SOPHOS
Security made simple.

Container für mobile Geräte: Die Matroschkas der Mobile-Security-Welt

Egal, ob ein Unternehmen ein Bring Your Own Device (BYOD) Programm oder ein Choose Your Own Device (CYOD) Programm implementiert: Das zentrale Problem ist und bleibt die Sicherheit. Dabei spielt es keine Rolle, wem das mobile Gerät gehört, mit dem auf Unternehmensdaten zugegriffen wird. Geht das Gerät verloren, ist die Sicherheit der auf ihm gespeicherten Unternehmensdaten gefährdet. Viele IT-Organisationen überfrachten mobile Geräte mit Sicherheitsbeschränkungen, um zu verhindern, dass Unbefugte im Falle eines Verlusts oder Diebstahls Zugriff auf Daten erhalten. Aber das Sicherheitsproblem ist nicht das Gerät selbst – das Problem sind die Daten. Hier helfen Container. Mit Containern können Sie sensible Daten und E-Mails auf Tablets und Smartphones schützen – unabhängig davon, wem das Gerät gehört. Container liefern IT-Abteilungen die Kontrollmechanismen, die sie benötigen, um Unternehmensdaten zu schützen, ohne die Privatsphäre oder die Produktivität der Benutzer zu beeinträchtigen.

Unternehmenssicherheit vs. Wahrung der Privatsphäre

Fast jeder nutzt heutzutage mobile Geräte – sowohl im Berufs- als auch im Privatleben. Die mobilen Geräte dienen uns zur Pflege unserer sozialen Beziehungen, als Kameras, Kalender und Telefon. Fast alle Mitarbeiter kaufen ihre eigenen Smartphones und Tablets. Jeder möchte vernetzt sein und von unterwegs aus arbeiten können – ob auf der Zugfahrt nach Hause oder im Wartezimmer einer Arztpraxis. Der Zugriff auf Unternehmensdaten und -E-Mails über mobile Geräte ist keine Ausnahme mehr, sondern längst die Norm.

Aktuell gibt es weltweit 2,6 Mrd. Smartphone-Verträge. Bis 2020 werden weltweit 6,1 Mrd. Smartphones im Umlauf sein. **– Ericsson Mobility Report**

Dank des Siegeszugs mobiler Geräte sind die Zeiten, in denen Unternehmensdaten sicher in Rechenzentren gespeichert wurden, endgültig vorbei. Daten werden in- und außerhalb des Netzwerks sowie über ungeschützte öffentliche Netzwerke hinweg auf hunderte, oder sogar tausende mobile Geräte übertragen. Die Vielfalt der übertragenen Daten ist groß und reicht von Kontaktdaten über Vertriebspräsentationen und Projektvorschläge bis hin zu Tabellenkalkulationen. Benutzer erwarten, dass sie auf ihren mobilen Geräten uneingeschränkt arbeiten können, wenn sie unterwegs sind.

4,3 % der von Unternehmen ausgegebenen Smartphones gehen jedes Jahr verloren oder werden gestohlen. **– Kensington**

Jedes Dokument, jede E-Mail und jede auf einem mobilen Gerät gespeicherte Datei ist potenziell gefährdet. Aufgrund ihres Taschenformats gehen mobile Geräte leicht verloren, werden liegengelassen oder gestohlen. In all diesen Situationen besteht die Gefahr, dass Unternehmensdaten in die falschen Hände geraten. Ein Angreifer muss ein mobiles Gerät nicht in den Händen halten, um auf die auf ihm gespeicherten Daten zugreifen zu können. Daten können auch von in Schad-Anwendungen eingebetteter Malware extrahiert werden. Oft akzeptieren Benutzer Anwendungsberechtigungen, ohne die möglichen Folgen zu bedenken. Auf diese Weise können sie Schad-Anwendungen Zugriff auf Kontakte und andere sensible Daten gewähren.

Der Schutz vor potenziell unerwünschten Anwendungen (PUAs) hat für viele Benutzer nur eine nachrangige Bedeutung. Sie denken lediglich an die Vorteile, die ihnen eine App persönlich verschafft – ob es sich um eine Blitzlicht-App oder eine App für Tischreservierungen in Restaurants handelt – die meisten Benutzer kümmert es nicht, dass viele Apps unnötige Zugriffsrechte auf Kameras und andere sensible Daten wie die Kontakte einfordern.

