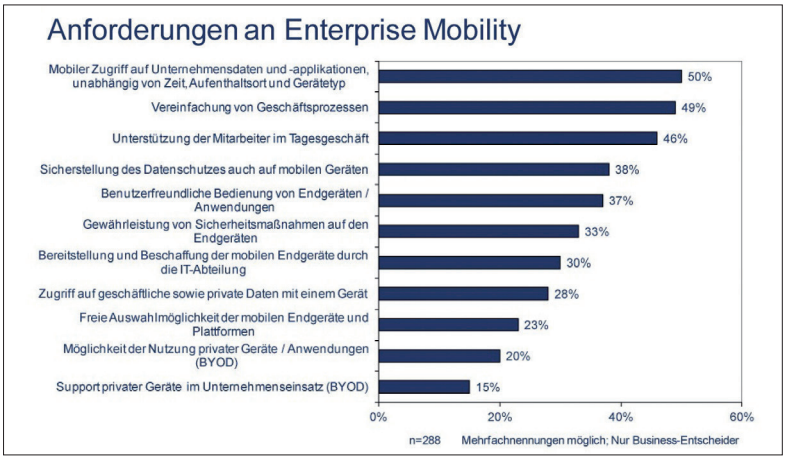
3.2 Security-Konzepte für Smartphone, Tablet und Co.

Große Analystenhäuser sehen Mobile IT als einen der maßgeblichen Trends des Jahres. Experton zählt vor allem Security und Datenschutz in den Bereichen Cloud, Mobility und BYOD zu den wichtigsten Themen, PAC sieht Mobile Collaboration weit vorne. Der Grund: Beschäftigte erledigen ihre Aufgaben zunehmend unabhängig von einem festen Büroplatz, beantworten unterwegs ihre E-Mails, prüfen Termine und greifen auf geschäftskritische Daten wie Finanzzahlen zu.



Details: Der Schutz der Daten sowie die Gewährleistung von Sicherheitsmaßnahmen auch auf mobilen Geräten zählen zu den wichtigsten Anforderungen an ein „Mobile Enterprise". (Quelle: IDC)

Laut der IDC-Studie „Managing Mobile Enterprises" vom September 2012 (www.idc.de/consulting/mc_mob2012.jsp) arbeiten durchschnittlich 54 Prozent der Belegschaft in Unternehmen zumindest hin und wieder mobil. Disruptive Technologien wie die Cloud schaffen die nötigen Voraussetzungen für mobile Infrastrukturen und Zusammenarbeit. Sie ermöglichen Reaktionen in Echtzeit, was insbesondere in den Bereichen Service und Vertrieb Vorteile bringt. So können mobile Mitarbeiter unterwegs auf das Unternehmensnetzwerk zugreifen, um für ihre Kunden Produkt- oder Preisinformationen abzurufen. Wenngleich der Einsatz mobiler Lösungen die Flexibilität und Produktivität erhöht, stellt vor allem die steigende Nutzung privater Endgeräte eine Herausforderung für Unternehmen dar: Diese müssen ihren Mitarbeitern eine möglichst hohe Mobilität bieten, benutzerfreundliche Anwendungen bereitstellen und gleichzeitig die IT-Sicherheit und Compliance-Vorschriften im Blick behalten. Denn die Gefahren sind vielfältig und reichen von Diebstahl über Spionage bis hin zu Datenmissbrauch.

3.2.1 Die IT für den mobilen Zugriff fit machen

Eine durch Datenschutztechnologien gesicherte IT-Umgebung stellt die Basis für die Integration mobiler Endgeräte in die firmeneigene Infrastruktur dar. So schützen Firewalls und Anti-Malware vor Manipulationen der Systeme, beispielsweise durch Viren, Trojaner, Spyware und Phishing. Außerdem hilft eine Intrusion-Detection-Lösung, Angriffe zu entdecken und abzuwehren, während Intrusion-Prevention-Systeme potenzielle Sicherheitslücken frühzeitig aufdecken und die Beseitigung von Schwachstellen ermöglichen. Eine solche Absicherung der Infrastruktur muss als Grundvoraussetzung gegeben sein – sonst entwickelt sich der mobile Zugang schnell zur Achillesferse der Unternehmens-IT.

