Virtual Solution

Mobile Software sicher ausrollen

[23.05.2022] Immer mehr Behörden, auch jene mit strengen IT-Sicherheitsregeln, setzen auf mobile Arbeitsgeräte. Beim Roll-out und Update dort installierter Software kann einiges schief gehen. Virtual Solution, Spezialist für sichere Mobil-Apps, klärt über die gefährlichsten Stolpersteine auf.

Mobiles Arbeiten ist für Unternehmen wie auch für Behörden zur Selbstverständlichkeit geworden. Dies gilt auch für die vielen Behörden und Organisationen mit Sicherheitsaufgaben (BOS). Sie alle sind darauf angewiesen, Mitarbeiter zur Erfüllung ihrer Aufgaben mit modernen iOS- und Android-Geräten auszustatten. Bei der mobilen Arbeit benötigt werden vor allem Kommunikations- und Kollaborations-Tools wie etwa E-Mail, Messenger und Kalender sowie solche für die Dokumentenbearbeitung. Nun hat das auf sichere mobile Anwendungen spezialisierte Software-Unternehmen Virtual Solutions, das zur Materna-Gruppe gehört (wir berichteten), einen Ratgeber-Artikel zum pannenfreien Roll-out solcher Kommunikationslösungen auf mobilen Endgeräten veröffentlicht.

Updates müssen zügig ausgerollt werden

Für das Management mobiler Endgeräte werden häufig MDM-Systeme (Mobile Device Management) eingesetzt. Sie sollen sicherstellen, dass die Kommunikationslösungen auf Smartphones und Tablets immer auf dem neuesten Stand sind. In der Praxis tauchen jedoch nach Einschätzung von Virtual Solutions immer wieder typische Probleme auf, die eine sichere, plattformübergreifende und nutzerfreundliche Einführung und Aktualisierung mobiler Kommunikationslösungen verhindern.
Virtual Solution hat vier typische Fallstricke identifiziert. Problematisch ist etwa das Timing. Sukzessive Roll-outs und das zeitversetzte Updaten von mobilen Endgeräten gilt es zu vermeiden. Durch den Einsatz von unterschiedlichen Versionen entstehen nicht nur relevante Sicherheitsrisiken, ein lang andauernder Roll-out kann auch die Zusammenarbeit erschweren. So könne es in diesem Fall etwa passieren, dass einzelne Mitarbeiter noch nicht auf Software, etwa den verwendeten Messenger, zugreifen können und bei der internen Kommunikation außen vor bleiben. Sie müssen dann entweder auf E-Mails oder das Telefon ausweichen, womit die Gefahr von fehlerhafter Kommunikation oder vielen zeitintensiven Rückfragen steigt.
In Zeiten von Homeoffice und mobiler Arbeit sollte der Roll-out außerdem nicht mehr an einen Ort gebunden sein. Schon bei mittelständischen Unternehmen oder mittelgroßen Behörden könne es zu Problemen kommen, wenn auch nur ein Teil der Mitarbeiter den IT-Administrator zwecks eines Updates persönlich aufsuche, so Virtual Solution. Mobile Kommunikationslösungen sollten aus diesem Grund zeitgleich flächendeckend ausgerollt werden und in gleicher Weise auch Updates erhalten.

Probleme können sich potenzieren

Bundesbehörden und BOS, aber auch KRITIS-Unternehmen besitzen strenge Vorgaben für die IT-Nutzung. Die teilweise sehr umfangreichen und komplizierten Regularien müssen auch beim Roll-out abgebildet werden. Dazu kommen Anforderungen wie beispielsweise Multi-Mandantenfähigkeit und schnelle Skalierbarkeit.
Die Vielzahl an möglichen Problemen kann nach Erfahrung von Virtual Solution bei einem Roll-out schnell zu einer großen Herausforderung werden. Für die technische Umsetzung, so das Unternehmen, haben

sich kosteneffiziente und schnell einsetzbare Containerlösungen bewährt (wir berichteten). Diese trennen geschäftliche Daten und Applikationen vom Rest des mobilen Endgeräts. Auf diese Weise bleiben private sowie berufliche Daten der Mitarbeiter separiert und geschützt. So sei ein sicherer, ultramobiler Arbeitsplatz mit der Container-Technologie von Virtual Solution nicht nur für Organisationen und Unternehmen, sondern auch für Bundesbehörden möglich, welche die VS-NfD-Vorgaben erfüllen müssen, erklärt Hermann Granzer, CTO bei Virtual Solution. Dabei trage ein hochautomatisierter Roll-out dazu bei, Anwendungen auch bei großen Nutzerzahlen laufend und synchron immer auf dem neuesten Funktions- und Sicherheitsstand zu halten.

(sib)

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