Unabhängig davon, ob sich ein Gerät im Privatbesitz befindet oder vom Unternehmen ausgeben wurde: Die meisten Benutzer – insbesondere die sogenannte Generation Y – nutzen ihr mobiles Gerät sowohl beruflich als auch privat. Und um die Sache noch komplizierter zu machen, fordern sie auch noch die Wahrung ihrer Privatsphäre. Unternehmen können verloren gegangene oder gestohlene Geräte also nicht einfach zurücksetzen, da in diesem Fall auch die privaten Daten des Benutzers gelöscht würden. In einigen Rechtssystemen können Unternehmen für die privaten Daten ihrer Mitarbeiter haftbar gemacht werden. Selbst wenn Benutzer separate Privatgeräte nutzen, befinden sich auf den vom Unternehmen ausgegebenen Geräten fast immer einige private Daten.

Zum Leidwesen der IT sind nicht alle Benutzer mit dem gleichen Gerätetyp zufrieden. Wenn die IT „nur" iOS, Windows und Android verwalten müsste, wäre die Lage noch einigermaßen übersichtlich. Doch nicht nur zwischen diesen drei Betriebssystemen gibt es gravierende Unterschiede im Hinblick auf Funktionalität, Verwaltung und Sicherheit. Durch die Fragmentierung des Android-Markts existieren laut OpenSignal mittlerweile mehr als 24.000 verschiedene Android-Gerätemodelle. Alle Hardware-Hersteller nehmen Optimierungen ihrer Betriebssysteme vor, um geräteseitige Funktionen zu verbessern. Google kann eine neue Version seines Betriebssystems einführen, hat jedoch keine Kontrolle darüber, ob OEMs diese auf ihre Geräte übertragen. Dies hat zur Folge, dass IT-Organisationen jedes einzelne Gerät in die Hand nehmen und Benutzern zeigen müssen, wie sie die Sicherheitskontrollen richtig implementieren.

Die Antwort: Sichere Container für mobile Geräte

Die effektivste Methode zur Lösung dieser Datenschutzprobleme ist die Implementierung von Containern. Container-Lösungen erstellen auf mobilen Geräten abgetrennte, sichere Bereiche, in denen die Nutzer auf Unternehmensdaten und Anwendungen zugreifen können. Der Container ist passwortgeschützt und verschlüsselt. So schützt und isoliert er Daten vor unbefugten Zugriffen, Malware, anderen Anwendungen und Systemressourcen. Die Container-Lösung wird als Software auf das mobile Gerät heruntergeladen. Innerhalb des Containers können Benutzer dann geschützte Anwendungen herunterladen und ausführen.

Viele Mobilgerätehersteller bieten native Container an. Drittanbieter-Container dagegen bieten Sicherheit und Konsistenz für eine Vielzahl von Plattformen und lösen damit ein zentrales Problem, mit dem IT-Organisationen zu kämpfen haben: die effiziente Verwaltung unterschiedlichster mobiler Geräte. Mit Containern lassen sich Daten auf mobilen Geräten einfach verwalten. Egal, ob es sich um private oder vom Unternehmen ausgegebene Geräte handelt und unabhängig vom Android-, Windows- und/oder iOS-Modell.

Für mobile Geräte gibt es verschiedene Arten von Containern:
Ein E-Mail-Container dient als PIM(Personal Information Management)-Lösung für E-Mails, Kalender und Kontakte und ist der am häufigsten genutzte Containertyp in Unternehmen. Der Container ermöglicht jedem Benutzer einen einheitlichen und sicheren E-Mail-Zugang, unabhängig vom genutzten Gerät. Unternehmens-E-Mails, -kalender und -kontakte werden von anderen Anwendungen auf dem Gerät isoliert. Auf diese Weise sind IT-Abteilungen in der Lage, gezielt nur die Unternehmensdaten zu entfernen, wenn ein Mitarbeiter das Unternehmen verlässt oder das Gerät verloren geht bzw. gestohlen wird. Die IT-Abteilung kann auch einen zusätzlichen Passwortschutz für berufliche E-Mails einrichten. Ein E-Mail-Container schützt nicht nur E-Mail-, Kalender- und Kontaktdaten, sondern löst auch das Android-Fragmentierungsproblem.

