Datenmanagement, Cloudcomputing und Sicherheit I

Das Cloud Computing und seine Tücken

Die Digitalisierung macht vor keinem Unternehmen halt. Vermehrt werden dabei sogenannte «Clouds» verwendet. Damit soll eine jederzeitige, ortsunabhängige Zugänglichkeit und Verarbeitung der digitalen Daten gewährleistet werden. In diesem Zusammenhang ist ein besonderes Augenmerk auf die Sicherheit der digitalen Daten zu werfen.

› Dr. Davide Pinelli, Dr. Markus Kaufmann

Der Markt bietet unzählige Mittel an, um Kommunikation, Verarbeitungsvorgänge oder Ablagemechanismen digitaler Daten zu vereinfachen. Im vorliegenden Artikel wird das Hauptaugenmerk auf das «Cloud Computing» gelegt. Dementsprechend werden die tatsächlichen und rechtlichen Risiken für das Verarbeiten von Daten mittels Cloud Computing beleuchtet und Massnahmen präsentiert, mit welchen solche Risiken minimiert werden können.

Cloud Computing: die Vorteile

Das amerikanische National Institute of Standards and Technology (NIST) definierte das Cloud Computing als einen Ansatz, um den allgegenwärtigen und bequemen Netzwerkzugriff on-demand auf einen gemeinsamen Pool konfigurierbarer Rechnerressourcen (beispielsweise Netzwerke, Server, Speichersysteme etc.) zu ermöglichen, die mit geringstem Managementaufwand schnell bereitgestellt und freigegeben werden können. Die Cloud ist also eine Infrastruktur, welche auf äusserst effiziente Weise Daten abspeichert und für den Nutzer über das Internet bereitstellt.

Es gibt verschiedene Arten des Cloud Computing: das sogenannte Infrastructure as a Service (IaaS), die Platform as a Service (PaaS) oder das Software as a Service (SaaS). Beim SaaS wird die Software vom Provider als Dienstleistung online bereitgestellt. Der grösste Vorteil, welchen das Abspeichern von Daten in der Cloud bietet, ist der standort- und zeitunabhängige Datenzugriff: Mittels einer Internetverbindung kann jederzeit und von überall auf die Firmendaten zugegriffen werden, was eine erhebliche Erleichterung des Geschäftsalltags darstellt. Zudem entfallen die Evaluationskosten bezüglich Anschaffung, Pflege und Wartung neuer IT-Systeme. Trotz dieser Vorteile, welche das Cloud Computing unbestrittenermassen bereithält, darf nicht darüber hinweggesehen werden, dass ihre Anwendung auch Risiken hat.

Die Risiken

Der Anwendungsbereich des Cloud Computings umfasst namentlich die Datenspeicherung, die Bereitstellung dieser Daten sowie der Datenaustausch über Mailservices. Dabei werden insbesondere Daten verarbeitet, welche empfindliche Informationen über Geschäftsgeheimnisse beispielsweise in Form von Forschungs- oder Kundendaten beinhalten und deren Preisgabe, Beschädigung oder Zerstörung zu einem erheblichen Schaden für das jeweilige Unternehmen führen würde.

Internetkriminalität, «schlechte» Mitarbeiter, Erdrutsche

Die Cyberkriminalität hat in den letzten Jahren stets zugenommen. Davon sind vermehrt auch die Schweizer KMU betroffen. Gemäss einer Umfrage der Hochschule Luzern vom November 2017 waren rund 40 Prozent der Unternehmen kürzlich einem Cyberangriff ausgesetzt, sei es durch Hacking von E-Mails oder Schäden durch eine Malware. Die Internetkriminellen agieren professioneller und effizienter mit neuen schädlichen Programmen. Sie erpressen Gelder, spionieren und zerstören Daten auf ihrem Streifzug durch die digitale Datenwelt.

