01/2013

UIMCommunic@tion

Dies ist keine stille Post:
Um interne Verteilung wird gebeten!

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Unternehmenssicherheit in Gefahr durch Smartphones?

Oder was wir aus der Causa WhatsApp im Unternehmen lernen sollten

[Pressemitteilung vom 31.01.2013] 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 zu 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 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“.

Mehr Pressemitteilungen und eine Historie der UIMCommunic@tion-Newsletter finden Sie hier:
www.UIMC.de/communication

Was ist UIMCommunic@tion?

UIMCommunic@tion ist der neue Informationsservice der UIMC und der UIMCert. Dieser „Newsletter“ wird regelmäßig erscheinen, Ihnen stets der Rechnung beigelegt und auf unserer Internetseite unter **www.UIMC.de/Communication** veröffentlicht.

Wenn Sie diesen Service auch dann nutzen möchten, wenn Sie keine Rechnung erhalten, können Sie die Zusendung auch unter o. g. Internetadresse bestellen oder schicken Sie an **communication@uimc.de** eine E-Mail.

Viel Spaß beim Lesen!

Haben Sie Fragen?
UIMC Dr. Vossbein GmbH & Co KG
Nützenberger Straße 119
42115 Wuppertal
Tel.: (02 02) 2 65 74 - 0
Fax: (02 02) 2 65 74 - 19
E-Mail: consultants@uimc.de
Internet: www.UIMC.de

auch als Download unter
www.UIMC.de/Communication

UIMCommunic@tion

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Hinweise für die sichere Nutzung von (dienstlichen) Smartphones!

Es sollten keinerlei Änderungen an den Sicherheitseinstellungen der Geräte vorgenommen werden (wie beispielsweise Verschlüsselung etc.). Auch sollten keine Veränderungen am Betriebssystem vorgenommen werden, die nicht vorab von der IT-Abteilung genehmigt wurden (z. B. Jailbrack oder andere „Customed ROMs“).

Es gilt zu beachten, dass auch Mobiltelefone von Schadsoftware befallen werden können, die über SMS, MMS etc. verbreitet wird. Gleiches gilt für den Download von Programmen (Apps). Bei Unregelmäßigkeiten sollte die IT-Abteilung unverzüglich informiert werden. Zudem sollte die IT-Abteilung gefragt werden, ob der Download einer App sicherheitstechnisch akzeptiert ist.

Es sollten ausschließlich von der IT-Abteilung freigegebene Apps installiert und genutzt werden. Das Herunterladen aus offiziellen Quellen (z. B. Apple Appstore oder Google Play Store) verringert das Risiko von Schadcodes.

Die auf dem Smartphone gespeicherten Daten sind entsprechend zu schützen. Hierzu ist ein Code/Passwort zur Anmeldung zu nutzen. Das Passwort ist mindestens numerisch und 4 Zeichen lang. Bei einer Inaktivität von maximal zwei Minuten sollte sich der Passwortschutz automatisch aktivieren.

Dies gilt auch für die SIM-Karte und die Mailbox. Selbst wenn die Mailbox nicht genutzt wird, sollte die voreingestellte PIN geändert werden, um eine Fremdnutzung zu verhindern. Es ist eine sichere, schwer zu erratene PIN zu verwenden.

Der beste Schutz ist hierbei jedoch, möglichst wenige vertrauliche Daten auf dem Mobiltelefon zu speichern. Hochvertrauliche Daten, E-Mails etc. sollten daher nicht unverschlüsselt auf dem Smartphones gespeichert werden.

Mehr Tipps finden Sie in der nächsten Ausgabe vom UIMCommunication-Newsletter oder erfahren Sie bei Ihrem Ansprechpartner!

Save the Date

20.03.2013:
Praxis-Workshop „Social Media im Unternehmen“ in Wuppertal

24.04.2013:
IT-Trends Sicherheit (Vortrag der UIMC zum Thema „Faktor Mensch“ in der IT-Sicherheit) in Bochum

14.-16.05.2013:
IT-Sicherheitskongress des BSI in Bonn/ Bad Godesberg

Weitere Infos & Termine:
www.UIMC.de/Termine

UIMCollege-Seminare

[kurzer Auszug]

- **Auditierung und Zertifizierung gemäß ISO/IEC 27001** [16.04.2013 in Wuppertal]
- **Datenschutz in katholischen Krankenhäusern** [05.03.2013 in Saarbrücken]
- **Datenschutz-Management, Teil 2 / Vertiefung** [05.03.2013 in Wuppertal]
- **Datenschutz-Management gemäß DSG NRW** [15.03.2013 in Wuppertal]

Mehr Seminare unter
www.UIMCollege.de

Bitte senden Sie mir zu den angekreuzten Themen weitere Informationen zu:

- „Unternehmenssicherheit in Gefahr durch Smartphones?“
- Bitte senden Sie mir zukünftig den UIMCommunic@ation-Newsletter und regelmäßig weitere interessante Informationen per E-Mail zu! Mir ist bekannt, dass ich der künftigen Zusendung jederzeit formlos durch die Zusendung einer E-Mail an communication@uimc.de widersprechen kann.

E-Mail: _____ Unterschrift: _____

per Fax an (0202) 265 74 - 19 oder formlos per Mail an communication@uimc.de