SCRYPTOS

Risiken für Daten **im Ausland**

Schutz sensibler Daten auf Geschäftsreise

Detlef Hastik
Henry Frenz

Datensicherheit

bei Geschäftsreisen ins Ausland

Geschäftsreisen ins Ausland sind auf Grund der Globalisierung und weltweiten Vernetzung von Unternehmen heute für viele Berufstätige ein alltäglicher Teil ihres Berufslebens.

Laptop, Tablet und Smartphone sind hierbei die ständigen Begleiter. In den meisten Fällen werden die Mobile Devices sowohl für geschäftliche als auch private Zwecke verwendet. Daher beinhalten die Geräte Arbeitsunterlagen, Unternehmenskorrespondenz und -daten ebenso wie private Bilder, Kommunikation und Zugänge zu sozialen Netzwerken.

Bei Reisen ins Ausland kommt dem Schutz dieser Daten eine besondere Bedeutung zu, da die persönlichen Rechte des Einzelnen nicht in jedem Land gleich bewertet und geachtet werden bzw. grundsätzlich eine höhere Gefahr von Wirtschaftsspionage herrscht.

Dies zeigt sich auch in den Warnungen des Bundesamtes für Verfassungsschutz (BfV) im Rahmen der Initiative Wirtschaftsschutz. So warnt das BfV bspw. vor der Möglichkeit der Totalüberwachung des Internets und der Telekommunikation sowie der Manipulation mobiler Endgeräte.

Zur Prävention wird zu Datensparsamkeit auf den mitgeführten Geräten und der Nutzung erlaubter Verschlüsselungsprodukte geraten. Außerdem weist das BfV explizit darauf hin, sensible Informationen nicht aus der Hand zu geben und benennt auch Hotelzimmer und –safe als nicht sichere Orte.[1]

Mit der Nutzung von SCRYPTOS wird all diesen vorgeschlagenen Gefahren und Maßnahmen Rechnung getragen, da die Dateien und Informationen nicht lokal auf den Endgeräten gespeichert sind, sondern nur in hochsicheren, zertifizierten Rechenzentren in Deutschland vorliegen. Somit sind die Daten auch nicht gefährdet, wenn der Datenträger oder das Gerät kopiert, gestohlen oder verloren werden. Greift der Nutzer aus dem Ausland auf den SCRYPTOS-Account zu, erfolgt die Datenübertragung verschlüsselt. Auch eine Überwachung des Datenverkehrs kompromittiert somit nicht die Datensicherheit.

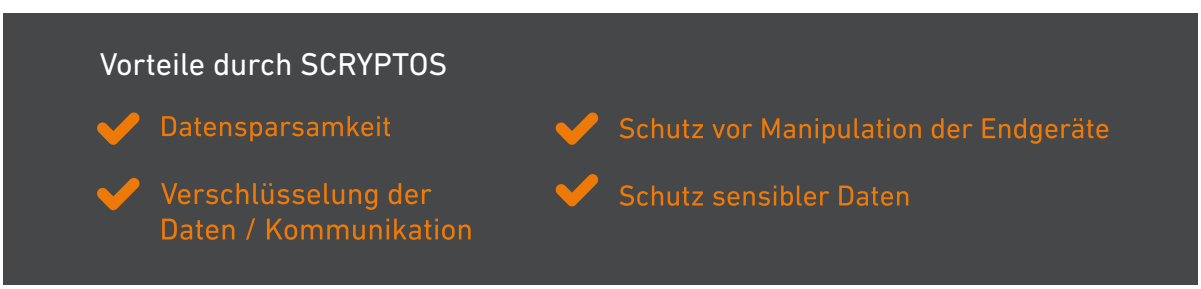

Abb.1: Vorteile durch SCRYPTOS

1 Vgl. Wirtschaftsschutz: Geschäftsreise – Sicherheit bei Auslandreisen

Neben diesen allgemeinen Gefahren hat sich in jüngerer Vergangenheit jedoch noch eine weitere Gefahr für die Datensicherheit gebildet. Diese betrifft hauptsächlich die Einreise in das Zielland, kann jedoch auch schon bei einer Durchreise relevant werden. Im Zuge der Grenzkontrollen dürfen in einigen Ländern auch die elektronischen Geräte der Einreisenden durchsucht werden.
Diese Kontrollen können auch stattfinden, wenn man auf seiner Reise nur eine Zwischenlandung bspw. in den USA hat.

