

TREND-MAGAZIN FÜR MOBILES MANAGEMENT

MOBILE  
CHALLENGES

# MOBILE

# BUSINESS

5-6.17



**MDM**  
GLÄSERNE  
MITARBEITER?

**RISIKO**  
MOBILE BANKING?

# HAUPTSACHE BEQUEM

STUDIE BESTÄTIGT: *Bei mobilen Bankgeschäften geht Bequemlichkeit oftmals vor Sicherheit*



... **INDUSTRIE-HANDEHELDS**: AKTUELLE MODELLE IM ÜBERBLICK ...

... **VERSICHERUNG DIGITAL**: **INSURTECHS BRINGEN DEN MARKT IN SCHWUNG** ...

ÖSTERREICH: 6,60 EUR  
LUXEMBURG: 6,90 EUR  
SCHWEIZ: 12,00 SFR  
DEUTSCHLAND: 5,90 EUR





„SCHLÜSSELANHÄNGER“ FÜR  
MEHR SICHERHEIT

# UNSICHTBAR IM HINTERGRUND

Wenn der Mitarbeiter sein eigenes Smartphone mitbringt, bleibt dann die **SICHERHEIT FÜR UNTERNEHMENS DATEN** auf der Strecke? Nicht zwingend, denn es gibt smarte Lösungen – z.B. in Form eines „Schlüsselanhängers“ –, auf die Unternehmen zurückgreifen können.

**B**ring Your Own Device (BYOD) wird immer populärer. Die Vorteile: nur ein mobiles Gerät für private und berufliche Themen; man entscheidet selbst, welches mobile Gerät verwendet wird; Entfall der aufwändigen Verwaltung physischer Geräte; Unabhängigkeit von vorgegebenen Nutzungsfristen und in der Regel niedrige Kosten für Firmen.

BYOD bedeutet jedoch auch, dass wichtige, vertrauliche Unternehmensdaten auf einem „fremden“, d.h. privaten, mobilen Gerät gespeichert werden. Die Herausforderung ist hier, trotzdem jederzeit die Sicherheit der Unternehmensdaten sicherzustellen. So müssen im normalen Einsatz alle Unternehmensdaten vor unautorisiertem Zugriff geschützt sein. Bei Verlust muss das Unternehmen die Möglichkeit haben, alle Unternehmensdaten

auf dem Gerät zu löschen. Hier ist natürlich zu beachten, dass das Gerät rechtlich dem Mitarbeiter gehört, der am Ende selbst entscheiden darf, was mit seinem Gerät im Ernstfall passiert.

Daher sollten Unternehmensdaten möglichst nur in dedizierten Apps gespeichert werden. Diese können dann, flexibel nach der Anforderung, durch zusätzliche Authentifizierungen wie Passwort, Fingerabdruck, Smartcard und Verschlüsse-

Smartcards, auf denen die Schlüssel in spezieller Hardware, einem sogenannten „Secure Element“, sicher gespeichert sind, bereits in der Praxis erprobt.

Aber eine zusätzliche Smartcard und entsprechende mobile Lesegeräte sind oft sperrig und unhandlich im mobilen Einsatz. Ganz neu sind an dieser Stelle z.B. kleine, mobile „Schlüsselanhänger“, welche die erforderliche Sicherheit praktisch unsichtbar im Hintergrund mitbringen. Diese Anhänger sind drahtlos via Bluetooth mit einem oder mehreren mobilen Geräten des Mitarbeiters verbunden und schützen so jederzeit alle wertvollen Unterneh-




lung und/oder Software-Container geschützt werden. Nur eine Passwortabfrage (oder Fingerabdruck) zur Authentifizierung und Datenentschlüsselung stellen dabei keinen wirksamen Schutz dar.

## Physische Trennung

Mobile Geräte bieten heute bereits das größte Einfallstor für Cyber-Attacken, doch lässt es sich durch physische Trennung von Daten und Schlüsseln nachhaltig schließen. Dadurch sind alle Unternehmensdaten auch bei Diebstahl oder Verlust sicher geschützt. Bei Desktop oder Laptops ist eine solche Trennung, z.B. durch den Einsatz von

mensdaten. Diese Off-Device-Key-Management-Lösungen, wie z.B. der Cgtoken von Certgate, lagern sämtliche Zugangsdaten auf eine Mini-Smartcard aus, sind durch eine Pin geschützt und ermöglichen so eine drahtlose Zwei-Faktor-Authentifizierung, E-Mail- und Datenverschlüsselung sowie Dokumentensignatur. Selbst bei Verlust des Gerätes ist ein unautorisierter Zugriff auf Unternehmensdaten und -funktionen nicht möglich. So behält die Firma die Hoheit über den Datenzugriff – auch auf den Geräten ihrer Mitarbeiter.

Bei der Auswahl solcher Schlüsselanhänger ist es wichtig, dass das Produkt robust ist, mit Windows-, Android- und Apple-Geräten funktioniert und am besten auch schick und wertig am Schlüsselbund des Chefs oder Mitarbeiter aussieht. 

JAN C. WENDENBURG, LEA SOMMERHÄUSER