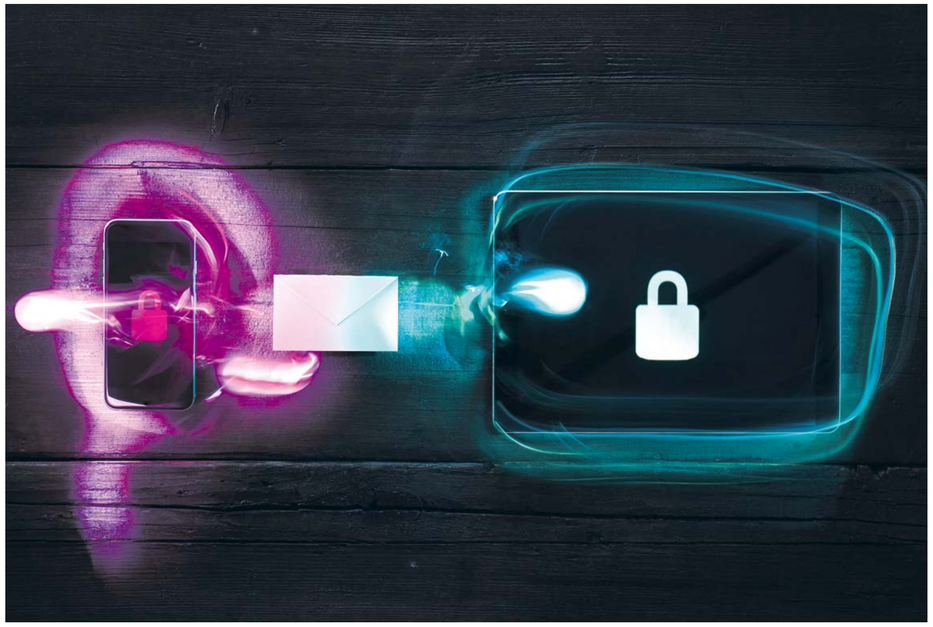
Handelsblatt
DONNERSTAG, 17. OKTOBER 2019, NR. 200



Philipp Dmitri / Westend61 / va

Verschlüsselung: Datentransfer an Subunternehmer birgt Risiken.

Recht

Der tägliche Kampf um den Datenschutz

Die DSGVO hat Firmen aufgeschreckt, die Cloud-Computing nutzen. In der Praxis bleiben viele Baustellen. Experten warnen: Es reicht längst nicht, sich auf die Anbieter zu verlassen.

Louisa Schmidt Köln

Den Finger in die Wunde legen - das ist Joachim Richters Auftrag. Dax-Konzerne und Mittelständler beauftragen den Partner der Managementberatung Axxcon, damit er ihre Cloud-Nutzung kritisch überprüft. Vor allem soll Richter Verstöße gegen die seit Mai 2018 geltende Datenschutz-Grundverordnung (DSGVO) aufspüren. „Die finde ich leider viel zu häufig“, sagt Richter. Mitunter bucht ein Manager naiv eine nützliche Software, die plötzlich sensible Mitarbeiterdaten in einer Cloud speichert. Und zwar ohne dass ein Datenschutzverantwortlicher geprüft hätte, ob der Cloud-Provider die europäischen Vorgaben erfüllt. „Das ist fatal“, urteilt Richter. „So weiß niemand, ob die Cloud-Nutzung im konkreten Einzelfall gegen die DSGVO verstößt.“

Nur Optimisten glauben, die Unternehmenspraxis habe sich seit dem DSGVO-Start flächendeckend zum Guten gewendet. „Immer wieder kommt es vor, dass Mitarbeiter schnell eine ganz bestimmte Software-Lösung für ihre Abteilung suchen und den langwierigeren Einkaufsprozess umgehen“, weiß Richter.

Der Wildwuchs geschieht selbst bei Großunternehmen, obwohl die eigentlich hohe Standards beim Einkauf von Cloud-Diensten verankert haben. Datenschutz-Experten stellen sicher, dass ein Vertrag zur Auftragsverarbeitung abgeschlossen wird, wie es die DSGVO fordert. Sie durchforsten Verträge, bewerten, welche Daten besonders geschützt werden müssen - und prüfen, wer Zugriff auf die Cloud-Server hat.

Viele Firmen können von solcher Professionalität nur träumen. „Sicherheitsbedenken werden zum Schlüsselhemmnis“, konstatiert der IT-Verband Bitkom im jüngsten „Cloud Monitor“. 73 Prozent der befragten Unternehmer sorgten sich um „unberechtigten Zugriff auf sensible Unternehmensdaten“, 64 Prozent befürchten Datenverlust.