Im Zuge der Einreisebestimmungen in den USA dürfen US-Grenzschützer die elektronischen Geräte von Einreisenden durchsuchen. Dieses Recht basiert auf dem Recht zu Gepäckdurchsuchungen ohne richterlichen Beschluss und wurde 2009 auf elektronische Geräte ausgeweitet.[2]

Im Regelfall ist niemand verpflichtet, seine Passwörter zu verraten oder Laptop und Smartphone zu entsperren. Allerdings riskiert man bei einer Weigerung ein Einreiseverbot und muss auf eigene Kosten zurückfliegen. Gestützt wird dies auch durch zwei Supreme Court-Urteile aus den Jahren 1976 und 2004, die feststellen, dass Einreisende einen größeren Eingriff in ihre Privatsphäre akzeptieren müssen, weil es im Interesse der Regierung sei, potenzielle Gefahren von den USA fernzuhalten.

Gerade wenn man aus geschäftlichen Gründen in die USA einreist, ist eine Offenlegung sensibler Geschäftskommunikation und Dateien mit einem hohen Risiko verbunden, da die Behörden auch das Recht haben, die Daten zu kopieren und zu speichern.[3]

Als bekanntes Beispiel hierfür kann der NASA-Mitarbeiter Sidd Bikkannavar angeführt werden. Dieser wurde stundenlang am Flughafen von Houston verhört, bis er schließlich das Passwort für sein Diensthandy weitergab. Nachdem die Beamten das Diensthandy kontrolliert und die Daten kopiert hatten, durfte Sidd Bikkannavar in die USA einreisen.
Laut Recherche der Bürgerrechtsorganisation ACLU wurden zwischen Oktober 2008 und Juni 2010 mehr als 6.500 Einreisende gezwungen, ihre elektronischen Geräte durch die US Grenzschützer kontrollieren zu lassen. In knapp der Hälfte der Fälle waren Geschäftsreisende und Touristen betroffen. 2015 wurden 5.000 Kontrollen durchgeführt. Im letzten Jahr der Amtszeit von Obama 2016 waren es circa 24.000 Kontrollen, wobei die Auswahlkriterien hinsichtlich der kontrollierten Personen nicht nachvollzogen werden können.

Somit lässt sich festhalten, dass die Anzahl der Kontrollen stark angestiegen ist. Und auch wenn dies noch immer nur 0,0061% der 390 Millionen Einreisen in die USA betrifft, sollte es Grund genug sein, mitgeführte Daten so gut wie möglich zu schützen.[4]

Auch hier greifen die in Abbildung 1 genannten Schutzmechanismen von SCRYPTOS, da die sensiblen Daten nicht auf dem Gerät gespeichert sind und somit vor dem Zugriff der Grenzschützer und möglichen Kopiervorgängen sicher sind.

Zwar basieren die derzeitige rechtliche Situation und die oben genannten Zahlen noch auf der Obama-Administration, doch durch den Leitsatz des jetzigen US-Präsidenten „America First“ erscheint es möglich, dass diese Kontrollen weiter steigen werden, da sie sowohl unter sicherheitspolitischen als auch wirtschaftlichen Gesichtspunkten nützlich erscheinen.

Im Februar 2017 unterzeichnete US-Präsident Trump einen Erlass zur „Verbesserung der Inneren Sicherheit“. Dieser Erlass schränkt den Geltungsbereich des Privacy Act (US Datenschutzgesetz) ein. Demnach sollen Behörden sicherstellen, dass nur US-Bürger und Personen mit dauerhafter Aufenthaltserlaubnis unter den Schutz des amerikanischen Datenschutzrechts „Privacy Act“ fallen.

---

2 Vgl. Privacy Impact Assessment for the Border Searches of Electronic Devices
3 Vgl. Inspection Electronic Devices Tearsheet
4 Vgl. SZ - So schützen Sie Ihre Daten bei der Einreise in die USA

Warum SCRYPTOS?

