Virtual Solution

Die passende Container-Lösung wählen

[21.12.2017] Was müssen Unternehmen und Behörden bei der Auswahl einer verschlüsselten Container-Lösung für ihre mobilen Geräte beachten? Das Unternehmen Virtual Solution hilft mit zehn Tipps weiter.

Die Nutzung mobiler Endgeräte wie Smartphones und Tablets ist in Behörden und Unternehmen mittlerweile gang und gäbe. Jedoch sind Daten und Anwendungen auf diesen Systemen zahlreichen Bedrohungen ausgesetzt – erst recht, wenn private Geräte für berufliche Aufgaben verwendet werden. Mit einem verschlüsselten Container werden Unternehmensinformationen geschützt und strikt vom privaten Bereich getrennt. Somit können Anwender mobil und zugleich sicher arbeiten.
Das Unternehmen Virtual Solution informiert, an welchen Kriterien sich Anwender bei der Auswahl einer Container-Lösung orientieren sollten. „Container-Lösungen werden mehr und mehr zum Standard für den professionellen Einsatz von Mobilgeräten“, sagt Günter Junk, CEO der Firma Virtual Solution in München. „Aber nicht jede Lösung passt für jedes Einsatzszenario. Hier müssen Unternehmen und Behörden ihre Anforderungen genau erfassen. Dabei sollten sie nicht nur vom Status quo ausgehen, sondern auch künftige Entwicklungsmöglichkeiten im Auge behalten.“ Mit ihrer verschlüsselten Lösung SecurePIM wolle die Firma daher ein möglichst breites Spektrum von Anwendungsbereichen abdecken. Folgende zehn Punkte sollten bei der Auswahl einer Container-Lösung laut der Firma Virtual Solution beachtet werden:

1. Der Container darf nur über PIN und Passwort zugänglich sein, damit kein Unbefugter Zugang zu den Unternehmensdaten bekommt.

2. Die Lösung sollte keine eigenen Verschlüsselungs-Algorithmen verwenden, sondern bewährte Krypto-Standards wie S/MIME, AES-256, SHA-256 oder Elliptic Curve; diese seien vielfach getestet und garantierten einen hohen Schutz.

3. Im Behördeneinsatz sollte die Lösung über eine Zulassung des Bundesamts für Sicherheit in der Informationstechnik (BSI) verfügen. Diese stellt sicher, dass die besonderen Sicherheitsansprüche der öffentlichen Verwaltung berücksichtigt werden.

4. Die Verschlüsselung der Daten muss sowohl auf dem Endgerät als auch während der Kommunikation erfolgen, also die Ende-zu-Ende-Verschlüsselung unterstützen.

5. Es muss die Möglichkeit bestehen, Sicherheitsvorgaben durchzusetzen wie die Unterbindung von Copy-and-paste vom geschützten in den ungeschützten Bereich. So kann der Nutzer vor Fehlern beim Datenschutz bewahrt werden.

6. Der Container sollte über eine sichere Verbindung zum Unternehmensnetzwerk verfügen, möglichst ohne VPN, die durch Verschlüsselung und Zertifikate geschützt wird. Damit wird verhindert, dass das mobile Endgerät zum Einfallstor von Schad-Software wird.

7. Eine Container-Lösung sollte optional auch Smartcards unterstützen und so bei hohem Schutzbedarf sicherheitsrelevante Prozesse wie die Entschlüsselung von Daten auf die Smartcard verlagern können.

8. Mobile Anwender fordern heute eine umfassende Funktionalität, vergleichbar der im stationären Büro. Neben den gewohnten Outlook-Funktionalitäten wie E-Mail, Kontakte und Kalender muss auch mobil der

sichere Zugriff auf die Daten und Programme des Unternehmens gewährleistet sein. Nur so können zum Beispiel die Anwender auch mobil Dokumente sicher in einem Container laden und dort beliebig bearbeiten. Die Lösung sollte einfach zu benutzen sein und sich möglichst eng an die Usability von Native Apps anpassen. Dabei darf die Sicherheit den Mitarbeiter nicht einschränken. Denn jede Einschränkung des Anwenders führt dazu, dass dieser sich andere Wege, nämlich unsichere, sucht, um auch mobil effizient zu arbeiten.

9. Die Lösung sollte einfach zu installieren und zu verwalten sein.

10. Neben der Sicherheit zeichnet sich eine gute Container-Lösung dadurch aus, dass diese in jede beliebige IT-Infrastruktur integriert werden kann. Ein guter Container stellt keine speziellen Ansprüche und ist lediglich eine gemanagte App, die auf die mobilen Endgeräte, egal ob Smartphone oder Tablet, egal ob Android oder iOS, aufgespielt werden kann.

(sav)

Stichwörter: IT-Sicherheit, Mobile Device Management, Virtual Solution AG