Die Daten in der Cloud sind zwar verschlüsselt, doch gelangen immer wieder ungewollt Daten in die Hände von Unbefugten. Zum einen geschieht dies durch Hackerangriffe, zum anderen wenn die Software des Cloud-Anbieters Sicher-

heitslücken aufweist oder wenn menschliche Fehler die ungewollte Datenfreigabe begünstigen, indem beispielsweise ein Mitarbeiter seinen Zugangsschlüssel zur Cloud unbefugten Personen preisgibt oder ungenügend sichert, sei dies nun gewollt oder ungewollt.

Zuletzt sind ebenso natürliche Einflüsse wie Feuer, Erdrutsche et cetera nicht ausser Acht zu lassen, durch welche ein Server eines Cloud-Anbieters bzw. die darauf gespeicherten Daten eines Unternehmens zerstört werden können.

Rechtliche Risiken: das Schweizer Recht

Gemäss Art. 1 des Bundesgesetzes über den Datenschutz (DSG) bezweckt dieses Gesetz den Schutz der Persönlichkeit und der Grundrechte, momentan sowohl von natürlichen als auch von juristischen Personen, über die Daten bearbeitet werden. Das sich in Revision befindliche Datenschutzgesetz wird jedoch nur noch Daten von natürlichen Personen schützen. Fallen solche Daten in die Hände von Unbefugten, kann dies bei der Verletzung von Sorgfaltspflichten im Zusammenhang mit dem Schutz dieser sensiblen Daten als Persönlichkeitsverletzung im Sinne des Datenschutzgesetzes qualifiziert werden, was existenzgefährdende, finanzielle und gravierende Reputationsschäden sowie strafrechtliche Folgen nach sich ziehen kann. Hinzu kommt, dass die verschiedenen Cloud-Anbieter zum Teil besondere

Verantwortlichkeitsbestimmungen in ihren allgemeinen Geschäftsbedingungen besitzen, die ihre Haftung zum Beispiel bei Datenverlustvorfällen erheblich einschränken.

So heisst es in den allgemeinen Geschäftsbedingungen eines Schweizer Cloud-Anbieters: «(…) Insbesondere haftet xxx in keinem Fall für indirekte oder unmittelbare Schäden, für entgangenen Gewinn, für Schäden aus Betriebsunfällen, Schäden aus Datenverlust oder Schäden durch Schadsoftware (Viren, Trojaner, etc.).»

Die europäische Datenschutz-Grundverordnung (EU-DSGVO)

Die Schweizer Exportwirtschaft setzte im vergangenen Jahr (2017) über 220 Milliarden Schweizer Franken um. Viele in der Schweiz ansässige Unternehmen liefern in die Europäische Union und bearbeiten dementsprechend Kundendaten aus der Europäischen Union. Am 25. Mai 2018 wird die Europäische Datenschutz-Grundverordnung ihre Wirkung auch auf in der Schweiz ansässige Unternehmen entfalten, welche ihre Waren und Dienstleistungen in der Europäischen Union an-

bieten und aufgrund dessen von in der Union ansässigen Personen personenbezogene Daten bearbeiten (Art. 3 Abs. 2 EU-DSGVO). Die neue Europäische Datenschutz-Grundverordnung bezweckt die personenbezogenen Daten besser zu schützen sowie deren Verarbeitung transparenter zu gestalten. Deshalb werden den Datenverarbeitern Pflichten auferlegt, um die Grundsätze der EU-DSGVO zu gewährleisten. Eine Verletzung dieser Pflichten kann, wie die Verletzung des DSG, empfindliche Folgen für die betroffenen Unternehmen nach sich ziehen.

