Götz Piwinger
Geschäftsführer GERMAN CLOUD

meine Firmendaten bleiben in Deutschland!

Das private Smartphone bringt die (Daten-)Seuche ins Unternehmen

BYOD: Die unterschätzte Spionage

BYOG steht für „Bring your own device“. Damit kann zum einen gemeint sein, dass Mitarbeiter ihre privaten Smartphones für die Arbeit nutzen dürfen und dafür ggf. entschädigt werden. Zum anderen bedeutet BYOG auch schlicht, dass man sein privates Gerät mit zur Arbeit bringt. In jedem Fall bringen Sie mit Privatgeräten Gefahren ins Unternehmen.

Warum braucht meine Taschenlampen-App ein Update?

Haben Sie jemals gefragt, warum eine Wasserwaagen-App ein Update braucht? Nein. Wir fragen überhaupt nicht mehr, sondern drücken einfach auf o.k. Damit die Anwendung endlich wieder läuft. Wer sich die Nutzungsbedingungen bei der Zustimmung zum Update ansieht erkennt schnell, was dahinter steckt; Der komplettem, allgegenwärtige und jederzeitige Zugriff auf die Smartphonedaten, verbunden mit den Erlaubnis an den Anbieter, dass dieser damit tun und lassen kann was er will. Er darf sogar in Ihrem Namen kostenpflichtige Anwendungen bestellen!

Zugriff auf alle Anwendungen heißt auch: Ortungsdienste jederzeit anzapfen, jederzeit Mikrofon oder Kamera aktivieren. Außerdem dürfen alle Email, SMS, Whatsapp, etc. mitgelesen werden. Alle im Smartphone gespeicherten Kontakte dürfen ausgelesen werden. Und ihre schönen Fotos auch. Da wird es einem heiß und kalt.

Was hat mein Unternehmen mit meinem privaten Smartphone zu tun?

Ihr Unternehmen stellt Ihnen beispielsweise ein Blackberry zur Verfügung. Das ist natürlich bei Weitem nicht so cool wie das private Iphone oder Samsung S5. Außerdem haben Sie ja privat sowieso eine Flatrate. Deshalb wird auch gerne das Privatgerät für dienstliche Zwecke genutzt. Wie in der PRISM Affäre festgestellt, werden die Mails bei US Anbietern ohnehin weitergegeben. Also kann ich folgende auslesen: Ihren Standort, Bewegungsprofil, Ihre (Kunden-)Kontakte, Bilder und Dateien, mitgeschnittene Gespräche und Ihre Fotos. Wir wissen derzeit nicht was mit Passwörtern geschieht, die über ein Smartphone eingegeben werden, welches Abhör-Apps installiert hat. Das kann und darf der Arbeitgeber nicht akzeptieren.

In einem aktuellen haben wir die ausgelesenen Handydaten eines Nutzers mit dessen Kommunikation in sozialen Netzen verglichen. Die Ergebnisse sind –leise gesagt- alarmierend.

Big Data: Wer liest die Daten aus?

Die ungeheure Menge von Daten, die auf weltweiten Servern liegt, muss ausgelesen und sortiert werden. Zum einen kann ich die Daten käuflich erwerben. Das ist Tagesgeschäft in der Werbe- und Internetbranche. Der Käufer benötigt die Daten entschlüsselt und sinnvoll zusammengefügt. Dafür haben nahezu alle US-Cloudanbieter Tochterfirmen (Datamining) gegründet. Der Cloudanbieter VERschlüsselt und darf verschlüsselte Daten verkaufen. Die Tochterfirma ENTschlüsselt die Daten auf geheimnisvolle Weise und kann diese zu hohem Wert weiterveräußern.

Wem es zuerst gelingt, die Daten aller Provider zu vernetzen, wird mächtiger sein, als wir uns vorstellen wollen. Zurück zum unserem Unternehmen.

Firmenspionage der übelsten Sorte

Wir konnte sehen, welche Gefahren davon ausgehen, wenn private Endgeräte im Unternehmen genutzt werden. Dadurch sind Unternehmenswerte, wie Kunden/Lieferanten, Preise, Mitarbeiterwissen gefährdet. Später fragt man sich: Wie war es möglich, dass wir diese Spitzenkraft verlieren? Warum war der internationale Wettbewerb so viel günstiger? Und so weiter.

Maßnahmen gegen Handyspionage

Zunächst gibt es zwei technische Möglichkeiten: Erstens überprüfe ich alle Apps auf den privaten Hady mit einem Tool für statische und dynamische Code Analyse. Das muss jedes Mal, wenn eine neue App geladen wird erfolgen. Der Besitzer des Handys muss dem natürlich zustimmen.

Variante 2: Der Arbeitgeber stellt stets aktuell Geräte zur Verfügung, die von der zentralen IT entsprechend gesichert werden. Bei unterschiedlichen Modellen im Einsatz ist das eine Herausforderung.

Variante 3: Könnte Windows 8 sein, Denn dann laufen alle Geräte in eigenen AD´s (Active Directories) und sind entsprechend gut administrierbar. In der Kombination mit W8-tauglichen Tabletgeräten könnte man sich vorstellen, dass Windows 8 ff. eine gute Zukunft bevorsteht.

Es fehlen derzeit standardisierte Prüfverfahren für Apps. Auch gibt es keine Zertifizierungsstelle, die Apps als sicher kennzeichnet. Die Arbeitsgruppe „SECU-APP“ von German Cloud untersucht derzeit die Möglichkeiten, sichere Apps über ein eigenes Portal anbieten zu können.

Das Wichtigste: Der Mensch

Das allerbeste ist es, wenn es gelingt, die Einsicht Sensibilisierung und Aufmerksamkeit der Beschäftigten zu wecken. Ein Weg dorthin führt über rollenspezifische Weiterbildungsmaßnahmen im Unternehmen. Passende Sensibilisierungs-Schulungen gibt es zum Beispiel auf der Webseite von German Cloud.

Fazit:

Die Spionagegefahr durch die Nutzung von privaten Smartphones im Unternehmen ist als „sehr gefährlich“ einzustufen. Fortschrittliche Unternehmen bringen Ihre Mitarbeiter durch ein Sensibilisierungs-Training mit Prüfung und nehmen dies als Zusatzvereinbarung in den AV auf. Denn am Ende haftet der Unternehmer/Geschäftsführer persönlich für Datenschutzverletzungen im Unternehmen.

Kontakt:

German Cloud
Universitätsstrasse 3
D-56070 Koblenz
info@german-cloud.de