Presseinformation

Das Smartphone wird zum „digitalen Aktenkoffer“

München, 06. Mai 2014. Viele Deutsche nutzen das Smartphone, um Firmen-Mails zu lesen, mit Kollegen über Skype oder per Handy zu konferieren und um Firmendokumente zu lesen, ob nun im Büro, in der Mittagspause, auf Dienstreise oder zuhause. Der Trend zu „Bring your own device“ gedeiht flächendeckend, vom Praktikanten über die Sekretärin und den freien Mitarbeiter bis zum Vorstandsmitglied. Nach einer aktuellen Umfrage nutzen vier von zehn Arbeitnehmern gelegentlich oder sogar oft ihre privaten Smartphones und Computer für die Firma (1). Da die meisten kein Smartphone und keinen Tablet-PC von der Firma bezahlt bekommen, nutzen sie eben ihre eigenen Geräte und Mobilfunk-Anschlüsse wie einen „digitalen Aktenkoffer, um rasch und bequem beruflich auf dem Laufenden zu bleiben.

Das erscheint auf den ersten Blick wie ein großzügiges Geschenk an die Arbeitgeber, aber ganz so einfach ist es nicht. Zum Beispiel lässt sich bei privaten Smartphones und Tablets kaum überprüfen, wo firmeninterne Dokumente landen: in der iCloud von Apple, auf dem Hotmail- oder Gmail-Konto, das mit einem Windows Phone oder einem Android-Gerät verknüpft ist oder in ein und dem selben Speicher, in dem auch privat heruntergeladene Android-Apps mit versteckter Schadsoftware residieren. Ein besonders alltägliches Beispiel dafür ist das Adressbuch im Smartphone, aber auch Firmen-Passwörter und vertrauliche Dokumente können leicht und unkontrolliert betroffen sein. Die Nutzer genießen den gewohnten Komfort ihres Geräts oft, ohne viel über die Sicherheits- und Datenschutz-Mängel zu wissen, die damit einhergehen und IT-Experten des Arbeitgebers können nur in den wenigsten Fällen auf die privaten Smartphones und Tablets ihrer technisch weniger geschulten Kollegen zugreifen und ihnen Vorschriften machen, wie sie diese nutzen – falls sie überhaupt wissen, wer welche privaten Geräte für die Arbeit nutzt. Berufliche Daten auf privaten Geräten werden deshalb zunehmend zum Sicherheitsproblem für Firmen. Für Kriminelle wird es dadurch viel leichter, deutschen Firmen Daten zu stehlen.

Deshalb ist es für deutsche Firmen dringend geboten, ihre vertraulichen Daten professionell zu schützen.

Eine Lösung, die sowohl die Interessen der Mitarbeiter als auch der Firmen berücksichtigt, gibt es jetzt mit der IDGARD-App. Mit IDGARD tauschen Arbeitnehmer versiegelt Dokumente und Nachrichten im Internet aus, ob vom Smartphone, vom Tablet-PC oder vom Notebook aus.

Mitarbeiter können damit unterwegs auf geschäftliche Unterlagen zugreifen, ohne ihre Firma in Gefahr zu bringen. Bearbeiten können sie die Dokumente in beliebigen Apps. Jeder nutzt also seine gewohnte Umgebung zum Arbeiten und kann Reise- oder Wartezeiten effizient und produktiv nutzen. Der Versand von Dokumenten erfolgt sicher über IDGARD. Zusätzlich gibt es in der App ein schnelles und unkompliziertes Messaging, das Tools mit Sicherheitslücken wie Viber oder Whatsapp überflüssig macht. Zum Beispiel lassen sich Push-Benachrichtigungen empfangen und versenden. Man ist also in Echtzeit mit dem Büro verbunden und profitiert von kurzen Reaktionszeiten. Die Daten stehen offline zur Verfügung, also auch bei schlechtem Empfang.

Das Unternehmen stellt mit dem Einsatz der IDGARD-App sicher, dass Daten vom Smartphone nicht versehentlich mit anderen Diensten synchronisiert werden, etwa mit solchen von Google und Apple in den USA. Das Konto des Mitarbeiters kann im Ernstfall remote geschlossen und zurückgesetzt werden. Und damit keine Unordnung entsteht, ist der neueste Datensatz automatisch zu erkennen und zu bearbeiten.

Im Hintergrund von IDGARD arbeitet die Sealed Cloud. (2) Alle genutzten Daten werden in einem deutschen Rechenzentrum gelagert. Allerdings werden Daten auf den Servern der meisten Rechenzentren unverschlüsselt verarbeitet. Das ist gefährlich, weil zum einen die Betreiberfirma des Datenzentrums selbst, zum anderen ein Angreifer von außen die Daten abzapfen können. Die Sealed Cloud Technologie von dem Münchner Sicherheits-Unternehmen Uniscon (3) verschließt daher diese Sicherheitslücke auf technische Weise. Bei der Sealed Cloud hat nicht einmal der Hersteller Unsicon selbst den Schlüssel zum Dechiffrieren der Informationen in der Cloud. Nur der Cloud-Nutzer selbst hat den Schlüssel zu diesen Daten und somit vollständige Kontrolle.

Ein Schutz der Verbindungsdaten ist ebenfalls sichergestellt. Verbindungsdaten können zum Beispiel verraten, wer mit wem, wann, wie oft und wie lange über das Internet verbunden war.

Sie verraten also potenziell die Strategie eines Unternehmens, Firmen-Informationen und Beziehungen. Bei der Sealed Cloud kann der Betreiber der Cloud die Verbindungsdaten nicht einsehen.

Zudem gewährleistet die Sealed Cloud, dass alle Daten des Nutzers in der Sealed Cloud bleiben. Das gilt gerade auch für sensible Dokumente, die heute beim Betrachten auf Smartphones und Tablets oft im Hintergrund auf unsichere Server geladen werden, zum Beispiel in die iCloud. Mit der Sealed Cloud wird verhindert, dass iCloud und andere US-Dienste mit Daten beliefert werden. Im Technologiewettbewerb „Trusted Cloud“ des Bundeswirtschaftsministeriums (BMWi) war die Sealed Cloud dank dieser Eigenschaften erfolgreich im Wettbewerb mit 115 anderen Lösungen. Seither fördert das BMWi die Weiterentwicklung dieser Technologie für die deutsche Industrie.

Dank dieser Sicherheitsfunktionen kann man bei IDGARD von einem abhörsicheren Kommunikationsdienst für Unternehmen sprechen. Mitarbeiter können mit IDGARD sicher und ohne weitere Software Dokumente mit ihren privaten Smartphones und Tablets austauschen, Nachrichten schreiben und abhörsicher chatten. Sie können also von ihren privaten Smartphones und Tablets mit Kunden, Partnern und Lieferanten sicher kommunizieren und in Teams arbeiten, ohne Sicherheitsprobleme zu verursachen.

(1) http://www.sueddeutsche.de/news/karriere/arbeit-gefaehrliche-mischungprivate-technik-fuer-den-job-nutzen-dpa.urn-newsml-dpa-com-20090101-140410-99-02532
(2) http://www.uniscon.de/sealedcloud/
(3) http://www.uniscon.de/firmenprofil/

Über Uniscon GmbH –

Uniscon – Kommunikation und Datenaustausch einfach | sicher | compliant – entwickelt technische Lösungen zur sicheren und bequemen Online- Geschäftskommunikation. Der Service ID|GARD 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, 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

PR-Agentur Xpand21 GmbH
Doris Loster
Romanstr. 10
80639 München
0170 / 21 53 172
uniscon@xpand21.com
www.pr-agentur-xpand21.de