Ein Inhaltscontainer sorgt für eine sichere, über Zugriffsrechte gesteuerte Arbeitsumgebung, in der Benutzer produktiv arbeiten können und in der die IT die Kontrolle über Unternehmensdaten behält. Benutzer können Dokumente aufrufen, austauschen und gemeinsam an diesen arbeiten. So ist gewährleistet, dass alle an derselben Version eines Dokuments arbeiten. IT-Abteilungen können kontrollieren, wie Benutzer Dokumente ändern, austauschen und verteilen. Außerdem können sie vorgeben, welche Cloudspeicher-

WICHTIGE FRAGEN FÜR DIE BEREITSTELLUNG VON CONTAINER-LÖSUNGEN

- **Welche Daten übertragen Sie an Ihre Mitarbeiter?**
- **Welche Dateien und Dokumente möchten Sie schützen?**
- **Auf welche Betriebssysteme sind Sie angewiesen?**
- **Müssen Sie den Austausch von E-Mails zwischen verschiedenen Android-Versionen ermöglichen?**

Anwendung genutzt werden darf. Durch die Einbindung einer Dateiverschlüsselung können verschlüsselte Dateien an den Inhaltscontainer gesendet und nur dann geöffnet werden, wenn das Gerät sich in einem sicheren Zustand befindet und der Benutzer seine Identität mit einem Passwort verifizieren kann. Die Verschlüsselung kann auch überwacht und kontrolliert werden, sodass nur verschlüsselte Dateien in der Cloud gespeichert werden. Zudem ist innerhalb eines Containers die Bereitstellung eines Unternehmensbrowsers möglich, über den ein sicherer Browser-Zugriff erfolgen kann. Die IT-Abteilung kann die am häufigsten genutzten geschäftsrelevanten und Unternehmens-Websites für einen sicheren Zugriff per Push an Benutzer übertragen. Der Browser ermöglicht zudem einen einfachen Single-Sign-On-Zugriff auf unternehmensinterne Intranet-Sites und andere häufig besuchte Websites. Die IT kann die „save password"(sicheres Passwort)-Funktion auf Wunsch aktivieren oder deaktivieren, um das Risiko für wichtige Unternehmens-Websites zu minimieren, und das Kopieren sensibler Daten aus dem Unternehmensbrowser unterbinden.

Container für mobile Geräte können wir uns als Matroschkas der Mobile-Security-Welt vorstellen: Jede Puppe repräsentiert eine andere Verschlüsselungsebene. Die erste, größte Puppe ist die Verschlüsselung des mobilen Geräts. Die nächste Puppe ist der Container des mobilen Geräts, der ebenfalls verschlüsselt ist, und die kleinste Puppe ist die verschlüsselte Datei. Container innerhalb von Containern bieten daher mehrere Verschlüsselungsebenen.

Container: Nur ein Element einer erfolgreichen Mobile-Security-Strategie

Zwar spielen Container-Lösungen beim Schutz von Unternehmensdaten auf mobilen Geräten eine wichtige Rolle. Für eine ganzheitliche Mobile-Security-Strategie müssen jedoch noch weitere Elemente berücksichtigt werden. Für Android-Geräte ist beispielsweise ein Malware-Schutz unerlässlich, da bei ihnen das Infektionsrisiko höher ist als auf iOS-Geräten. Außerdem muss die IT in der Lage sein, Sicherheitsmaßnahmen wie die Verwendung sicherer Passwörter und die Sperrung von Geräten mit Jailbreak durchzusetzen. Der Zugriff auf Container sollte über ein gesondertes Passwort erfolgen, jedoch nur dann gewährt werden, wenn gewährleistet ist, dass das Gerät nicht gerootet, mittels Jailbreak manipuliert oder von Malware infiziert wurde.

Container sollten benutzerfreundlich sein und die Verschlüsselung sollte für Enduser nahtlos erfolgen. Das bedeutet allerdings nicht, dass IT-Organisationen die Benutzeraufklärung außer Acht lassen dürfen. Besonders im Fall von BYOD müssen Benutzer darüber aufgeklärt werden, warum ein Container erforderlich ist, welchen Schutz er bietet und welche Auswirkungen er auf die Benutzerfreundlichkeit hat. Benutzer müssen beispielsweise verstehen, dass ihr Gerätepasswort weiterhin eine vierstellige PIN sein kann, der Container selbst jedoch ein zusätzliches, längeres Passwort hat, das sich nicht so leicht knacken lässt.

