

## **No-Spy-Garantie jetzt auch von Ländern gefordert: Aus für ausländische IT-Firmen mit Geheimdienst-Hintergrund**

*München, 16. September 2014. Der Bund hat sie schon vor Monaten gefordert, fast alle deutschen Länder ziehen nun nach: IT-Firmen, die irgendeiner Verpflichtung unterliegen, an ausländische Geheimdienste zu berichten, sollen von sicherheitsrelevanten öffentlichen Aufträgen künftig ausgeschlossen werden. Es sei denn, sie können verbindlich garantieren, dass sie keinerlei entsprechender Verpflichtung unterliegen. Datenschutz-Experten warnen, dass beispielsweise viele IT-Unternehmen aus den USA durch Gesetze wie Patriot Act oder Protect America Act entsprechenden Verpflichtungen unterliegen. Laut dem früheren US-Geheimdienstmitarbeiter Edward Snowden sollen Unternehmen den Geheimdiensten der USA und Großbritanniens Zugang zu vertraulichen Kundendaten gewährt haben. Jetzt werden öffentliche Aufträge an Firmen aus dem angelsächsischen Raum auch in den Medien in Frage gestellt, da man ihnen entsprechende Verbindungen zu ausländischen Geheimdiensten nachsagt.*

Auch wenn entsprechende Textbausteine in alle Verträge aufgenommen werden, die Bund oder Länder mit IT-Dienstleistern abschließen, dürfte es schwierig sein, die Einhaltung der entsprechenden Verpflichtungen zu untersuchen. Laut heise Online äußerte Schleswig-Holsteins Datenschutzbeauftragter Thilo Weichert dazu die Empfehlung, so wenig Daten wie möglich weiterzugeben, "so dass Auftraggeber möglichst wenig sicherheitsrelevante und auch personenbezogene Daten" erhalten. (1)



Noch weiter geht Datenschutzexperte Dr. Hubert Jäger, Geschäftsführer des Münchner Unternehmens Uniscon, in seiner Empfehlung: „Ein NoSpy-Ausschluss durch Technik ist an vielen Stellen sinnvoller als Verpflichtungen auf Papier. Für eine technische Umsetzung eignen sich Ansätze wie die Sealed Cloud. (2) Ziel der Sealed Cloud ist, eine „versiegelte“ Infrastruktur für alle Anwendungen des Cloud Computing zu schaffen. Mit „Versiegelung“ ist gemeint, dass der Betreiber

Pressemitteilung

*einer Infrastruktur entlang der ersten Verteidigungslinie des Rechenzentrums – also während der Verarbeitung der Nutzerdaten in der Cloud – ausschließlich mit technischen Maßnahmen daran gehindert wird, auf unverschlüsselte Daten zuzugreifen, seien es Inhalte oder Metadaten.“*

**Druckfähiges Bildmaterial erhalten Sie auf Anfrage bei [presse@uniscon.de](mailto:presse@uniscon.de)**

(1) <http://www.heise.de/newsticker/meldung/Oeffentliche-Auftraege-nur-gegen-No-Spy-Garantie-2305043.html>

(2) [http://de.wikipedia.org/wiki/Sealed\\_Cloud](http://de.wikipedia.org/wiki/Sealed_Cloud)

#### **Über Uniscon GmbH –**

Uniscon – Kommunikation und Datenaustausch einfach | sicher | compliant – entwickelt technische Lösungen zur sicheren und bequemen Online-Geschäftskommunikation. Der Service IDGARD für Unternehmen 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 Unternehmensdaten bleiben damit ausschließlich im Besitz des Eigentümers. 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](http://www.uniscon.de), [www.sealedcloud.de](http://www.sealedcloud.de) und [www.idgard.de](http://www.idgard.de).

#### **Pressekontakt**

Uniscon GmbH/Claudia Seidl  
Agnes-Pockels-Bogen 1  
80992 München  
089 / 41 615 988 110  
[presse@uniscon.de](mailto:presse@uniscon.de)  
[www.uniscon.de](http://www.uniscon.de)

PR-Agentur Xpand21 GmbH  
Doris Loster  
Romanstr. 10  
80639 München  
089 / 71 68 07 35  
[uniscon@xpand21.com](mailto:uniscon@xpand21.com)  
[www.pr-agentur-xpand21.de](http://www.pr-agentur-xpand21.de)