EU-Bürger sind hiervon zunächst jedoch nicht betroffen, da der EU-US-Privacy-Shield nicht auf dem Privacy Act, sondern auf dem von der Obama-Administration verabschiedeten Judicial Redress Act basiert.[5]

Dennoch sollte die Entwicklung aufmerksam verfolgt werden. Die Forderung des ehemaligen Heimatschutzministers John Kelly, „Einreisende an der Grenze zu zwingen, ihre Social Media Passwörter herauszugeben“[6] lässt zumindest vermuten, dass es Versuche geben könnte, die Kontrollrechte auszuweiten.

Die Gefahr für die Datensicherheit bei der Einreise ist jedoch nicht auf die USA beschränkt. Bei der Einreise nach Australien gelten seit 2009 verschärfte Gesetze, hinsichtlich einer möglichen Einfuhr von Gewalt verherrlichenden Filmen oder Pornografie. Unter dieser Maßgabe ist es australischen Behörden erlaubt, bei der Einreise die Datenträger von Reisenden nach unerwünschtem Material zu durchsuchen. Im Rahmen von Zufallsprüfungen können theoretisch Datenträger von jedem Einreisenden überprüft werden. Die Prüfungen müssen nicht im Beisein des Reisenden erfolgen, somit sind Daten, Korrespondenz und Informationen einem potenziellen Risiko (Verlust, Kopieren, Einsichtnahme) ausgesetzt.[7]

Auf Auslandsreisen insgesamt und teilweise auch bei den Einreisekontrollen sind Daten einer erhöhten Gefahr der Spionage oder ungewollten Einsichtnahme ausgesetzt.

Durch die Nutzung von SCRYPTOS umgehen Sie dieses Risiko, da die Dateien nicht auf dem Endgerät, sondern in sicheren Rechenzentren in Deutschland gespeichert sind. Somit sind die Daten sowohl vor Kriminellen als auch vor ausländischen Sicherheitsbehörden geschützt.

Darüber hinaus wird jeder Zugriff auf SCRYPTOS im Auditlog verzeichnet, so dass jederzeit nachvollziehbar ist, welcher User wann auf welche Daten zugegriffen hat.

Überzeugen Sie sich selbst und melden Sie sich noch heute für einen 30-tägigen Testzugang auf **www.scryptos.com** an.

Weiterführende Informationen und Tipps zur Datensicherheit hinsichtlich der Einreise in den USA geben die Electronic Frontier Foundation (EFF; www.eff.org) und die American Civil Liberties Union (ACLU; www.aclu.org)

---

5 Vgl. Datenschutz nur noch für US-Bürger – Privacy Shield in Gefahr?
6 Vgl. SZ - So schützen Sie Ihre Daten bei der Einreise in die USA
7 Vgl. Australien Info – Einreise und Zoll

Quellen:
[1] Wirtschaftsschutz: Geschäftsreise – Sicherheit bei Auslandreisen; https://www.wirtschaftsschutz.info/SharedDocs/Publikationen/DE/SicherheitGeschaeftsreisen/Geschaeftsreisen.html?nn=6556052
[2] Privacy Impact Assessment for the Border Searches of Electronic Devices; https://en.wikipedia.org/wiki/United_States_v._Arnold
[3] Inspection Electronic Devices Tearsheet; htttps://www.cbp.gov/sites/default/files/documents/inspection-electronic-devices-tearsheet.pdf
[4], [6] SZ - So schützen Sie Ihre Daten bei der Einreise in die USA; http://www.sueddeutsche.de/digital/2.220/grenzkontrollen-so-schuetzen-sie-ihre-daten-bei-der-einreise-in-die-usa-1.3388338
[5] Datenschutz nur noch für US-Bürger – Privacy Shield in Gefahr?; https://www.datenschutz-notizen.de/datenschutz-nur-noch-fuer-us-buerger-privacy-shield-in-gefahr-1317186/
[7] Australien Info – Einreise und Zoll; http://www.australien-info.de/anreise-einreise.html

SCRYPTOS

Kontakt:
SYGNOMI GmbH
Am Kreuzstein 80 | 63477 Maintal
06109-24 54 0 | mail@sygnomi.de

Vertrieb:
SMC Consult GmbH
040-8888 299 69 | vertrieb@sygnomi.de

Autor:
Detlef Hastik

Version 1.0
Veröffentlichungsdatum: 06.10.2017

EINFACH VIERFACH SICHER.