nur das Tagebuch, sondern auch den Schlüssel dafür übergeben. Würden Sie das tun? Eben! Eine Lösung dafür kann beispielsweise die sog. Verschlüsselung oder auch englisch „Encryption" sein. Damit übergeben Sie den Dritten das abgeschlossene Tagebuch zur Aufbewahrung, den Schlüssel selbst behalten Sie aber.

© imago images / Ikon Images

Daten in der Cloud: Ihr Schutz ist entscheidend.

Finden sich in den Daten auch personenbezogene Daten, die in die Cloud verlagert werden sollen, dann müssen die Anforderungen der verschiedenen datenschutzrechtlichen Bestimmungen beachtet werden. Diese Bestimmungen fordern grundsätzlich, dass personenbezogene Daten durch sog. „technische und organisatorische Maßnahmen" besonders geschützt werden.

Dabei ist der Entwicklungsstand der IT, die Menge der Daten und die Art und der Zweck der Datenverarbeitung zu berücksichtigen. Partiell wird die Möglichkeit der Verschlüsselung explizit im Gesetz genannt: Die EU-DSGVO nennt die Verschlüsselung ausdrücklich in Art. 32 Abs. 1 EU-DSGVO. Das BDSG führt die Verschlüsselung in § 22 Abs. 2 Nr. 7 „Verschlüsselung personenbezogener Daten" auf. Für Österreich wird die Verschlüsselung im neu überarbeiteten DSG in Art. 2 § 7 Abs. 5 genannt. Das aktuell gültige Schweizer DSG enthält noch keine entsprechende Bestimmung, jedoch ist es sehr wahrscheinlich, dass insbesondere die demnächst ebenfalls revidierte VDSG (Verordnung zum Bundesgesetz über den Datenschutz), die bereits aktuell in Art. 9 sehr detaillierte Vorgaben bzgl. der technischen und organisatorischen Maßnahmen bei der automatisierten Bearbeitung von Personendaten macht, auch die Verschlüsselung mit aufnehmen könnte.

Alle gängigen Verfahren bieten entweder einen Schutz für das Speichern oder das Übermitteln von Daten. Der potenzielle Schwachpunkt liegt beim Übergang von einer Umgebung in die andere. Wenn es darum geht, Daten von ihrer Generierung bis zu ihrer Nutzung lückenlos zu schützen, so deckt nur das formatbewahrende, datenzentrische Verfahren diese Anforderung ab.

Bei der Wahl einer technischen Verschlüsselung stehen für Unternehmen zwei Aspekte im Fokus. Zunächst muss sichergestellt sein, dass die Verschlüsselung den Anforderungen des Datenschutzkonzepts gerecht wird, damit im Falle einer Überprüfung keine Buße droht. Bei der Auswahl kann es hilfreich sein, sich an der technischen Richtlinie „Kryptographische Verfahren: Empfehlungen und Schlüssellängen (BSI TR-02102)" des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu orientieren. Zudem muss das Unternehmen in der Lage sein, das Verschlüsselungsverfahren und seine Komponenten in die eigene Datenverarbeitungskette zu integrieren.

Anja Schmitz und Thomas Ducret

Anja Schmitz

Anja Schmitz ist Juristin und Senior Consultant sowie Partner der Projektas GmbH, mit Sitz in Zug/Schweiz. Sie ist spezialisiert auf die Themen Corporate Governance, Compliance und Datenschutz sowie dem Business Continuity Management. Ein Schwerpunkt ihrer Arbeit liegt in der Management-Beratung und in der Projektleitung.

Thomas Ducret

Thomas Ducret ist Ingenieur, Senior Consultant und ebenfalls Partner der Projektas GmbH. Er erbringt Beratungsleistungen in Industrie, Bankenumfeld und öffentlicher Verwaltung für das Suchen, Klassifizieren und Verschlüsseln von Daten. Zudem ist er Projektleiter für die Implementation von IT-Lösungen und das IT Service Management.