Anbindung von mobilen Geräten an Firmennetzwerke

Um mobilen Geräten von zu Hause oder im Außendienst sicheren Zugriff auf Firmennetzwerke und die dort gespeicherten Informationen zu gewähren, kommen in der Regel unterschiedliche Techniken zum Einsatz:

1. Sogenannte virtuelle private Netzwerke („VPN“) ermöglich mit einer auf dem mobilen Gerät installierten Software („VPN-Client“) das Herstellen einer verschlüsselten Verbindung zum VPN-Server des eigenen Unternehmens. Dieser prüft anhand mehrerer Kriterien, ob der Anmeldeversuch von einem bekannten Gerät und einem autorisierten Benutzer stammt und gewährt dann Zugriff auf alle Netzwerkressourcen (Dateien, Verzeichnisse, Drucker), für die der jeweilige Benutzer Berechtigungen besitzt. Aus Sicht des Anwenders verhält sich sein mobiles Gerät wie ein am Standort des Unternehmens ans Netzwerk angeschlossener Büro Computer. Je nach Einstellung laufen nach Aufbau der VPN-Verbindung („VPN-Tunnel“) die genutzten Internetdienste (Webbrowser, E-Mail, Chat-Programme, Videokonferenz) über das Firmennetzwerk.

2. Häufig wird bei bestimmten mobilen Anwendungen das Verschlüsselungsprotokoll Transport Layer Security (TLS, meint Transportschichtsicherheit, früher bekannt unter Secure Sockets Layer, SSL) eingesetzt. Die TLS-Verschlüsselung wird heute bei gesicherten Webseiten mit HTTPS, z.B. beim Online Banking oder beim Einkaufen per Internet eingesetzt. Auch bei der Nutzung von beruflichen E-Mail Konten (MS Outlook, Lotus Notes etc.) kommt häufig TLS zum Einsatz. Hierbei muss der Benutzer auf dem mobilen Gerät nicht selbst eine gesicherte Verbindung herstellen, vielmehr sorgen die Programme und Webdienste für die Verschlüsselung der Verbindung. In Webbrowsern kann man dies häufig am Schlosssymbol neben der Adresse der Webseite erkennen.

3. Weit verbreitet ist auch die Nutzung von Terminal Servern. Dabei installiert die Unternehmens-IT das Betriebssystem und die zu nutzenden Anwendungen auf einem einzigen Server. Als Benutzer greift man dann über eine Remote Software auf diesen Server zu und steuert mit dem mobilen Endgerät die Anwendung, die nur auf dem Server ausgeführt wird, fern. Die Übertragung von Daten und Bildschirmansichten erfolgt ebenfalls verschlüsselt.