Mobile Security im Wandel

Durch die Konsolidierung der Branche sind viele Technologien verschmolzen. Das zwingt die Anwender, Mobilität und Sicherheit als miteinander verbundene Teilaspekte zu betrachten anstatt als separate Silos des IT-Budgets und IT-Managements.

Rund um das Thema Enterprise Mobility haben sich einige Binsenweisheiten etabliert, die man als gegeben annehmen kann: BYOD und externe Cloud-Dienste sind Realität. Business-Apps werden unterhalb des Radars der IT-Sicherheit entwickelt. Und der Zustrom neuer Gerätetypen und Formfaktoren ist ungebremst. Allerdings befinden wir uns noch immer in einer Phase, in der die mobilen Sicherheitstechnologien und Architekturentscheidungen die Gewährleistung der Mobile Security kurz- und langfristig eklatant beeinflussen können. Das bedeutet konkret:

- Unternehmen müssen die Einführung mobiler Geräte und Technologien weiter vorantreiben. Der Druck dazu kommt sowohl von der Führungsebene als auch von den Fachbereichen und einzelnen Mitarbeitern. Die Sicherheit ist damit bei der Einführung mobiler Apps oft zweitrangig.
- Unternehmen müssen mobile Produktivität, Effizienz und Kostensenkungen in Einklang bringen mit der unternehmensweiten Sicherheitsstrategie und den Prioritäten der Informationssicherheit. Mobile Geräte greifen zunehmend auf sensible Workloads und Daten zu. Damit steigt das Risiko von Datenlecks, Produktivitätsausfällen und verlorenen Umsätzen. Auch der gute Ruf des Unternehmens wird beschädigt, wenn die mobile Sicherheitsarchitektur zu viele Schwachstellen aufweist.

Der Fokus bei Mobile Security verschiebt sich weiter zu Apps und Daten

Die IT-Abteilung im Unternehmen wird sich immer mit der Sicherheit physischer Mobilgeräte befassen: Konfiguration, Speicher-Richtlinien, Zugangsrechte. Allerdings bestehen sowohl der größte Nutzen als auch die größten Risiken auf Seiten der Apps und Daten, die sich auf einem Gerät befinden, und weniger bei der Hardware. Technologien zum Schutz verlorener oder gestohlener Geräte wie Löschung aus der Ferne und das so genannte „Bricking“ sind heute allgemein üblich. Auch das Sperren oder Sichern einzelner Peripheriegeräte oder Aktivitäten sind weit verbreitet, um Missbrauch zu verhindern. Dazu zählen etwa das Deaktivieren der Kamera, das Setzen von Passwörtern oder die Verhinderung von Jailbreaks.

Durch BYOD verschiebt sich der Security-Fokus vom Gerät hin zu den Apps und den Inhalten. Denn viele Mitarbeiter, die ihre privaten Geräte dienstlich nutzen, wollen die Kontrolle darüber nicht an den Arbeitgeber abgeben. Zudem verschieben die Unternehmen immer mehr individuelle Apps und Daten in das erweiterte Unternehmen mit freien Mitarbeitern, Partnern, Drittanbietern und dergleichen. In solchen Szenarien sind Sicherheitsmechanismen auf App- und Datenebene die einzige Option.

Mobile Application Management (MAM) und Mobile Content Management (MCM) sind zwei der drei Säulen eines vollständigen EMM-Stacks. MDM ist zwar der Einstieg in EMM, doch die zunehmende Bedeutung von App- und Datensicherheit hat den Fokus der EMM-Plattformen von den Geräten hin zu MAM und MCM verschoben. Geräte sind Fenster oder Zugriffsportale für Unternehmens-Apps. Sie repräsentieren die zentrale Schnittstelle zwischen den Mitarbeitern und den Enterprise- oder Cloud-Systemen. Lösungen, die mehr Flexibilität und Kontrolle über die Apps auf dem Smartphone bieten, beginnen sich durchzusetzen.

Der Einsatz von Containern oder App-Wrapping, womit die Interaktivität zwischen Gerät und App eingeschränkt wird, ist weit verbreitet. Viele dieser Lösungen sind allerdings an umfassende EMM/MDM-Plattformen gebunden. Häufig entstehen bei Konfiguration und Absicherung des EMM-basierenden App-Deployments interne Entwicklungsaufwände und Kosten. Hier bilden sich gerade stärker spezialisierte Technologien im App-Management wie dynamisches App-Wrapping heraus, mit denen Unternehmen die Sicherheit auf App-Ebene ohne aufwändige Entwicklungsarbeit oder Code-Anpassungen durchsetzen können.

