Smarte Lecks

Smartphones und Tablet-Computer haben einen Boom ausgelöst, der viele Unternehmen vor ein massives Problem stellt: Was tun mit dem mobilen Sicherheitsrisiko?

Die Flutwelle ist beispiellos. Ausgelöst hat sie Apple-Gründer und iPhone-Erfinder Steve Jobs. Seitdem schwemmen Massen an Smartphones und Tablet-Computern den Markt – und die Unternehmen fast aller Branchen. Doch was dem Mitarbeiter sein Status-Symbol, ist den IT-Sicherheitsexperten meist ein Dorn im Auge. Denn wie sollen Android- oder iOS-Geräte in die IT-Infrastruktur sicher integriert werden?

Christian Rückert ist Experte auf diesem Gebiet. Der Business Development Manager von Netlution aus Mannheim fordert, dass Unternehmen ein konsequentes Mobile Device Management (MDM) durchsetzen, um die Sicherheit der Unternehmensdaten zu garantieren. Denn die smarten Alleskönner werden schnell zu smarten Lecks. Wie ein solches MDM aussehen soll, erklärt er der Karlsruher IT-Sicherheitsinitiative.

Das Problem: „Die Vielzahl von Betriebssystemen, ständig neue Applikationen sowie neue Geräte sind eine echte Herausforderung." Auch die Zahl der Anbieter von MDM-Software ist recht unübersichtlich, der Markt stark in Bewegung. Wichtig: Unternehmen müssen sich im Vorfeld über die Richtlinien klar werden, die sie ansetzen wollen, sagt Rückert.

Die grundsätzliche Frage lautet, so der IT-Experte: Werden etwa sensible Unternehmensdaten wirklich auf dem mobilen Endgerät benötigt? Rückert rät zur Zurückhaltung, schränkt aber ein: „Es ist ein schmaler Grat: Wie weit schränke ich durch die Sicherheitsmaßnahmen die Usability ein?" Problematisch wird es vor allem, wenn die Mitarbeiter ihr eigenes Gerät ins Unternehmensnetzwerk mitbringen, im Fachjargon: „Bring Your Own Device". Hier rät Rückert zu rechtlichem Beistand bei der Umsetzung des MDM. „Hier müssen Unternehmen klare betriebliche und vertragliche Regelungen definieren. Zudem spielt der Datenschutz eine wichtige Rolle, ebenso wie Haftungsfragen", so Rückert. „Und: Es ist immer die Frage, ob der Nutzen diesen organisatorischen Aufwand rechtfertigt." Denn der ist durchaus immens, sei es durch private oder dienstliche Mobilgeräte: Verschlüsselung, Zertifikatsdienste, Jailbreak-Erkennung, Maßnahmen für eine sichere E-Mail-Verbindung, Anti-Virus-Programme, App-Black- und Whitelisten, Remote Steuerung – all diese Sicherheitsmaßnahmen der jeweiligen Betriebssysteme, Endgeräte, MDM- und weitere Software müssen aufeinander abgestimmt werden. Die Implementierung eines MDM wird so schnell zu einer zeitraubenden Angelegenheit.

Andersherum können auch Unternehmensgeräte, die privat genutzt werden, zu Sicherheitslecks mutieren, etwa wenn sie sensible Daten enthalten. Rückert macht klar, dass sich die Flutwelle zwar nicht stoppen lässt. In ein Unternehmen sollte man sie aber nur kontrolliert schwappen lassen.

Robert Schwarz

www.netlution.de

KA-IT-Si
Karlsruher IT-Sicherheitsinitiative

Veranstaltung

Gemeinsam mit der IHK Karlsruhe und dem Cyber-Forum präsentiert die KA-IT-Si zum vierten Mal den **Tag der IT-Sicherheit**. Thema: aktuelle IT-Sicherheitsbedrohungen für Unternehmen und wie sich diese dagegen schützen können.

Wo Saal Baden, IHK Karlsruhe Haus der Wirtschaft,
Wann 12. Juli, 14 Uhr
Mehr Informationen und die Vortragsunterlagen der vergangenen Veranstaltungen unter www.ka-it-si.de.

Christian Rückert, Business Development Manager bei Netlution

Foto: Jigal Fichtner