Pressemitteilung

Wie ein Geheimnis geheim bleibt – auch in der Cloud

München, 21. 09. 2016. Geheimnisse hat bekanntlich jeder: Michael K. erzählt, dass er an Kehlkopf-Krebs erkrankt ist und möchte nicht, dass darüber geredet wird. Ulli F. hat einen Stalker im Internet am Hals und denkt, es könnte ihre Karriere ruinieren. Alfred Z. plant den Kauf eines Unternehmens, dessen Preis möglichst nicht steigen soll – und Anatol P. ist Beamter. Er bekommt täglich Informationen von Bürgern, die unter das Grundrecht der informationellen Selbstbestimmung fallen und von denen niemand möchte, dass sie weitergetragen werden. Als Beamter ist er an das Amtsgeheimnis gebunden, darf also nichts von dem weitererzählen, was ihm Bürger anvertrauen. Wie ist es aber mit den anderen Berufsgruppen, die mit Geheimnissen konfrontiert sind?

Im Strafgesetzbuch (StGB) ist die Verletzung von Geheimnissen geregelt und wird mit einer Freiheits- oder Geldstrafe geahndet. Im Gesetzestext unterscheidet man

1. Das Privatgeheimnis, das den persönlichen Lebensbereich eines Menschen betrifft. Sei es, dass er unter einer Krankheit leidet oder eine Klage erwägt… Geheimnisträger wie Ärzte oder Anwälte, denen er sich anvertraut, unterliegen der Geheimhaltungs- und Schweigepflicht (§ 203 StGB).

2. Den Begriff Unternehmensgeheimnis, also das betriebliche „Know-how“, verstehen Juristen sehr weit. Für sie erfasst es alle Tatsachen, die mit dem Betrieb in Zusammenhang stehen, an deren Schutz und Geheimhaltung ein berechtigtes Interesse des Unternehmens besteht und die nach dem Willen des Unternehmensinhabers auch geheim bleiben sollen (§ 203 StGB). Betriebsgeheimnisse sind dabei unabhängig vom Patent-, Marken- oder Urheberrecht.

3. Unter einem Amtsgeheimnis wird eine bestimmte Erkenntnis oder eine Tatsache verstanden, die nur für einen eng eingegrenzten Personenkreis verfügbar gemacht werden darf. Deshalb unterliegt diese Information der Geheimhaltungspflicht. Generell gilt für alle Beamten die Verschwiegenheitspflicht (§ 61 BBG, Bundesbeamtengesetz und § 39 BRRG, Beamtenrechtsrahmengesetz). Wer als Amtsträger seine Geheimhaltungspflichten verletzt und dadurch wichtige öffentliche Interessen gefährdet, wird gemäß § 353 b StGB mit Freiheitsstrafe bis zu fünf Jahren oder Geldstrafe bestraft.

Anwälte, Wirtschaftsprüfer, Ärzte, Psychologen, Finanzberater, Beamte, Prokuristen, Geschäftsführer Datenschutzbeauftragte… sie alle gehören zu Geheimnisträgern und müssen neben den geltenden Datenschutzgesetzen auch dem strengen, nicht dem Grundsatz der Verhältnismäßigkeit unterliegenden, § 203 StGB zur Verletzung von Privatgeheimnissen folgen.

Die oben genannten Gesetze verbieten die „Offenbarung von Geheimnissen“ – und gerade hier ist der Haken, wenn Geheimnisträger einen Internetdienst nutzen wollen.

Welches Problem haben Geheimnisträger in der Cloud?

Anders als bei anderen Berufsgruppen fallen täglich unzählige Akten, Dokumente oder

Patientendaten an, die Geheimnisträger unzugänglich für Dritte aufbewahren müssen. Um immer größer werdende Berge an Papier zu vermeiden, sehen viele in einem internetbasierten Dienst die Lösung. Dort könnten sie alle Dateien an einem Ort aufbewahren, ohne Raum oder Papier zu verschwenden.

Geheimnisträger benötigen aber wegen einer möglichen „Offenbarung von Geheimnissen“ einen Cloud-Dienst, der eine besonders sichere Datenverarbeitung und-speicherung gewährleistet. Das Verbot der „Offenbarung von Geheimnissen“ bedeutet nämlich, dass allein schon die technische Möglichkeit strafbar ist, dass Dritte auf Daten zuzugreifen. Doch selbst dann, wenn Daten in einer Cloud durchgängig verschlüsselt werden, kann es „zu einer Offenbarung von Geheimnissen auf dem Umweg über Metadaten kommen“, erklärt der Jurist, Dr. Steffen Kroschwald, Autor des Buches „Informationelle Selbstbestimmung in der Cloud“, in dem sich der wissenschaftliche Mitarbeiter im Projekt verfassungsverträgliche Technikgestaltung (provet) an der Universität Kassel mit der datenschutzrechtlichen „Bewertung und Gestaltung des Cloud Computing aus dem Blickwinkel des Mittelstands“ beschäftigt. Da die Verknüpfung von Metadaten äußerst verräterisch sein kann, müssen diese Berufsgruppen glaubhaft alles zu deren Schutz unternehmen.

Wann kann ein Geheimnisträger einen Cloud-Dienst nutzen?

Damit Geheimnisse gewahrt bleiben, muss ein Geheimnisträger eine Cloud nutzen, die den hohen technischen Anforderungen zum Datenschutz entspricht.

Im Trusted Cloud Datenschutzprofil (TCDP), das vom Bundesministerium für Wirtschaft und Energie mithilfe aller maßgeblichen Datenschutz-Stellen erarbeitet wurde, sind für Geheimnisse die Anforderungen für ein Zertifikat mit der Schutzklasse 3 ausschlaggebend [2]. Für Geheimnisträger gilt also:

In die Cloud darf ein Geheimnis nur, wenn der beauftragte Dienst all jene Maßnahmen umsetzt, die der Schutzklasse 3 entsprechen.

1. https://dejure.org/gesetze/StGB/203.html
2. https://stiftungdatenschutz.org/startseite/
3. http://www.digitale-technologien.de/DT/Redaktion/DE/Downloads/Publikation/Trusted-Cloud/trustedcloud-ap9-schutzklassen-datenschutz-zertifizierung.pdf?__blob=publicationFile&v=3

Pressemitteilung

Druckfähiges Bildmaterial erhalten Sie auf Anfrage bei presse@uniscon.de
Weiter Informationen zu Funktionen und Aussehen:

Über Uniscon GmbH

Uniscon – The Web Privacy Company
Die Uniscon GmbH entwickelt technische Lösungen zur effizienten und sicheren Zusammenarbeit im Internet. Ihr Service iDGARD basiert auf der weltweit patentierten Sealed Cloud Technologie. Mit dieser werden die Daten in der Cloud so geschützt, dass selbst der Betreiber des Dienstes keinen Zugriff auf die Daten seiner Kunden hat. Als einziger Dienst schützt iDGARD nicht nur die Inhalte, sondern auch die Metadaten. Diese bleiben ausschließlich unter der Kontrolle der Nutzer. Weitere Informationen finden Sie unter www.uniscon.de, www.sealedcloud.de und www.idgard.de.

Pressekontakt
Uniscon GmbH, Claudia Seidl
Agnes-Pockels-Bogen 1
80992 München
089 / 41 615 988 103
presse@uniscon.de
www.uniscon.de