Eine Mobile-Security-Strategie sollte auch ein Self-Service-Portal vorsehen, in dem Benutzer bestimmte Helpdesk-Aufgaben selbst erledigen können, um die IT-Abteilung zu entlasten. Mit Zustimmung der IT-Abteilung sollten Benutzer beispielsweise in der Lage sein, ihre eigenen Geräte zu registrieren, einen Container und andere Unternehmensanwendungen zu installieren, Passwörter zurückzusetzen, ihr Gerät zu sperren und zurückzusetzen sowie ein Gerät außer Betrieb zu setzen.

Die Container-Lösung sollte auch in das WLAN des Unternehmens eingebunden sein, um zu verhindern, dass ein schädliches oder kompromittiertes Gerät sich mit Unternehmensressourcen verbinden kann. Wenn ein schädliches Gerät versucht, sich mit dem Netzwerk zu verbinden, sollte die Lösung den Container sperren, das Gerät isolieren und es in die Quarantäne verschieben oder das Gerät bei einer Kompromittierung daran hindern, sich mit dem E-Mail-Server zu synchronisieren.

Ein besonders wichtiges Element jeder Mobile-Security-Strategie ist außerdem eine zuverlässige Verschlüsselung. Eine Verschlüsselung schützt Daten innerhalb eines Containers. Wenn Dateien außerhalb des Unternehmens ausgetauscht werden müssen, kann als zusätzliche Sicherheitsvorkehrung auch eine Dateiverschlüsselung ergänzt werden.

Fazit

Egal, für welches Mobilitätsprogramm sich ein Unternehmen entscheidet – BYOD oder CYOD – die Sicherheit der Daten auf mobilen Geräten muss gewährleistet sein. Container-Lösungen sind die beste Methode, berufliche und private Daten sauber zu trennen. Unternehmen schützen sich damit effektiv vor Datenverlusten und Malware, gleichzeitig bleibt die Privatsphäre der Benutzer gewahrt. Doch so wichtig Container sind – sie stellen nur ein Element von mehreren innerhalb einer Mobile-Security-Strategie dar. Suchen Sie sich deshalb einen Technologieanbieter, der Sie bei der Umsetzung einer ganzheitlichen Mobile-Security-Strategie unterstützen kann, die auf robusten Containern gegründet ist. Achten Sie unbedingt darauf, dass der Anbieter die Sicherheit sowohl für die Benutzer als auch die IT-Abteilung einfach gestaltet.

Sophos Mobile Control

Mit Sophos Mobile Control schützen Sie Ihre mobilen Geräte, ohne die Benutzer bei der Arbeit zu behindern. Sophos Mobile Control verfügt über leistungsstarke Container, die Unternehmensdaten schützen, ohne die private Nutzung des Geräts zu beeinträchtigen. Über das einfache Verwaltungs-Dashboard können IT-Abteilungen Geräte komfortabel einrichten und verwalten und schnell auf Probleme reagieren. Sophos Mobile Control kann sowohl mit Sophos UTM (zur administratorseitigen Sperrung des WLAN- und VPN-Zugriffs für nicht richtlinienkonforme Geräte) als auch mit Sophos SafeGuard (für den benutzerseitigen Zugriff auf verschlüsselte Daten über Mobiltelefone und Tablets) integriert werden.

Sophos Mobile Control beinhaltet E-Mail-, Inhalts- und native Betriebssystem-Container sowie einen Unternehmensbrowser. Zu den Top-Features zählen:

- Eine sichere Lösung für Unternehmens-E-Mails, -kalender und -kontakte
- Sicherer Zugriff auf Dateien auf mobilen Geräten mit Möglichkeit zur Bearbeitung und Erstellung neuer Dateien
- Kontrolle des Zugriffs und der Veröffentlichungsrechte für Cloudspeicher (z. B. Dropbox, Google Drive)
- Sicherer Browser-Zugriff auf die am häufigsten genutzten Unternehmens-Websites
- Unterstützung nativer Betriebssystem-Container – Samsung Knox und iOS-verwaltet
- Vielfach ausgezeichneter Malware-Schutz aus den SophosLabs

Erfahren Sie mehr

und testen Sie die Online-Demo unter
www.sophos.de/mobile

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

03.16/NP.wpde.simple

SOPHOS