Unternehmen wie zum Beispiel Versicherungen, deren Geschäftsmodell die Zusammenarbeit mit unabhängigen Vertretern vorsieht, oder Franchise-Geber in der Gastronomie führen in diesen erweiterten Unternehmensbereichen Apps ein, die einen spezifischen Zugriff auf Daten oder Services benötigen. Das können zum Beispiel Aufgaben wie das Ausfüllen eines Unfallberichts oder Nachbestellungen sein. Unternehmen, die solche Apps verteilen, benötigen unabhängig vom Endgerät ein hohes Maß an Kontrolle über das Deployment und den Zugriff auf diese Apps. Zugriffssteuerung und die Möglichkeit, Apps zurückzuziehen oder zu löschen, unterstützen die Unternehmens-IT dabei, Apps in einem Umfeld zu sperren, in dem Sicherheit und Kontrolle vom eigentlichen Gerät losgelöst sind.

Letztlich nehmen Mobile Content Security und Management in einem Post-MDM-Framework eine besonders wichtige Position ein. Technologien, die eine granulare und kontextsensitive Zugriffs- und Rechteverwaltung für bestimmte Dokumente wie Tabellen, Präsentationen, Dokumente oder Bilder ermöglichen, werden zu einer Grundanforderung. Viele Unternehmen verfügen heute beim Schutz des Enterprise Contents über einzelne Silos wie Digital Rights Management, Data Loss Management oder Verschlüsselung, die – wenn überhaupt – nur lose

miteinander verbunden sind. Doch der Bereich, den EMM abdeckt, wird größer. Die IT-Teams im Unternehmen sollten Punkte suchen, an denen eine tiefere Integration bestehender ERM- und Content-Management-Lösungen in die eigene Architektur möglich ist. Und sie sollten die inzwischen verfügbaren Angebote der EMM-Provider im Bereich des Mobile Content Managements nutzen.

Cloud-Plattformen werden der Schlüssel zu Mobile Security

Um die Aktivitäten der mobilen Anwender zu schützen und zu steuern, werden Cloud-basierende Sicherheitslösungen immer wichtiger. Hier wird sich die Entwicklung auf zwei Arten vollziehen: Erstens werden bereits vor Ort betriebene EMM-Lösungen auf SaaS-Plattformen als primäres Deployment-Modell migrieren. IDC erwartet, dass innerhalb der kommenden fünf Jahre bis zu zwei Drittel aller EMM-Implementierungen als SaaS betrieben werden oder als hybride Cloud-Dienste, bei denen Cloud- und On-Premise-Lösungen kombiniert sind.

Zweitens werden Sicherheitstechnologien wie Mobile Threat Detection, Schwachstellenanalyse oder Identitäts- und Content-Sicherheit für mobile Geräte primär aus der Cloud bezogen werden. Insgesamt erwartet IDC, dass Cloud-basierende Sicherheitslösungen innerhalb der kommenden fünf Jahre weltweit um über zehn Prozent wachsen werden. Die für den mobilen Einsatz wichtigen Technologien aus der Cloud wie Identitätsschutz und Schwachstellen-Management werden um 14, respektive 17 Prozent zulegen. EMM-Plattformen aus der Cloud werden beim Schutz der mobilen Endgeräte zunehmend kritisch. Damit werden Unternehmen vermehrt auch Cloud-basierende Mobile-Security-Lösungen einführen, um ihren Schutz zu verbessern. MDM und EMM sind beim aktiven Schutz der Endpoints in weiten Teilen asymmetrisch: Richtlinien werden im Push-Verfahren an die Geräte und App-Container ausgeliefert, die Anwender müssen mit Einschränkungen zurechtkommen. Werden die Richtlinien verletzt, können die Administratoren Apps zurückziehen oder die Konnektivität des Geräts unterbinden.