Provider in der Pflicht

„Der Schutz personenbezogener Daten steht in der Cloud-Strategie von Unternehmen ganz oben auf der Agenda“, bestätigt Marko Vogel, Partner der Beratungsgesellschaft KPMG. Neun von zehn Unternehmen halten es für unabdingbar, dass der Cloud-Provider die Vorgaben der EU erfüllt. Es ist das wichtigste K.o.-Kriterium bei der Auswahl eines Dienstleisters. Vogel warnt jedoch, dass es damit nicht getan ist: „Unternehmen, die die Cloud nutzen, dürfen sich nicht allein auf ihre Provider verlassen.“

64 PROZENT
der Unternehmen befürchten Datenverluste in der Cloud.
Quelle: Bitkom

Cloud-Kunden sind selbst verantwortlich für den Schutz personenbezogener Daten, die sie einem Dienstleister anvertrauen, sagt Johanna Hofmann, Datenschutzexpertin in der Kanzlei CMS. „Es reicht nicht, sich auf Werbeversprechen der Anbieter zu verlassen.“ Im Gegenteil: „Die Auftraggeber müssen prüfen, ob ein Anbieter die DSGVO-Vorgaben wirklich erfüllt, und dies jederzeit gegenüber Behörden nachweisen können“, erklärt die Anwältin. Ein staatlich anerkanntes Zertifikat, das Rechtssicherheit geben würde, stecke noch in der Entwicklung. Auch sind viele Cloud-Anbieter so groß, dass es Nutzern schwerfällt, auf Vertragsbedingungen einzuwirken.

Mehr Gestaltungsspielraum, um personenbezogene Daten besonders sicher zu speichern, haben Unternehmen, wenn sie auf private Cloud-Lösungen setzen. Dabei stellen die Provider ihre Dienste exklusiv für einzelne Organisationen zur Verfügung, die nicht für die Allgemeinheit über das Internet erreichbar sind. „Doch nicht alle Firmen haben das Know-how und die finanziellen Mittel für solche Lösungen“, gibt Cyber-Security-Experte Vogel zu bedenken.

Tatsächlich ist der Anteil der Firmen deutlich gestiegen, die auch personenbezogene Daten in der öffentlichen Cloud speichern, so ein Ergebnis der Bitkom-Studie. „Viele Firmen verschlüsseln die Daten in der Cloud nicht einmal“, beobachtet Vogel. „Und das, obwohl die Provider entsprechende Lösungen anbieten.“

Mit einigen Regeln lasse sich auch in der Public Cloud das Sicherheitsniveau massiv anheben, sagt Kai Hinke, Abteilungsleiter des Münchener IT-Hauses Consol. Grundlegend ist die Verschlüsselung aller gespeicherten und ausgetauschten Daten. Die Schlüssel zur Cloud sollte man im eigenen Rechenzentrum managen. Auch die Zwei-Faktor-Authentifizierung sei wichtig: Um auf Daten in der Cloud zuzugreifen, müssen sich dann Mitarbeiter nicht nur per Passwort, sondern auch etwa mit einem mobilen Gerät identifizieren. Wichtig sei zudem, Prozesse zu definieren: Was tun, wenn ein Kunde auf Datenlöschung besteht? Was tun bei einem Datenleck? „Viel zu wenige Firmen legen das im Vorfeld fest“, sagt Hinke.

Schatten-IT im Fokus

Auch dem Problem der inoffiziell beschafften Software, sogenannter Schatten-IT, könnte man effektiv entgegentreten. Technisch lasse sich auswerten, ob unautorisierte Cloud-Dienste aktiv sind, so Axxcon-Partner Richter. Finanzabteilungen können prüfen, wer wofür Geld ausgegeben hat. „Doch viele Unternehmen gehen das Thema nicht an“, sagt er. Oft fehlten auch Vereinbarungen mit Arbeitnehmervertretern für den Umgang mit der Cloud. Die Folge: Mitarbeiter wüssten oft nicht einmal, was sie falsch gemacht haben.

Hinzu kommt: Gerade kleinere Software-Anbieter binden oft Subunternehmen in die Datenverarbeitung ein. Richter hat das bei einem Anbieter cloudbasierter HR-Software erlebt, die DSGVO-konform war. Um eine Kalenderfunktion zu nutzen, musste man sich aber bei einem weiteren Dienstleister mit Sitz in den USA registrieren. „So räumten einige Mitarbeiter dem Subunternehmen Rechte zum Zugriff auf sensible Mitarbeiterdaten ein.“ Bei einer späteren Überprüfung durch den Datenschutzbeauftragten sei der Anbieter sang- und klanglos durchgefallen.

Subunternehmen sieht auch CMS-Anwältin Hofmann als eine der großen Herausforderungen beim Datenschutz in der Cloud. Firmen, die bei der Datenverarbeitung mitwirken, müssten in den Verträgen unbedingt benannt werden. „Tatsächlich ist das in der Praxis schwierig“, sagt sie. Denn die Subunternehmer hätten oft wiederum Unterauftragnehmer. „Die gesetzlich gewünschte Transparenz ist unglaublich schwer abzubilden.“

Trotz vieler Herausforderungen sieht IT-Rechtsexperte Peter Bräutigam vor allem Positives: „Wer Cloud-Lösungen nutzt, verbessert die IT-Sicherheit in der Regel deutlich“, ist der Partner der Kanzlei Noerr sicher. Cloud-Lösungen helfen vielfach den Anwendern, den großen Cyber-Sicherheitsrisiken adäquat zu begegnen. Zwischen der Sicherheit, die ein professioneller Provider bietet, und der Sicherheit bei kleineren Unternehmen lägen Galaxien.