Mobil arbeiten
Sicher, flexibel, überall

Ihr Experte
Stephan Sachweh
Geschäftsführer
Pallas GmbH
stephan.sachweh@pallas.com

Termine vereinbaren, E-Mails senden, im Firmenadressverzeichnis suchen: das geht heute prinzipiell jederzeit und überall, jedenfalls solange Smartphone, Tablet oder Laptop per WLAN oder Mobilfunk mit dem Internet verbunden ist.

7

Vor dem Kundenbesuch noch schnell dessen Website anschauen, nachher die Pünktlichkeit der geplanten Bahnverbindung prüfen, in der Bahn den Besuchsbericht verfassen und in die Firmendatenbank hochladen, diese höchst mobilen Erweiterungen von IT und TK sind inzwischen fester Bestandteil unserer Arbeit. Smarte Uhren, Brillen, Kleidung und Körpersensoren bilden die nächste Stufe der mobilen IT.

Ein Drittel Sicherheit, zwei Drittel Funktionalität
Bei Smartphones geht es zunächst einmal um neue Funktionen, die uns den (Arbeits-)Alltag erleichtern. Immerhin wird die Sicherheit inzwischen auch ernst genommen, so ergab eine Umfrage des eco Verbandes der deutschen Internetwirtschaft e.V. zur Internet-Sicherheit 2013, dass der Faktor Sicherheit mit gut einem Drittel Gewicht in die Beschaffungsentscheidung eingeht.

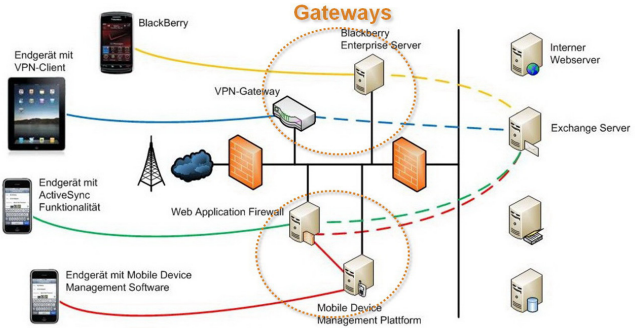
Sicherheit ab Werk
Die Umfrage des eco Verbandes ergab auch, dass nur eine Minderheit der Unternehmen (etwa 10 % der Befragten) für die Zukunft von einer homogenen Smartphone-Infrastruktur ausgeht. Größere mittelständische und erst recht Großunternehmen müssen sich stets um mehrere Betriebssysteme (Android, Apple iOS, Windows Phone, Blackberry OS) kümmern. Das ist tatsächlich auch ein Sicherheits-Plus: Systeme mit Artenvielfalt sind weniger anfällig für Infektionen als solche einer Monokultur. Auch in anderer Hinsicht bringen Smartphones bereits eingebaute Sicherheit mit:

- Backup ist von Hause aus Standard.
- Meist gibt es abgeschirmte „Sandboxes" für die Apps.

Was zusätzlichen Schutz braucht
Smartphones und Tablets bringen aber auch neue Angriffsflächen in die IT, die zu schützen sind:

- das mobile Gerät selbst: **Schutz des Gerätes**
- die Kommunikation mit dem Gerät: **Verschlüsselung**
- die Unternehmens-Infrastruktur: **Sicherung des Zugangs**

Wichtigste Maßnahme ist die Schaltung eines Gateways zwischen mobilem Gerät und Firmeninfrastruktur, z.B. dem Mailserver.



Das Gateway sorgt für den Zugangsschutz und die Ende-zu-Ende-Verschlüsselung der Kommunikation, hilft also gegen zwei der drei genannten Angriffsvektoren.

Mobile Device Management (MDM)
Für den Schutz des Gerätes selbst gibt es zahlreiche Regeln:

- Apps nur aus vertrauenswürdigen Quellen laden
- Updates machen
- Display-Sperre mit Kennwort (Zugangscode)
- Automatische Abschaltung nach ein paar Minuten
- Geräteverschlüsselung
- Malware-Schutz (jedenfalls bei Android)

Um ein passendes Regelwerk in einem Unternehmen einzuführen und auch bei heterogener Infrastruktur durchzusetzen, greift man am besten auf ein MDM-System zurück.

Spätestens hier sollte man sich beraten lassen oder gleich einen Provider suchen, der das MDM-System betreibt. Dann kann das Unternehmen zentral auch:

- das Gerät zurücksetzen (Wipe)
- das Gerät sperren (Lock)
- das Gerät komplett vom Firmennetz trennen
- die Softwareverteilung zentral steuern

Nicht zuletzt braucht man das MDM-System auch zur Inventarisierung und Verwaltung der mobilen IT-Geräte.

Mobiles Arbeiten mit Laptops – Etablierte Standards

Smartphones und Tablets müssen erst noch den Sicherheitstand vom mobilen Arbeiten mit Laptops erreichen. Für mobiles Arbeiten mit Laptops gibt es etablierte Standards, die eingehalten werden sollten:

- zentrales Management der Software-Installation durch die IT
- Updates machen
- Display-Sperre mit Kennwort
- Automatische Abschaltung nach ein paar Minuten
- Festplattenverschlüsselung
- Virenschutz
- Backup oder – besser noch – keine Speicherung unternehmenskritischer Daten auf dem mobilen Gerät
- Desktop-Firewall
- VPN Zugang zum Unternehmensnetz – idealerweise mit starker Authentifizierung