Diese Aktionen müssen jedoch angestoßen werden, die Automatisierung ist nicht weit gediehen. Es fehlt am Monitoring des Inline-Traffic und an der Durchsetzung der Policies – insbesondere, wenn die Geräte aus einem 4G-Netz ins WLAN wechseln und auf Cloud-Dienste unterschiedlicher Herkunft zugreifen. Cloud-Sicherheitslösungen können den Inline-Traffic zwischen mobilen Geräten und den Cloud-Diensten und anderen Quellen untersuchen. In dem Rahmen, in dem mehr Anwendungen auf SaaS- und Cloud-Umgebungen verschoben werden, müssen die

Unternehmen auch diese Datenströme unter die Lupe nehmen. Es ist durchaus üblich, dass Unternehmen ihre mobilen Anwender dazu zwingen, Public Clouds über die eigene Netzwerk-Infrastruktur zu nutzen. Der mobile Cloud-Traffic wird mittels VPN zurück ins Unternehmen geholt, um dort durch die Security Gateways geleitet zu werden. Das macht die Apps langsam und ist für die Anwender frustrierend.

Indem der SaaS-Datenverkehr durch Cloud-basierende Sicherheits-Services mit Identity Access und fortlaufendem Monitoring der Datenströme überwacht wird, kann das Problem langsamer Apps abgeschwächt werden. Dieser Aspekt wird kritisch, da immer mehr Unternehmen von einem gerätezentrischen Ansatz bei Mobile Security zu einem App-/Data-zentrischen Ansatz wechseln und zugleich dem erweiterten Unternehmen mehr mobile Möglichkeiten einräumen.

Rapid Mobile App Development – ein Schreckensszenario?

Unternehmen, die rasch mobile Anwendungen innerhalb eines Fachbereichs oder der Belegschaft einführen wollen, nutzen dazu vermehrt Rapid App Development und mobile Backend-as-a-Service (MBaaS)-Plattformen. Die Tools für Rapid App Development ermöglichen es, neue Apps von Grund auf zu entwickeln; häufig mittels einer GUI-basierenden Entwicklungsumgebungen, die kaum Programmierwissen voraussetzt. Vermarktet werden diese Systeme an die Fachbereichsleitungen als eine Möglichkeit, mobile Anwendungen auf den Markt oder in den eigenen Bereich zu bringen mit dem Ziel, die Produktivität und Effizienz zu verbessern.

Analog dazu ist MBaaS eine Cloud-Plattform, die die Legacy-Anwendungen und Datenspeicher hinter der Firewall mit den anwenderorientierten mobilen Apps verbindet. Häufig arbeiten Unternehmen sowohl mit Tools zum Rapid Mobile App Development als auch mit MBaaS-Plattformen, um schnell Schnittstellen zwischen mobilen Front-End-Apps und den Daten und Legacy-Systemen im Back-End zu schaffen. IDC erwartet, dass der weltweite Gesamtmarkt für derartige Entwicklungsplattformen für mobile Apps von 1,9 Milliarden Dollar im Jahr 2015 auf über vier Milliarden bis 2019 wachsen wird.

Entscheidet sich ein Unternehmen bei der Entwicklung von B2B-Apps für ein schnelles „Mobile First", bleibt dabei leider oft als Nebeneffekt die Sicherheit auf der Strecke. Nur 26 Prozent der US-Unternehmen testen laut der Mobile Enterprise Software Survey von IDC aus dem Jahr 2015 die Sicherheit ihrer mobilen Anwendungen im Rahmen des üblichen Entwicklungsprozesses. Im Gegensatz dazu pla-

nen demnach 70 Prozent der Unternehmen, innerhalb der kommenden zwölf bis 18 Monate in die Sicherheit der mobilen Geräte zu investieren. Man könnte sagen, bei dieser Strategie wird das Pferd von hinten aufgezäumt. Oder die mobile Sicherheit von hinten angegangen. Aus der Design-Sicht ist es eine sehr kraftvolle Idee, die Business Units ihre eigenen Apps und Tools bauen zu lassen. Aus Sicht der Security ist es eher ein Albtraum, dass Mitarbeiter ohne Programmierkenntnisse und Erfahrung mit Sicherheitskonzepten – oder Kenntnis gesetzlicher Vorgaben und branchenspezifischer Normen – Apps entwickeln. Mobile Geräte oder Mails und unstrukturierte Daten darauf sind nur in seltenen Fälle der Grund für umfassenden Datenverlust. Das kann sich jedoch ändern, wenn sich hastig gebaute mobile Apps mit den Datenbanken im Unternehmen verbinden. Unternehmen, die Rapid Mobile App Development nutzen, sollten eine Sicherheitslösung in Betracht ziehen, die den Fluss sensibler Informationen überwachen kann. Das betrifft insbesondere strukturierte Daten aus Quellen wie Datenbanken und Back-End-Systemen.

