

Deutsche Steuerberater und Anwälte als Spionagehelfer

München, 15. Juli 2013. Gerade erreichte die Empörung in Deutschland über den Spionageskandal amerikanischer Behörden einen neuen Höhepunkt, als das Magazin DER SPIEGEL in der Ausgabe vom 8. Juli 2013 titelte: „*Die stecken unter einer Decke mit den Deutschen*“ – Edward Snowden über die grenzenlose Macht des US-Geheimdienstes NSA. Mit *den Deutschen* meinte DER SPIEGEL offensichtlich deutsche Geheimdienststellen – was schon bedenklich genug erscheint. Die Wirklichkeit ist aber noch viel dramatischer: Nicht nur die NSA, sondern beamtete und freiberufliche Spione aus aller Welt arbeiten mit einer großen Zahl deutscher Internetnutzer beim Ausforschen vertraulicher wirtschaftlicher Daten zusammen; wobei letztere keineswegs im Auftrag von BND oder BKA den fremden Spionen Daten zuliefern, sondern ihre Zuträgerdienste freiwillig und unbezahlt leisten. Zu diesen deutschen „Hilfsspionen“ zählen zahlreiche Steuerberater, Rechtsanwälte sowie Mitarbeiter vieler bekannter deutscher Unternehmen. „Geliefert“ werden jede Menge Steuerdaten von deutschen Firmen und Privatpersonen sowie Verträge, Geschäftspläne und andere vertrauliche Dokumente. Wo die Dokumente landen, wer sie in wessen Auftrag und zu welchem Zweck liest, das ist noch unklarer als bei den Massen von Daten, die amerikanische Geheimdienste in Deutschland abfangen. Klar ist nur, dass die deutschen Hilfsspione sich nach deutschem Recht strafbar machen.

Wie funktioniert dieser informelle Spionagering und wie konnte es geschehen, dass bisher kein Whistleblower diese besorgniserregenden Tatsachen aufdeckte? Technisch funktioniert die Lieferung der Daten ganz einfach so, dass ein Steuerberater, Anwalt oder Firmenmitarbeiter an einen echten, tatsächlich zum Empfang der Daten berechtigten Ansprechpartner eine unverschlüsselte Mail mit sensiblen Daten schickt - natürlich mit der Erlaubnis des Empfängers. Auf dem Weg durch das Internet werden diese Daten von nicht näher bekannten Interessenten gelesen – was dadurch möglich ist, dass die Daten unverschlüsselt gesendet wurden oder dass sie bei Dropbox und ähnlichen Diensten abgelegt und vom Empfänger von dort wieder heruntergeladen wurden. Bekannt gemacht wurde dieser Datenskandal, der unvorstellbare Ausmaße besitzt, auch bereits, aber merkwürdiger Weise, ohne dass er große Empörung hervorrief: Zum Beispiel veröffentlichte die Süddeutsche

Presseinformation

Zeitung in ihrer Wochenendausgabe vom 22./23. Juni 2013 den Artikel „Die Steuererklärung auf der Postkarte“, der genau diese Veruntreuung von Daten durch unverschlüsselte E-Mails, also quasi digitale Postkarten, zum Thema hat. Allerdings handelt es sich bei den Datenlieferanten nicht um Konzerne mit hohem Aufmerksamkeitswert wie Apple, Google und Microsoft oder aus Steuergeldern finanzierte Geheimdienste wie den BND, sondern um die Steuerkanzlei und das Anwaltsbüro um die Ecke sowie – möglicherweise – um den freundlichen Mitarbeiter aus der Lohnbuchhaltung, der in der Kantine mittags immer am Nachbartisch sitzt. Das ist vielleicht ein Grund, warum dieser Skandal bisher weder öffentlich ausreichend aufgearbeitet noch aufgeklärt oder gar verhindert wurde.

