Mobile Security

Schicke Apps und neue Smartphones überholen IT-Sicherheit

Smartphones und Tablets sind zu ständigen Begleitern geworden und erleichtern uns den Alltag in vielen Bereichen. Die stetig wachsende Verwendung mobiler Endgeräte und Apps im Unternehmensumfeld ist aber auch eine der größten Bedrohungen für sensible Firmen- und Kundendaten und für die Privatsphäre von Benutzern. Häufig wird sie von Managern und IT-Entscheidern noch unterschätzt oder schlichtweg ignoriert.

Definition

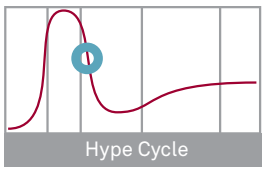
Durch den zunehmenden Einsatz von Smartphones und Tablets im geschäftlichen Umfeld wird die klassische Sicherheitsarchitektur vieler Unternehmen mit einem durch Firewalls abgeschotteten Netzwerk unterwandert. Daten werden vermehrt auch außerhalb dieser sicheren Zone auf mobilen und im Fall von „Bring Your Own Device“ (BYOD) auch auf privaten Endgeräten abgespeichert und verarbeitet.

Umso wichtiger ist es, dass die mobilen Geräte und darauf gespeicherte, sensible Daten angemessen abgesichert werden. Insbesondere sind Smartphones und Tablets durch ihre Mobilität zusätzlichen Risiken ausgesetzt, wie der Verbindung in öffentliche und unsichere Netze, dem leichten Verlust oder Diebstahl und der Möglichkeit zur Ortung und Überwachung von Benutzern.

Mobile Security umfasst aber nicht nur die Technologien der Geräte, Plattformen und Apps, sondern auch organisatorische Aspekte, Administrationsprozesse und Compliance-Themen. Zunächst ist es wichtig, das Thema Mobile im unternehmensweiten Sicherheitskonzept zu verankern und dabei Compliance-Vorgaben wie Datenschutz mit zu berücksichtigen. Dabei ist die Unterstützung des Managements ein kritischer Erfolgsfaktor. Über Richtlinien, Policies und Awareness-Maßnahmen werden die identifizierten Anforderungen an Administratoren, Entwickler und Anwender kommuniziert und nach Möglichkeit auch technisch erzwungen. Denn erfahrungsgemäß halten sich nicht alle Benutzer an Vorgaben auf dem Papier.

Administratoren und App-Entwickler mit Sicherheits-Know-how sind Voraussetzung für die technische Umsetzung von Mobile Security. Bei der App-Entwicklung gilt es, ähnliche Sicherheits-Maßnahmen wie in der klassischen Softwareentwicklung zu berücksichtigen, wie Security by Design, Datensparsamkeit und Verschlüsselung. Letztlich sollten die Maßnahmen durch unabhängige Sicherheitstests überprüft werden. Eine sog. App-Validierung kann sicherstellen, dass eine App keine ungewünschten „Zusatzfunktionen“ hat, wie das Auslesen und Versenden von Adressbüchern oder das unbefugte Erstellen von Benutzerprofilen zu Marketing-Zwecken. Aktuelle Studien zeigen sogar, dass ein Großteil der Smartphone-Anwender allein durch ihr Bewegungsprofil identifiziert werden können.

Reifegrad



Mobile Security ist kein klassisches Trendthema, sondern wie

Sicherheit im Allgemeinen, eine Notwendigkeit, wenn Vertrauen versagt. Mobile Security folgt mit gewissem Abstand dem Technologie-Trend Mobile Computing und minimiert damit verbundene Risiken. Sicherheit wird jedoch erfahrungsgemäß selten hoch priorisiert, bevor ausreichend hoher Schaden und damit Druck entstanden ist.

Marktübersicht

Mobile Security ist ein sehr vielschichtiges Thema und kann daher nicht auf einige wenige Marktteilnehmer beschränkt werden. Die aktuell am weitesten verbreiteten mobilen Plattformen sind Android und iOS, wobei Windows Phone aufholt und Blackberry trotz vergleichsweise guter Sicherheit an Boden verliert. Mobile-Device-Management Hersteller bieten Lösungen zur zentralen Verwaltung und sicheren Konfiguration von Smartphones und Tablets an. Dennoch können diese Technologien ein Sicherheitskonzept und Richtlinien zum Umgang mit mobilen Endgeräten und zur sicheren App-Entwicklung nicht ersetzen.

Alternativen

Bei zunehmenden Mobilitätsanforderungen von Unternehmen und Mitarbeitern ist der Verzicht auf Smartphones und Tablets kaum mehr vorstellbar. Daher gibt es zur angemessenen Umsetzung von Mobile Security nur wenige Alternativen. Allenfalls die Behandlung von identifizierten Risiken kann je nach Situation unterschiedlich erfolgen: Hier kann in Einzelfällen auch eine Übertragung von Risiken (Versicherung, Verträge) oder eine Restrisikoakzeptanz sinnvoll sein. Auch eine Risikovermeidung durch Verbot von potentiell unsicheren mobilen Geräten, Plattformen und Apps im Firmennetzwerk durch Blacklisting oder Whitelisting ist möglicher Bestandteil einer umfassenden Lösung.

Referenzszenario

Mobile Security ist ein relativ junges und dynamisches Thema. Trotzdem gibt es dafür Best Practices und Vorgehensmodelle. So haben zum Beispiel die anerkannten Vereinigungen OWASP (Open Web Application Security Project) und ENISA (European Network and Information Security Agency) Richtlinien und Vorgaben zu unterschiedlichen Themen der Mobile Security entwickelt und auch die msg hat einen Leitfaden zur sicheren App-Entwicklung veröffentlicht. Essentiell beim Thema Mobile Security ist vor allem die ganzheitliche Betrachtung. Denn es hilft zum Beispiel wenig, nur die Geräte gut abzusichern, aber den User dennoch alle – auch potentiell unsichere – Apps installieren zu lassen.

Business Impact

Der rasante Anstieg von Bedrohungen für mobile Endgeräte (allein 2012 126% mehr Malware) zeigt, dass ein Fehlen von Mobile Security längst ein Business-Risiko ist. Trotzdem wird der Impact von vielen Firmen noch unterschätzt – auch weil es wie bei fast allen Security-Themen zunächst keinen positiven ROI gibt und so Investitionen gescheut werden. Kommt es dann aber zu einem Vorfall, kann der Schaden durch Offenlegung von Geschäftsgeheimnissen, Know-how-Abfluss zur Konkurrenz, Rufschädigung oder Gesetzesverstöße beträchtlich sein.

Pro	Contra
Reduktion des Risikos von Sicherheitsvorfällen	Aufwand und Kosten, ohne ersichtlichen ROI
Kostenersparnis und Effizienzsteigerung durch sicheres, mobiles Arbeiten – BYOD wird möglich	Fehlendes Wissen und Risikobewusstsein bei Managern, IT-Leitern und Entwicklern
Compliance zu Gesetzen und Regulierungen	Consumerization – mobile Geräte sind oft nicht für den Einsatz in Firmen konzipiert

msg systems ag
Robert-Bürkle-Straße 1 | 85737 Ismaning/München
Telefon: +49 89 96101-0 | Fax: +49 89 96101-1113
www.msg-systems.com | info@msg-systems.com

Stand: September 2013
http://www.msg-systems.com/techrefresh
XT-310-1309-1