Unternehmenssicherheit in Gefahr durch Smartphones? Oder was wir aus der Causa WhatsApp im Unternehmen lernen sollten

Unternehmenssicherheit in Gefahr durch Smartphones? Oder was wir aus der Causa WhatsApp im Unternehmen lernen sollten

In den vergangenen Tagen haben Datenschutz-Behörden ihre Kritik am SMS-Konkurrenten für Smartphones "WhatsApp" für den automatisierten Adressbuchabgleich geäußert. Um diese (eine der weltweit fünf beliebtesten) App nutzen können, wird das gesamte Adressbuch dem Anbieter zugänglich gemacht. Die Nutzung ist freilich freiwillig, doch können sich diejenigen, die im Adressbuch des Nutzers gespeichert sind und eigentlich kein WhatsApp nutzen wollen, nicht dagegen wehren. Zudem wurde die App in der Vergangenheit schon oftmals aufgrund der grundsätzlich unzureichenden Sicherheit kritisiert. In diesem Zusammenhang entstehen nunmehr auch Risiken für Unternehmen und die Vertraulichkeit von Daten.
Nicht zuletzt aufgrund des sog. "Smartphone-Booms" durch sehr benutzerfreundliche Geräte und Systeme wie das Apple iPhone oder den Android-Betriebssystemen, ist die Nutzung von sog. Mobile Devices auch in Unternehmen sehr verbreitet. Geräte, Systeme und Apps sind aber primär für den Konsumentenmarkt und nicht für das Geschäftsumfeld entwickelt worden, so dass die Schwerpunkte mehr auf Bedienungsfreundlichkeit als auf Sicherheit und Rechtskonformität liegen.
Die Nutzung solcher Systeme aus unternehmerischer Sicht führt zu entsprechenden Risiken, wenn beispielsweise Kalender online synchronisiert, E-Mails abgerufen oder - wie bei der Nutzung von WhatsApp - Daten aus dem Adressbuch des Nutzers (automatisch oder nach Bestätigung) mit einem fremden Anbieter (der auch noch in den USA sitzt, was datenschutzrechtlich ein zusätzliches Problem darstellt) abgeglichen werden.
Dies zeigt - und dies gilt nicht nur für WhatsApp -, dass diese Systeme oftmals datenschutzrechtlich und zum Teil mehr noch im Hinblick auf die Informationssicherheit höchst problematisch sind. Diese mobilen Systeme bieten in der Regel nicht die erforderlichen Sicherheitsfunktionalitäten (wie z. B. Verschlüsselung, zentrale Administration oder Benutzerauthentifizierung), wie es bei anderen mobilen Geräten - Laptops - heute zum aktuellen Stand der Technik gehört.
Diese Problemstellung wird durch den aktuellen Trend des "bring your own device" (BYOD) noch verstärkt, also die Nutzung von privaten Geräten für geschäftliche Zwecke und mit Zugriff auf geschäftliche Systeme. Anders als bei rein dienstlichen Geräten, die idealerweise durch die IT zentral verwaltet und streng kontrolliert werden, bestehen bei der (auch) geschäftlichen Nutzung privater Geräte Probleme dahingehend, dass die Beschäftigten beim Nutzungsverhalten oftmals keine Unterscheidungen zwischen Privat- und Arbeitsleben vornehmen und dass auch technisch keine Trennung zwischen beiden Nutzungsarten vorgenommen werden kann. Folglich werden ungeprüfte Programme/Apps installiert, die Schadcode enthalten können oder den o. g. Datenabgleich mit z. T. sensiblen Unternehmensdaten vornehmen, was einen Datenschutzverstoß darstellen kann.
Jede IT- und Geschäftsleitung sollte sich daher fragen, ob die Nutzung von aktuellen IT-Trends (wie die Nutzung von Smartphones oder einer BYOD-Strategie) mehr Wert oder mehr Gefahr für das Unternehmen darstellt. Im Rahmen der Nutzen-Risiko-Abwägung ist es erfahrungsgemäß zielführend, dies in den jeweiligen Unternehmensbereichen und vor allem in der Geschäftsführung durch einen Praxis-Workshop zu diskutieren? schließlich ist oftmals auch die Unternehmensleitung die treibende Kraft bei der Umsetzung "mobiler Strategien".
Näheres unter http://www.uimc.de/praxis-workshops

UIMC Dr. Voßbein GmbH
 Co. KG
Dr. Jörn Voßbein
Nützenberger Straße 119
42115 Wuppertal
Tel.: 0202 / 265 74 - 0
Fax: 0202 / 265 74 - 19
E-Mail: consultants@uimc.de
Internet: www.UIMC.de
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=521292" width="1" height="1">

Pressekontakt

UIMC

42115 Wuppertal

consultants@uimc.de

Firmenkontakt

UIMC

42115 Wuppertal

consultants@uimc.de

Die UIMC DR. VOSSBEIN GmbH & Co KG, gegründet 1997, hat die damals seit über 10 Jahren laufenden Beratungsgeschäfte der Partner und Gesellschafter Dr. Reinhard Voßbein, Professor für Wirtschaftsinformatik und Dr. Jörn Voßbein in einer Beratungsgesellschaft vereint. Seit 1999 ist Dr. Heiko Haaz, der schwerpunktmäßig den Datenschutz betreut, als dritter Partner zur UIMC gestoßen.Kerngebiete ihrer Arbeit sind die IT-Sicherheit und der Datenschutz. Sie kann beachtliche Referenzen von Institutionen aus einer Vielzahl von Wirtschaftszweigen sowie Behörden aufweisen und hat eine umfangreiche Projekt- und Betreuungserfahrung, auch international. Felder, auf denen ihre Erfahrungen branchenführend sind.Ihr Leistungsspektrum/Produktprogramm unterscheidet sich von dem anderer Beratungsunternehmen: Sie setzt ein toolgestütztes Analyse- und Konzeptionierungssystem mit einer wissensbasierten Expertensystem-Komponente in Form einer Shell ein, das ständig ausgebaut und ergänzt wird. Dieses ermöglicht die rationelle und kostengünstige Analyse betriebswirtschaftlicher sowie IT-sicherheits- und datenschutzspezifischer Kern- und Teilgebiete sowie die Berichterstattung und Konzeptionserstellung, womit Rationalisierungs- und Effizienzvorteile für ihre Kunden generiert werden. Im Verlaufe der Zeit wurden eine Vielzahl von individuellen Füllungen für diese Shell erarbeitet und in diese eingebracht. Firmenindividuelle Füllungen sind konzeptionell vorgesehen und auf der Basis der Struktur des Tools komplikationslos zu realisieren.Sie führt Workshops, Schulungen sowie Fortbildungsmaßnahmen auf den Sektoren IT-Sicherheit und Datenschutz mit ihrer Marke UIMCollege auch als Inhouse-Veranstaltungen durch.