Link: https://www.cio.de/a/die-richtige-strategie-fuer-mobile-security,2961991

Mobil? Aber sicher!

Die richtige Strategie für Mobile Security

Datum: 30.06.2014
Autor(en): Sebastian Christe

Hacker haben es bei Smartphones und Tablets besonders leicht, an hochsensible Daten zu gelangen. Mit der richtigen Sicherheitsstrategie sind Unternehmen gut gegen Angriffe geschützt und für das mobile Zeitalter gerüstet

Ob Smartphones, Tablets oder Laptops, ob privat oder geschäftlich erworben: Mobile Geräte sind längst im Unternehmensalltag angekommen. Die Kehrseite der Medaille: Sie sind zum neuen Einfallstor für den Zugriff auf Unternehmensdaten geworden. Technische Punktlösungen, heute weit verbreitet, reichen nicht aus, um dieses zu schließen. Ein holistischer Ansatz ist notwendig - einerseits mit technischen Lösungen für den Schutz von Geräten, Anwendungen und Inhalten, andererseits mit entsprechenden Prozessen und dem richtigen Verhalten von Mitarbeitern.

Sebastian Christe, Security Consultant, HP Enterprise Security Services
Foto: HP Deutschland

195 Millionen Tablets und fast eine Milliarde Smartphones sind nach Angaben von Gartner 2013 weltweit verkauft worden. Gegenüber dem Vorjahr waren dies 68 beziehungsweise 36 % mehr. Für 2014 prognostizieren die Marktforscher ein weiteres Wachstum für mobile Geräte - einschließlich Notebooks und anderen Hardwarekategorien. Wie viele dieser Geräte heute auf Daten im Unternehmen zugreifen, ist in den Organisationen selbst oft unklar. Denn die Grenzen zwischen dem Einsatz im Arbeits- und persönlichen Umfeld lösen sich gerade in der mobilen Welt zunehmend auf. Verstärkt durch Konzepte wie Bring your own Device (BYOD), Choose your own Device (CYOD) oder Corporate Owned Personally Enabled (COPE), die das traditionelle Modell "Unternehmen stellt seinen Mitarbeitern Geräte zur Verfügung" ergänzen.

Ganz gleich, welches Konzept Unternehmen in Bezug auf mobile Geräte verfolgen: Die Zahl der Hardware- und Softwareplattformen, die sie unterstützen müssen, ist groß. Dies erhöht die Komplexität für die dringlichste Herausforderung in diesem Umfeld: Die IT-Sicherheit.

Hacker haben leichtes Spiel bei Smartphones

Geschäftlich genutzte Smartphones sind eine wahre Fundgrube für Angreifer: 79 % der User greifen nach einer Untersuchung von **Dimensional Research**[1] damit auf ihre Unternehmens-E-Mails zu, 65 % auf ihre Geschäftskontakte, 47 % auf sensitive Kundendaten, 38 % auf gespeicherte PINs und Passwörter und 32 % auf Unternehmensinformationen über Business-Anwendungen.

Das Risiko, dass neben den internen Mitarbeitern auch Externe unbefugt auf Unternehmensdaten zugreifen, ist groß:

- Viele Mitarbeiter nutzen ungesicherte WLAN-Netze wie etwa an Flughäfen oder Bahnhöfen anstatt über gesicherte VPN-Zugänge ins Unternehmensnetz zu gelangen. Nach einer Umfrage von **Motorola**[2] unter 1000 Anwendern haben dies in der Vergangenheit bereits 48 % getan - und sich damit der Gefahr eines Man-in-the-Middle-Angriffs ausgesetzt.

- Nur 7 % der Unternehmen gehen nach Erhebungen von Citrix davon aus, dass ihre Mitarbeiter keine private Apps auf ihren beruflich eingesetzten Smartphones und Tablets nutzen. Dabei ist die Sicherheit mobiler Apps als kritisch einzustufen, wie der **HP Cyber Risk Report 2013**[3] aufdeckt: Über die Third-Party-Apps erhalten Unberechtigte durch zu lax gehandhabte Berechtigungen Zugriff auf sensible Unternehmensdaten

Viele Unternehmen sind sich der Gefahren zwar bewusst. Doch nur ein Drittel nutzt nach Erhebungen von **Forrester Research**[4] aktuell Technologien für die mobile Sicherheit. Die Mehrzahl dieser Unternehmen setzt aktuell auf Lösungen für das Mobile Device Management (MDM). Sie stellen zum Beispiel Funktionalitäten für die Administration und Steuerung von Geräteeinstellungen oder für den Echtzeit-Blick auf installierte Anwendungen und Sicherheitskonfigurationen zur Verfügung. Doch traditionelle MDM-Lösungen greifen zu kurz angesichts der Komplexität und der sich ständig verändernden Rahmenbedingungen für Mobile Security.

MDM-Lösungen schützen nur Geräte, nicht Anwendungen und Daten

MDM-Lösungen wurden für Geräte im Unternehmensbesitz konzipiert und ignorieren etwa Ansätze wie BYOD. Außerdem fokussieren sie sich auf die Sicherheit von Geräten; wesentlich zielführender ist jedoch der Schutz der darunter liegenden Unternehmensdaten.

Um den Mitarbeitern von überall den sicheren Zugriff auf Unternehmensdaten zu ermöglichen - und dabei gleichzeitig deren Produktivität zu garantieren und die Kosten im Griff zu haben, bedarf es mehr als technischer Punktlösungen wie MDM - oder die zweifellos positiv zu bewertende Entwicklung hin zu Mobile Application Management. Enterprise Mobility Management tritt daher an die Stelle von MDM: ein ganzheitlicher und granularer Ansatz, um mobile Geräte, Applikationen und Inhalte zu managen und zu schützen.

