Mobile Devices und Bring Your Own Device: Wildwuchs bringt Unternehmen in Schwierigkeiten

Mobile Devices und Bring Your Own Device: Wildwuchs bringt Unternehmen in Schwierigkeiten

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 im Unternehmen Einzug halten, sollten über entsprechende Einführungskonzepte und Schulungen die Wahrung der Sicherheit und des Datenschutzes sichergestellt werden.
 www.uimc.de/communication

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: http://www.uimc.de
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=531247" 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.