04/2013

UIMCommunic@tion

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

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Mobile Devices und Bring Your Own Device

oder: Wildwuchs bringt Unternehmen in Schwierigkeiten

[Pressemitteilung vom 02.05.2013] Die Vorteile der mobilen Arbeit mit Smartphones und Laptops liegen auf der Hand: erhöhte Verfügbarkeit, schnellere Reaktionszeiten, größere Flexibilität und damit einhergehend eine größere Zufriedenheit der Mitarbeiter. Doch die Nutzung dieser Mobile Devices birgt auch Gefahren für Datenschutz und Informationssicherheit.

Viele Risiken, die hierbei existieren, sind grundsätzlich nicht neu: Neben Diebstahl und Verlust des Geräts sind es vor allem Schadprogramme und die unsachgemäße Handhabung, die zu einem Vertraulichkeitsverlust sensibler Mitarbeiterdaten führen können und damit auch datenschutzrechtlich relevant sind. Aber auch die Vermischung von privaten und dienstlichen Daten ist in diesem Zusammenhang nicht unproblematisch.

Während es für Desktop- und mobile PCs (Laptops/Notebooks) schon umfangreiche und etablierte Verfahren und Produkte gibt, um die Datensicherheit zu gewährleisten, stehen diese für Smartphones und Tablets noch aus. Denn die zurzeit verfügbaren Smartphones sind in der Regel für Konsumenten und deren Bedürfnisse entwickelt und sollen eher durch Features und Benutzerfreundlichkeit als durch Sicherheit begeistern. Auf zahlreiche sicherheitstechnische Anforderungen wie zum Beispiel die Verschlüsselung des Datenspeichers, den Einsatz von Firewall und Virenscanner sowie komplexe Beschränkungen von Zugangsrechten haben die Smartphone-Hersteller bislang noch nicht oder nur unvollständig reagiert (Blackberry bildet hierbei teilweise eine Ausnahme). Somit wurden viele Geräte an den Sicherheitsbedürfnissen der Unternehmen vorbei entwickelt.

Umso wichtiger ist es, dass Unternehmen, die mobile Personalarbeit einführen oder erlauben möchten, entsprechende Regelungen in Form von Organisationsanweisungen und Betriebsvereinbarungen sowie technische Maßnahmen zur IT-Sicherheit treffen, die die Sicherheitsrisiken mindern, wenn sie sie auch nicht eliminieren können. Dies ist auch – oder insbesondere – bei einer „Bring your own Device"-Strategie zu beachten (BYOD), bei der Mitarbeiter ihre privaten Endgeräte dienstlich nutzen dürfen. Zum Teil wird auch ein „inoffizielles" BYOD an der IT-Abteilung und der IT-Sicherheit vorbei „eingeführt", indem sich Mitarbeiter E-Mails auf Ihre Smartphones weiterleiten, Internetkalender zur Teamkoordination oder Cloud-Speicher für die Ablage und den Austausch von Dateien nutzen.

Mobile Devices werden demnach an den Sicherheitsanforderungen vorbei entwickelt und zum Teil in den Unternehmen ohne Beteiligung der Sicherheitsverantwortlichen eingeführt. Es ist aber unumgänglich, dass Unternehmen nicht nur verbindliche Richtlinien schaffen, sondern die Mitarbeiter auch für die sicherheitstechnisch und datenschutzrechtlich relevanten Themen sensibilisieren. Denn viele notwendige Maßnahmen sind – mangels technischer Lösungen noch stärker als bei anderen Geräten – durch den Mitarbeiter selbst umzusetzen. Neben Präsenzschulungen durch die IT-Abteilung oder den Datenschutzbeauftragten sind E-Learning-Lösungen denkbar, mit denen eine kontinuierliche Sensibilisierung erreicht werden kann, da die Informationen laufend aktualisiert werden.

Fazit: Bevor Mobile Devices und BOYD schleichend Einzug halten, sollten über entsprechende Einführungskonzepte und Schulungen die Wahrung der Sicherheit und des Datenschutzes sichergestellt werden.