Dazu ist es notwendig, Sicherheits- und Zugangsmechanismen zu entwickeln, die um die mit Rapid Mobile App Development und MBaaS-Plattformen geschaffenen Unternehmens-Apps herum gebaut sind. Unternehmen sollten Mobile App Development Plattformen (MADPs) einsetzen, die gut in die EMM-Lösungen integriert sind und die nach der Entwicklung der App Container und Authentifizierungsdienste anbieten. Einige MADP-Anbieter verfügen auch über Lösungen, mit denen Container und Authentifizierungsfunktionen bereits vor der Entwicklung einer App angelegt werden können. Das kann dabei helfen, die schnell gebauten Apps bereits vor der Verteilung über EMM oder den unternehmenseigenen App-Store zu schützen.

Einige kürzlich angekündigten Brancheninitiativen und Partnerschaften haben zum Ziel, die App-Entwicklung und EMM-Plattformen enger zu verzahnen und so den Integrationsprozess zu unterstützen. Beispiele dafür sind die Partnerschaft zwischen Oracle und VMware AirWatch oder die jüngst angekündigte Integration der Remote Access Security von Pulse Secure für mobile Apps, die mittels SAP Fiori gebaut wurden. Die herstellerübergreifende AppConfig-Community ist ein weiterer Standardisierungsversuch im Bereich App-Sicherheit und -Entwicklung der Unternehmen.

Aus Sicht des Post-Deployments sollten die App-Entwicklungsteams und die Führungskräfte der Lines of Business auch Schwachstellenmanagement sowie Security Information and Event Management (SIEM) -Systeme in die EMM-Plattformen integrieren. Diese sind häufig für mobile Apps das Tor zum Unternehmen. Weitere Tools wie Mobile Application Performance Monitoring und Mobile User Activity Monitoring sind hilfreich, um die sich schnell entwickelnden und dynamischen Initiativen bei der App-Entwicklung abzusichern.

Fazit: Unternehmen brauchen eine „Mobile-Security-First-Strategie“

Die Zusammenarbeit der Hersteller und die Interoperabilität sind in den vergangenen Jahren ein ganzes Stück vorangekommen. Heute gibt es starke Allianzen zwischen den Geräteherstellern, den Anbietern von Enterprise-Mobility-Plattformen und Sicherheits-Providern. Durch die Konsolidierung der Branche sind viele Technologien verschmolzen. Das zwingt die Anwender, Mobilität und Sicherheit als miteinander verbundene Teilaspekte zu betrachten anstatt als separate Silos des IT-Budgets und IT-Managements. Unternehmen mit einer Mobile-First-Strategie sollten diese besser als „Mobile Security First“ auffassen, um besser von den Fortschritten dieser produktivitätsgetriebenen Technologie zu profitieren, die das mobile Universum betritt.

Unternehmen, die den Wildwuchs mobiler Projekte ohne Übersicht, ohne sichtbare Sicherheitstechnologien und ohne partnerschaftliche Deployment-Taktik erlauben, müssen sich auf mehr Zwischenfälle, Streitereien zwischen den Abteilungen und Verzögerungen bei der Einführung mobiler Apps einstellen.

Mark Alexander Schulte

Mark Alexander Schulte verstärkt seit 2011 das IDC-Team in Frankfurt. Der studierte Betriebswirt ist mit der Durchführung von kundenspezifischen Consulting-Projekten sowie der Erstellung von Studien betraut. Als Analyst konzentriert Schulte sich insbesondere auf die Themen Enterprise Mobility, Internet of Things, Industrie 4.0 sowie Social Enterprise Collaboration und steht dabei im engen Austausch mit allen Akteuren des Marktes. Schulte ist Autor zahlreicher Artikel und wird regelmäßig in der einschlägigen Wirtschafts- und Fachpresse zitiert.