Pressemitteilung

USA: „Würden Sie das Smartphone daheim lassen?“

Wer seine Privatsphäre schützen will, setzt am besten auf sichere Cloud-Lösungen

München, 28. Februar 2017. *Dürfen Grenzbeamte bei der Einreise in die USA mein Smartphone und das Passwort dazu verlangen? Und was passiert, wenn ich mich weigere? Dr. Hubert Jäger, Cloud-Security-Experte und CTO bei Cloud-Anbieter Uniscon, bezweifelt, dass Smartphone und Laptop auf Reisen zuhause bleiben. Seine Lösung: Sensible Daten in einer sicheren europäischen Cloud abzulegen.*

Es hört sich fast an wie eine Phantasie aus einem Überwachungsroman: Vor einigen Wochen wurde der in den USA geborene NASA-Mitarbeiter Sidd Bikkannavar bei der Einreise in die vereinigten Staaten am Flughafen festgehalten [1]. Grenzschützer hatten ihm sein Smartphone abgenommen und ihn aufgefordert, ihnen den Zugangscode zu verraten – verbunden mit der Drohung, ihn so lange nicht gehen zu lassen, bis er kooperiere. Nach einer Weile gab Bikkannavar auf und gewährte den Beamten Zugriff auf das Gerät – und damit nicht nur auf persönliche Daten, sondern auch auf möglicherweise sensible Daten des Arbeitgebers, da es sich um ein Diensthandy der NASA handelte.

Auch wenn es sich dabei bislang noch um einen von wenigen Einzelfällen handelt, könnte sich das in naher Zukunft ändern: Anfang Februar 2017 forderte US-Heimatschutzminister John Kelly schärfere Überprüfungen von Besuchern und schlug dabei unter anderem vor, Einreisende künftig nach den Passwörtern zu ihren Profilen in sozialen Netzwerken wie Facebook zu fragen [2]. Sich im selben Zuge auch gleich das Smartphone vorzuknöpfen, ist nur der logische nächste Schritt. Und da es sich bei den Grenzgebieten der vereinigten Staaten nicht um US-Territorium handelt, dürfen die Grenzschützer hier vieles tun, was in den USA schlicht illegal wäre – beispielsweise Reisende festsetzen und die Herausgabe von Geräten und Passwörtern verlangen [3].

Abgesehen davon, dass es sich bei solchen Zugriffen um eine Verletzung von Persönlichkeitsrechten handelt, ist beispielsweise im Fall Bikkannavar noch nicht geklärt, auf welche Daten die Grenzbeamten tatsächlich zugegriffen

haben. Der NASA-Mitarbeiter ist sich nicht einmal sicher, ob das Smartphone überhaupt heikle Daten enthalten habe. Seine Vorgesetzten im Jet Propulsion Laboratory der US-Raumfahrbehörde seien allerdings „nicht glücklich“ über den Vorfall gewesen [4].

Soll man jetzt das Smartphone zuhause lassen?

Müssen sich nicht nur Reisende sorgen, sondern auch Unternehmen, die ihre Mitarbeiter auf Geschäftsreise schicken? Nicht unbedingt, gibt es doch einen recht einfachen Weg, sich und seine Geräte vor unerwünschten Zugriffen zu schützen: „Es ist ja wohl keine Option, Hardware wie Smartphones, Tablets oder Notebooks auf internationalen Reisen künftig einfach daheim zu lassen“, meint Dr. Hubert Jäger, CTO bei dem deutschen Cloud-Security-Anbieter Uniscon.
Eine effektive Möglichkeit sei, „die Unternehmensdaten in einer versiegelten Cloud abzulegen, so dass man selbst von überall aus darauf zugreifen kann“. Dort sind diese Daten jedoch zuverlässig vor unbefugten Zugriffen geschützt. „Hierfür bietet sich ein Dienst wie iDGARD an, der nach der höchsten Schutzklasse des Trusted Cloud Datenschutz Profils (TCDP) zertifiziert und damit sogar für Berufsgeheimnisträger geeignet ist“, rät Jäger.

Weitere Informationen:
[1] https://netzpolitik.org/2017/us-grenzbeamte-zwingen-nasa-mitarbeiter-sein-diensttelefon-zu-entsperren/

[2] https://www.heise.de/newsticker/meldung/US-Regierung-ueberlegt-Zwang-zur-Passwort-Herausgabe-fuer-US-Visum-3619659.html

[3] https://www.eff.org/deeplinks/2016/12/law-enforcement-uses-border-search-exception-fourth-amendment-loophole

[4] http://www.sueddeutsche.de/digital/grenzkonztrolle-us-amerikaner-muss-bei-einreise-smartphone-passwort-verraten-1.3376781

Druckfähiges Bildmaterial erhalten Sie auf Anfrage bei presse@uniscon.de

Pressemitteilung

Über Uniscon GmbH

Die Uniscon GmbH entwickelt technische Lösungen zur effizienten und sicheren Zusammenarbeit im Internet. Ihr Service iDGARD basiert auf der in den weltweit wichtigsten Ländern 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, 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