3.2.2 Autorisierte Nutzung durch Zugriffskonzepte

Auch die Bestimmung von Richtlinien für Endgeräte und Nutzergruppen ist ein wichtiger Bestandteil des Mobile-Security-Konzepts. Denn: Ein umfassendes Identity-Access-Management (IAM) mit entsprechenden Zugriffskonzepten ist entscheidend, um in Zeiten von BYOD und Online-Collaboration eine kontrollierte Nutzung der ICT-Ressourcen zu gewährleisten. Innerhalb der Identitätsarchitektur können Unternehmen festlegen, wer mit welchem Endgerät und in welchem Umfang auf welche Daten zugreifen darf.

Mit dieser Autorisierung erhält jeder Mitarbeiter Nutzungsberechtigungen gemäß seiner Rolle im Unternehmen. Durch die Einteilung in verschiedene Gruppen ist es möglich, die Vergabe der Governance-Richtlinien zu vereinfachen und die jeweiligen Sicherheitsstufen sowie Nutzungsrechte gebündelt zu vergeben. Network-Access-Control-Systeme (NAC) erlauben zudem eine objektbasierte Kontrolle, indem sie nichtautorisierte Geräte als solche sichtbar machen und deren Zugriff auf das Netzwerk ausschließen. Hierzu müssen Unternehmen zunächst alle mobilen Endgeräte mit Zugriffsrecht erfassen und zertifizieren. Dabei sollten sie darauf achten, dass die Konfiguration anerkannte Sicherheitsstandards erfüllt.

3.2.3 Härtung des Endgeräts bietet hohe Sicherheit

Die Verbindung über sichere VPNs (Virtuale Private Networks) sowie eine verschlüsselte Datenübertragung schützen vor verbotenen Zugriffen, Manipulation und Spionage, unabhängig von welchem Ort aus sich ein Smartphone mit dem Unternehmensnetzwerk verbindet. Zusätzlich sollten Informationen mobil in verschlüsselter Form gespeichert und nur über ein Passwort zugänglich sein. Eine mögliche Technologie hierfür ist ein Kryptoprozessor. Dieser wird mittels einer MicroSD-Karte integriert und erzeugt private Schlüssel. Die Kryptokarte funktioniert wie eine Art Tresor: Selbst wenn ein unautorisierter Zugriff auf das Endgerät gelingen sollte, bleiben die Schlüssel und die damit gesicherten Daten geschützt.

Eine weitere Sicherheitsebene lässt sich mit Mikrokernen einbauen. Diese werden so nah wie möglich am Bootloader eingebettet, was die Sicherheit des Systems erhöht, da das Endgerät an sich gehärtet wird. Außerdem sind sie in der Lage, verschiedene Bereiche sicher voneinander zu trennen. Sensible Informationen können deshalb in einem zweiten, völlig autarken Betriebssystem abgelegt werden – verschlüsselt und passwortgeschützt sowie isoliert von den restlichen Anwendungen. Basierend auf diesem Prinzip lassen sich private und geschäftliche Applikationen auf einem Endgerät verwenden. So können Funktionen wie die Kamera, WLAN und der Zugang zu sozialen Netzwerken genutzt werden, ohne geschäftskritische Daten und Vorgänge zu gefährden. Zusätzlich bietet VoIP-Sprachverschlüsselung die Möglichkeit, Telefonate abhörsicher zu machen.