Datenschutzmassnahmen

Die vorgenannten Risiken verlangen konkrete Datenschutzmassnahmen durch die datenbearbeitenden Unternehmen. Hinsichtlich der zu treffenden Massnahmen ist zu erwähnen, dass die Gefahren, welche sich in der Anwendung der Clouds verbergen, weder vollständig beherrscht noch ihre Realisierung vollständig verhindert werden kann. In diesem Sinne erheben anschliessende Ausführungen keinen Anspruch auf Vollständigkeit. Sie können indes dazu dienen, durch folgende, relativ einfach umzusetzende Massnahmen bestehende Datenschutzrisiken erheblich zu minimieren.

Organisatorische Massnahmen

Organisatorische Massnahmen betreffen vor allem die Schulung der Mitarbeiter hinsichtlich der IT-Sicherheit und die Aufklärung über die Gefahren, welche mit der Anwendung der Cloud verbunden sind. Die Definition einer effektiven Passwortpolitik und ihre technische Umsetzung ist ein erster Schritt dazu. Die Zugangsschlüssel zur Cloud sind mit der nötigen Sorgfalt zu verwenden, dabei sollen die Mitarbeitenden nur auf jene Daten Zugriff haben, welche sie für die Ausführung der ihnen zugetragenen Arbeit benötigen (sogenannte least-privilege-Prinzip). Schliesslich sollte auch abgeklärt werden, ob die Bestimmungen der Europäischen Datenschutz-Grundverordnung auf das Unternehmen Anwendung finden und falls ja, ob der Cloud-Anbieter den relevanten EU-Bestimmungen Rechnung trägt.

Technische Massnahmen

Als technische Massnahmen werden insbesondere jene bezeichnet, welche mithilfe von technischen Mitteln die Gefahr des Datenverlusts oder die Zerstörung der Daten zu reduzieren vermögen. Um einem Datenverlust vorzubeugen, sollten heikle Daten ausserhalb der Cloud separat gespeichert werden. Die Notwendigkeit, Daten zu sichern, wird durch das Cloud Computing nicht obsolet. Hinzu kommt, dass Daten bereits im Unternehmen verschlüsselt werden sollten, bevor sie in die Cloud gestellt werden, um insbesondere gesetzliche oder vertragliche Geheimhaltungspflichten zu gewährleisten, denn auch die Cloud-Mitarbeiter sollten keine Einsicht in diese Daten haben. Auch sollte nur mit einer verschlüsselten Internetverbindung gearbeitet werden, wenn über das Internet Daten aus der Cloud zu bearbeiten sind.

Zum Schluss sind sowohl ein Virenschutzprogramm als auch eine Firewall – beides jeweils auf dem neusten Stand der Technik – aus einem sich in der digitalen Welt bewegenden Unternehmen nicht mehr wegzudenken.

Fazit

Wo Computer und Menschen aufeinandertreffen, entstehen Schwachstellen für die Datensicherheit. Unternehmer müssen sich im Klaren sein, dass die Benutzung der Clouds zwar Vorteile hat, aber auch erhebliche Risiken in sich birgt. Die datenverarbeitenden Unternehmen sind daher aufgefordert, alles zu unternehmen, um den Datenschutz dem Stand der Technik entsprechend zu gewährleisten. Mangelnde Sorgfalt im Bereich des Datenschutzes kann schnell gravierende Folgen für die betroffenen Unternehmen haben. Daten sind wertvoll und darum auch dementsprechend zu behandeln. «

Porträt

Dr. Davide Pinelli
Rechtsanwalt

Dr. Davide Pinelli ist Rechtsanwalt bei Kaufmann Rüedi Rechtsanwälte AG.

Dr. Markus Kaufmann
Rechtsanwalt, Partner

Dr. Markus Kaufmann ist Rechtsanwalt / Partner bei Kaufmann Rüedi Rechtsanwälte AG.

Kaufmann Rüedi Rechtsanwälte ist eine national und international tätige Wirtschaftskanzlei, inklusive Notariat, mit Büros in Luzern und Baar (ZG).

Kontakt

davide.pinelli@krlaw.ch, markus.kaufmann@krlaw.ch, www.krlaw.ch