Mehr Pressemitteilungen und den kompletten Artikel „Risiken reduzieren - So schützen Sie Ihre Personaldaten" (veröffentlicht im „personal manager 2/2013") finden Sie hier: www.UIMC.de/communication

Praxis-Workshop „Mobile Devices"

Innerhalb des UIMCollege-Praxis-Workshops diskutieren wir mit Ihnen die Risiken, die mit der Nutzung von Mobile Devices (also Laptops und Smartphones) und durch das Verfolgen einer BYOD-Strategie im Hinblick auf den Datenschutz und die Informationssicherheit bestehen. Auch werden Ihnen entsprechende Hinweise gegeben, wie diesen Risiken begegnet werden kann. Hierbei betreiben wir keine Systemberatung, sondern zeigen vielmehr Risikominderungsstrategien auf.

19.06.2013, 13:30 Uhr

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

Vorherige Info-Briefe einsehen?
www.UIMC.de/Communication

UIMCommunic@tion

Interessantes zu Datenschutz und Informationssicherheit präsentiert von UIMC und UIMCert

Tipps zum sicheren, datenschutzkonformen Einsatz von Fernwartungs-Tools

Ein Fernwartungs-Tool erlaubt den Fernzugriff auf PCs und deren Fernsteuerung. Hierzu werden Bildschirminhalte sowie Tastatureingaben und Mausbewegungen über das Netzwerk übertragen. Die wesentliche Arbeitserleichterung für Administratoren besteht darin, dass sie ihren Arbeitsplatz während der Wartung oder des Supports nicht mehr verlassen müssen.

Hierbei sind folgende Einstellungen **bei der Konfiguration** vorzunehmen:

1. Authentifizierung der Administratoren bei der Verbindungsaufnahme durch Eingabe eines Passworts;
2. Verbindungswünsche von Administratoren durch Mitarbeiter explizit bestätigen lassen;
3. Änderungen der Tool-Einstellungen nur von Administratoren ermöglichen.

Ferner ist Folgendes **bei der Nutzung** zu beachten:

1. Es sind Verschlüsselungsverfahren zu etablieren, wenn auf Rechner zugegriffen werden soll, auf denen Daten mit hoher Sensitivität (z. B. personenbezogen) verarbeitet werden.
2. Alle beteiligten PCs sind über restriktiv konfigurierte Firewalls zu schützen.
3. Die (unverschlüsselte) Übertragung der Daten über offene Netze/ Internet ist zu verhindern.
4. Eine Fernwartung durch Dritte ist nur auf Basis expliziter Datenschutzvereinbarungen mit dem Dienstleister zulässig (Rücksprache mit Datenschutzbeauftragten empfehlenswert).
5. Sämtliche Wartungsvorgänge sollten anhand eines Wartungsprotokolls nachvollziehbar sein.

Mehr Tipps finden Sie in der nächsten Ausgabe vom UIMCommunic@tion-Info-Brief oder erfahren Sie bei Ihrem Ansprechpartner!

Bisher erschienene Hinweise/Tipps:
„Tipps für die Beantwortung telefonischer Anfragen/ Auskünfte“ (03/2013)
„Nutzung von sozialen Netzwerken“ (02/2013)
„Sichere Nutzung von Smartphones“ (01/2013)

Save the Date

Der BSI IT-Sicherheitskongress selbst bietet neben interessanten Fachvorträgen auch ausreichend Möglichkeiten, im Rahmen der Begleitausstellung informative Fachgespräche zu führen. Sie finden eine vielfältige Auswahl an Anbietern zur IT-Sicherheit.

Besuchen Sie uns auf unseren Messestand; wir halten ein kleines Bonbon für Sie bereit.

IT-Sicherheitskongress, Bonn
14. bis 16.05.2013

eCollege (Update)

Innerhalb des eCollege-Pakets „Classic“ haben nun die Nutzer ein Update erhalten. Mit der neuen Funktion kann die erfolgreiche Selbstschulung nun **teilautomatisiert nachverfolgt** werden, wie z. B. das generieren einer entsprechenden Bestätigungsmail an eine vorher definierten Empfänger im Unternehmen (z. B. Personalabteilung).

Für die Nachverfolgung (mittels E-Mail oder Formular) kann zusätzlich auch die UIMC beauftragt werden, so dass keinerlei Organisationsaufwand im Unternehmen verbleibt.

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

- Praxis-Workshop „Mobile Devices und BYOD“ (19.06.2013)
- „Risiken reduzieren - So schützen Sie Ihre Personaldaten“ (Fachartikel im personal magazin)
- **Unser Tipp:** Bitte senden Sie mir zukünftig den UIMCommunic@tion-Info-Brief und regelmäßig weitere interessante Informationen per E-Mail zu! Mir ist bekannt, dass ich der künftigen Zusendung jederzeit formlos per 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