Dr. Ralf Rieken beschäftigt sich als Geschäftsführer der Uniscon GmbH damit, technische Lösungen zum sicheren Versand von sensiblen Daten anzubieten. Er kommentiert die Vorfälle: „Wer zum Beispiel als Steuerberater oder Lohnbuchhalter Daten seiner Mandanten oder Kollegen über unverschlüsselte Mails sendet, macht sich seit dem Jahr 2008 strafbar nach dem § 203 „Verletzung von Privatgeheimnissen“ des Strafgesetzbuches. (1) Und heute kann sich niemand mehr hinter dem Scheinargument verstecken, dass das Verschlüsseln von Daten angeblich zu schwierig, zu teuer oder zu umständlich sei.“

Er nennt als Beweis den von Uniscon entwickelten sicheren Kommunikationsdienst IDGARD gegen diese „Ausflüchte“, wie er es nennt: Herzstück des Datenschutzes-Angebots IDGARD ist die von Uniscon entwickelte Sealed Cloud Technologie. Wer anderen vertrauliche Unterlagen oder Nachrichten schicken will, legt sie einfach in der Sealed Cloud ab, entweder direkt aus Outlook heraus oder über den Web Browser. Der Empfänger holt dann auf dieselbe Weise die für ihn bestimmten Daten ab. Die Sealed Cloud umfasst ein vollständiges System von technischen Maßnahmen zur technischen „Versiegelung“ eines Rechenzentrums. Es reicht von der Verschlüsselung mit besonderer Schlüsselverteilung bis hin zu Speichermanagement und Datenlöschfunktionen. Deutsche Firmen können ohne Bedenken dieses Cloud-Angebot nutzen, weil der Zugriff auf die Nutzerdaten hier tatsächlich nur für den Eigentümer der Daten und seine von ihm gewählten Kommunikationspartner möglich ist. Uniscon hat mit seiner Sealed Cloud Technologie die neuartige Situation

Presseinformation

geschaffen, dass die Firma selbst als Eigentümer und Betreiber des Systems gar nicht an die Daten ihrer Kunden herankommt. Damit ist der Zugriff natürlich auch anderen, unerwünschten Interessenten verwehrt.

Wichtig ist Rieken und seinen Mitstreitern neben hoher technischer Sicherheit eine einfache und verständliche Bedienung ihrer Lösung. Denn damit Nutzer ein „Mehr“ an Sicherheit akzeptieren, darf dieses nicht mit einem Verlust an Komfort einhergehen. Deswegen funktioniert IDGARD ohne eine für andere Lösungen notwendige Public-Key-Infrastruktur (PKI) (4) sowie vor allem ohne zusätzliche lokale Software. Somit kann die Kommunikation sofort von allen Endgeräten aus geschützt erfolgen. „Da fehlende PKI-Infrastrukturen eine einfache Nutzung verschlüsselter E-Mails erschweren, ist unser Cloud-Service IDGARD so gestaltet, dass er völlig ohne PKI auskommt. Der Nutzer muss noch nicht einmal Software installieren – ein normaler Browser genügt“, erklärt Dr. Rieken.

- (1) <http://dejure.org/gesetze/StGB/203.html>
- (2) <https://de.wikipedia.org/wiki/Public-Key-Infrastruktur>

Über Uniscon GmbH – The Web Privacy Company

Uniscon – The Web Privacy Company – entwickelt technische Lösungen zur sicheren, bequemen Nutzung des Internets bei gleichzeitigem Schutz der Privatsphäre der User. Uniscons Web Privacy Service ID|GARD basiert auf der weltweit patentierten Sealed Cloud Technologie. Dabei werden die Daten in der Cloud geschützt, so dass selbst der Betreiber des Portals keinen Zugriff auf die Daten seiner Kunden hat. Die Sealed Cloud Technologie wird durch ein von Uniscon geführtes Konsortium im Rahmen der Trusted Cloud Initiative des BMWi zur generellen Nutzung durch die deutsche Industrie weiter entwickelt. 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 / 41 615 988 110
presse@uniscon.de
www.uniscon.de



Presseinformation

PR-Agentur Xpand21 GmbH
Doris Loster
Romanstr. 10
80639 München
089 / 12 00 72 77
uniscon@xpand21.com
www.pr-agentur-xpand21.de