Offene Strategie, die auch künftige Anforderungen erfüllt

Gefragt ist dabei eine offene und modulare Mobile Security Strategie, auf deren Basis Unternehmen nicht nur den aktuellen, sondern auch den künftigen Anforderungen an das mobile Business schnell und komplett begegnen können. Sie muss als ganzheitlicher Ende-zu-Ende-Prozess gesehen werden.

Dabei muss eines klar sein: Unternehmen müssen eine Balance finden zwischen den für die Informationssicherheit erforderlichen Maßnahmen einerseits und der Benutzerfreundlichkeit andererseits. Denn Mobile-Security-Maßnahmen dürfen letztlich nicht die Produktivität der Endanwender einschränken,da diese sonst oft zu anderen Tools ausweichen, die die Nutzerfreundlichkeit in den Vordergrund stellen. Es ist aber nicht gewährleisten, dass diese denselben Anspruch an Security haben. Ein Beispiel in diesem Zusammenhang ist die Verwendung von Dropbox in Unternehmen; die Security wird durch diese Schatten-IT massiv untergraben.

Mit den richtigen Lösungen können Organisationen angemessen antworten, Risiken minimieren und ihre Angriffsflächen deutlich reduzieren. Doch welchen Weg sollten Unternehmen für eine solche Mobile Security Strategie einschlagen? Es empfiehlt sich, zunächst alle Anwendungsfälle und Anforderungen des Business und die damit verbundenen Sicherheitsrisiken und -anforderungen zu analysieren und identifizieren - unabhängig von der im Einsatz befindlichen Technologie: Welche Business-Risiken bestehen heute und in Zukunft für das Unternehmen? Welche Compliance-Anforderungen muss es erfüllen? Welche rollenspezifischen Anwendungsfälle gibt es im Unternehmen? Sollten E-Mails grundsätzlich verschlüsselt sein? Auf welche Technologien und Konzepte will das Unternehmen in den nächsten Jahren setzen? Sollten Business-Anwendungen in passwortgeschützten Containern, die unabhängig von der "normalen" Arbeitsumgebung eines mobilen Geräts agieren, gesichert werden?

Die Vorteile dieser Container:Die IT-Abteilung hat die Kontrolle über sie, kann also deren Inhalte ändern oder den Container bei Bedarf komplett löschen.

Auf Basis dieser Analyse gilt es dann, eine Strategie und Roadmap zu entwickeln, mit der auch in Zukunft die Mobile Security Ziele erreicht werden können. Ein Ansatz mit mehreren Management-Schichten ist dabei empfehlenswert: Neben MDM sollten Mobile Application Management (MAM) und Mobile Content Management (MCM) adressiert werden. MAM sorgt für die sichere Verwaltung und Verteilung von mobilen Anwendungen für beliebige Geräte.

Dazu gehört auch ein unternehmenseigener App-Store, in dem die IT-Abteilung den Endanwendern sichere Anwendungen gekapselt und mit sicherem Zugang zum Intranet zur Verfügung stellt. Mittels MCM gewährt die ITden Mitarbeitern im Unternehmen einen mobilen und zugleich sicheren Zugriff auf Unternehmensdokumente sowie deren Austausch und Collaboration mit Kunden und Partnern. Dabei können Management- und Sicherheitsrichtlinien zentral angewendet und durchgesetzt werden, um die Sicherheit aller Unternehmensinformationen zu gewährleisten. Welche Lösungen für dasEnterprise Mobility Management konkret zum Einsatz kommen sollten, hängt dabei von den individuellen Anforderungen eines Unternehmens ab.

Technik alleine reicht nicht

Wesentlicher Bestandteil des Enterprise Mobility Management sind neben der Technik entsprechende Prozesse und das Bewusstsein der Mitarbeiter für die Gefahren. Immerhin 72 % der Unternehmen beklagen in der Studie von Dimensional Research, dass sorglose Mitarbeiter ein größeres Sicherheitsrisiko darstellen als Hacker. Daraus ergeben sich neue Fragestellungen: Verfügen die Mitarbeiter im Unternehmen über ein entsprechendes Sicherheitsbewusstsein? Wurden Sie entsprechend geschult? Gibt es bereits eine Mobility-Strategie? Welche Risiken sind für das Unternehmen mit Mobility verbunden? Welche regulatorischen Vorgaben müssen eingehalten werden? Welche Regeln gibt es im Unternehmen? Werden Themen dieser Art nicht adressiert, werden Unternehmen sehr schnell von der Realität überholt - und können nur noch reagieren. Das Beispiel BYOD hat es gezeigt.

HP bietet eine Reihe von Services zum Thema Mobile Security an, die sich über den gesamten Lebenszyklus von Mobilty Services erstrecken - angefangen bei der Strategie und der Anforderungsanalyse über Integration und Implementierung sowie verschiedene Betriebsmodelle bis hin zur kontinuierlichen Weiterentwicklung. HP Enterprise Security Services hat dafür verschiedene Workshops in Modulbauweise entwickelt, die Unternehmen den Start erleichtern.

Darüber hinaus hilft HP Enterprise Services Unternehmen, die für sie individuell richtigen Ende-zu-Ende-Mobility-Lösungen zu finden: HP verfügt selbst über viele Security-Lösungen wie etwa HP Helion Mobility und arbeitet darüber hinaus mit einem Netzwerk von Partnerunternehmen wie Citrix und SAP eng zusammen, die über große Expertise in diesem Bereich verfügen.

Links im Artikel:

[1] **http://www.dimensionalresearch.com/**
[2] **http://www.motorola.de/**
[3] **http://www8.hp.com/hpnext/posts/hp-cyber-risk-report-2013-and-state-security-operations#.U6w4xrGvz9o**
[4] **http://www.forrester.com/home/**