3.2.4 „Kill Pill" ermöglicht Fernlöschung

Der Verlust oder Diebstahl des mobilen Endgeräts birgt einer Erhebung der IDG Business Research Services (TrendMonitor „Mobile Security", Februar 2013) zufolge das größte Gefahrenpotenzial. 45 Prozent der befragten Unternehmen sehen darin eine starke oder existenzielle Bedrohung. Ein zentraler Fernzugriff erlaubt es jedoch, das Endgerät zu sperren und sämtliche Informationen zu löschen, und gehört laut IDC-Studie mit 30 Prozent zu den meist genutzten Funktionen innerhalb des Mobile-Device-Managements. Der Sicherheitsmechanismus, auch „Kill Pill" genannt, versetzt das Gerät in den Ursprungszustand zurück. In einem weiteren Schritt zum Schutz der Unternehmensdaten ersetzt eine zentrale die lokale Speicherlösung. Ein Beispiel dafür ist ein ECM-Portal (Enterprise Content Management): Die Mitarbeiter rufen benötigte Informationen über einen Link von einem virtuellen Server ab. Das Endgerät dient in diesem Fall lediglich der Anzeige von Inhalten. Um auf das Intranet zugreifen zu können, muss der Nutzer online sein. Es gibt jedoch auch Informationen, etwa Kontaktdaten im Adressbuch, die jederzeit verfügbar sein sollten, auch wenn der Anwender nicht mit dem Unternehmensnetzwerk verbunden ist. Somit kann eine lokale Speicherung nie vollständig vermieden werden. Remote-Access und Verschlüsselung werden durch eine zentrale Lösung zur Datenspeicherung also nicht ersetzt, sondern lediglich ergänzt.

3.2.5 Die sieben wichtigsten Security-Mechanismen

1. Datenschutztechnologien stellen die Basis für ein lückenloses Sicherheitskonzept dar und schützen vor Schadsoftware.
2. Identity-Access-Management (IAM) bietet Schutz vor nicht autorisierten Zugriffen.
3. VPNs (Virtual Private Networks) verhelfen zu einer gesicherten Datenübertragung.
4. Datenverschlüsselung macht Informationen für Unbefugte unbrauchbar.

5. VoIP-Sprachverschlüsselung ermöglicht abhörsichere Telefonate.
6. Remote-Access hilft bei Diebstahl/Verlust des Endgeräts.
7. Zentrale Speicherlösung sichert Daten in einem geschützten Raum.

3.2.6 Sichere Smartphone-Architektur – ein Beispiel

Ein Beispiel für sichere Smartphone-Architektur ist SiMKO 3 von T-Systems, die folgende Features bietet:

- Herstellung unter **TrustCenter-Bedingungen**
- Vergabe einer eindeutigen **„digitalen Identität“** zur Autorisierung und Vergabe von Sicherheitsschlüsseln
- Sichere Verbindung über **VPNs**
- Datenverschlüsselung durch **Kryptokarte**
- Duale Softwarearchitektur durch Mikrokerne: **offener und geschäftlicher Modus** durch zwei eigenständige, voneinander getrennte Betriebssysteme und Datenbereiche
- **Verschlüsselung** als Datenschutz bei Diebstahl oder Verlust des Endgeräts
- Ende-zu-Ende-Verschlüsselung nach **S/MIME-Standard** für Signatur und Versand von E-Mails
- **VoIP-Sprachverschlüsselung** mit verschiedenen Verschlüsselungs-Modi für abhörsichere Telefonate

3.2.7 Fazit

Ein umfassendes Sicherheitskonzept, das sowohl Nutzer und Endgeräte als auch die IT-Infrastruktur beinhaltet, stellt den Kern einer professionellen Mobile-Device-Strategie dar. Dabei ist entscheidend, dass Technologien und Maßnahmen auf den mobilen Zugriff zugeschnitten sind. Nur so können Unternehmen Risiken und Angriffspunkte minimieren und einen Echtzeitzugriff auf aktuellste Daten und Prozesse zuverlässig umsetzen. Das schafft die Nähe zwischen Unternehmen und Mitarbeitern im mobilen Einsatz, die nötig ist, um schnell auf Kundenanforderungen zu reagieren. Mobile Enterprise wird so zum Wettbewerbsvorteil.

Dr. Ferri Abolhassan

Der promovierte Informatiker **Ferri Abolhassan** ist Mitglied der Geschäftsführung von T-Systems und leitet den gesamten Bereich Delivery bei T-Systems. Darüber hinaus ist er Autor und Herausgeber zahlreicher Publikationen und Bücher.