Virtual Solution

CONTAINER

EINE SICHERE LÖSUNG FÜR MOBILE GERÄTE

Mobile Geräte wie Smartphones oder Tablets geraten immer stärker ins Fadenkreuz von Hackern, weil sie vermehrt Funktionen für geschäftskritische Prozesse bieten und mit dem Backend des Unternehmens verbunden sind. Doch bislang verfügen nur etwas mehr als die Hälfte aller Smartphones in Firmen über effiziente Sicherheitslösungen gegen Cyberangriffe. Hier besteht großer Nachholbedarf. Anstatt die Hardware zu schützen geht es künftig verstärkt um den Schutz der auf dem Gerät gespeicherten Daten. Das Modell der Zukunft für die sichere mobile Kommunikation auf Smartphone und Tablet sind Container.

Container packen firmeninterne Daten, E-Mails, Kontakte, Kalender, Notizen oder auch Dokumente in einen sicheren, verschlüsselten und abgeschotteten Bereich. Damit befinden sich die Daten eines Unternehmens auf dem mobilen Gerät in einer geschützten Umgebung - egal, ob es privat ist oder von der Firma gestellt wird. Daten werden so vor unbefugten Zugriffen, Verlust oder Manipulation geschützt. Container gewährleisten zudem die strikte Trennung von firmeninternen und privaten Daten. Bei der Auswahl einer Container-Lösung sollten Unternehmen unter anderen darauf achten, dass sie eine direkte Verbindung zwischen Client und Server herstellt, auf einem geprüften Security-Framework basiert, kryptografische Standards einsetzt und die Option für Hardware-basierte Sicherheit mit Smartcards unterstützen kann.

CONTAINER

Die Zukunft der Arbeit ist mobil

Der stationäre Arbeitsplatz wird zum Auslaufmodell. Beschäftigte, die vorwiegend an einem einzigen, stationären Arbeitsplatz sitzen, stellen mit 46 Prozent mittlerweile die Minderheit. Mehr als die Hälfte der Beschäftigten (54 Prozent) sind vorwiegend oder sogar ausschließlich mobil an wechselnden Arbeitsplätzen tätig, etwa auf Geschäftsreisen, an wechselnden Orten innerhalb des Unternehmens oder im Home Office.

Das sind die zentralen Ergebnisse der Studie „Mobiles Arbeiten“, welche die Deutsche Gesellschaft für Personalführung (DGFP) gemeinsam mit der Hochschule für Technik und Wirtschaft Berlin (HTW), der spring Messe Management sowie dem Büro für Arbeits- und Organisationspsychologie (bao GmbH) veröffentlicht hat. Der Trend zum mobilen Arbeiten wird sich künftig weiter fortsetzen.

Für die IT-Abteilung stellt die Integration mobiler Geräte in die vorhandene Infrastruktur allerdings eine große Herausforderung dar - unabhängig davon, ob die Mitarbeiter ihre privaten Smartphones oder Tablets beruflich nutzen (Bring Your Own Device - BYOD), oder ob das Unternehmen das mobile Gerät etwa im COPE-Ansatz (Corporate Owned, Personally Enabled) zur Verfügung stellt.

Neben der eigentlichen Verwaltung der Geräte stellt sich vor allem die Frage nach Sicherheit und Datenschutz. Mobile Endgeräte können leicht verloren gehen. Für diesen Fall muss sichergestellt sein, dass kein Unbefugter Zugriff auf die Firmeninformationen bekommt und die Daten auf einem Ersatzgerät schnell wieder verfügbar sind. Geräte enthalten oft persönliche Inhalte des Mitarbeiters (z. B. Fotos oder Kontakte) und es besteht die Gefahr, dass die IT-Administratoren auf private Daten der Mitarbeiter zugreifen, was die Mitarbeiter nicht gerne sehen. Die Mitarbeiter selbst müssen die Grenze zwischen privater und beruflicher Nutzung erkennen, da die betrieblich genutzten Smartphones auch sensible Unternehmensdaten enthalten. Und es muss sichergestellt werden, dass Mitarbeiter keine unerlaubten Anwendungen auf ihren Geräten installieren, die gut getarnte Malware beinhalten oder Firmendaten abgreifen.

Mobile Geräte immer stärker im Fadenkreuz von Hackern

Stichwort Malware: Mobile Geräte wie Smartphones oder Tablets werden grundsätzlich zu einem immer attraktiveren Ziel für Hacker, weil sie vermehrt Funktionen für geschäftskritische Prozesse bieten und mit dem Backend des Unternehmens verbunden sind. Alarmierend sind hier die Zahlen aktueller Studien von Kaspersky Lab und IDC.

CONTAINER

Kaspersky Lab entdeckte im Jahr 2016 mit 8,5 Millionen schädlichen Installationen fast dreimal so viele mobile Schädlinge wie im Jahr 2015. Im Bericht[1] über die mobile Bedrohungslage im Jahr 2016 weist der Security-Spezialist zudem auf den starken Anstieg von mobiler Ransomware hin, mit der Angreifer Daten auf dem Smartphone verschlüsseln, um Lösegeld für deren Freigabe zu erpressen.

Laut Kaspersky gehören 16 der 20 häufigsten mobilen Schädlinge aus dem Jahr 2016 zur Kategorie „Mobile Werbetrojaner“ - im Vorjahr waren es noch 12. Das Problem: Werbetrojaner sind in der Lage, Super-Nutzer-Rechte zu erlangen, über die sie neben lästigen Werbeeinblendungen auch andere Anwendungen heimlich installieren oder Apps in Google Play kaufen können.

Dass sich die Sicherheitslage für Smartphones und Tablets im letzten Jahr weiter verschärft hat, bestätigt die Studie „Mobile Security in Deutschland 2017“ der Marktforscher von IDC. Ihr zufolge berichten 65 Prozent der befragten Unternehmen von Angriffen auf mobile Endgeräte, das sind acht Prozentpunkte mehr als 2015 - die Dunkelziffer an unentdeckten Vorfällen nicht berücksichtigt. Laut IDC erlitten 26 Prozent der Unternehmen im vergangenen Jahr einen Schaden von mehr als 100.000 Euro durch Sicherheitsvorfälle mit mobilen Technologien - ganz zu schweigen von Einbußen an Reputation und Vertrauen. Insbesondere Anwaltskosten, Strafzahlungen oder Geschäftseinbußen treiben hier die Kosten in die Höhe.

Schutz von Geräten oder Daten - Welche Möglichkeiten gibt es?

Angesichts der zunehmenden Gefahren durch mobile Malware sollten Unternehmen und Mitarbeiter firmeninterne Daten und Informationen auf ihren Smartphones und Tablets umfassend schützen. Die Realität sieht aber anders aus. Kaspersky Lab hat 2016 in einer Umfrage[2] festgestellt, dass 2016 weltweit nur 53 Prozent aller Smartphones in Firmen über Sicherheitslösungen gegen Cyberangriffe verfügten. Hier besteht also großer Nachholbedarf. Neben der Hardware geht es künftig verstärkt um den Schutz der auf dem Gerät gespeicherten Daten beziehungsweise Inhalte.

Firmen lösen die Herausforderung traditionell mit einer vollständigen Kontrolle über das Endgerät (Mobile Device Management). Das primäre Ziel ist es, die mobilen Geräte zentral zu verwalten, einheitliche Sicherheitseinstellungen und Richtlinien für Smartphones oder Tablets festzulegen, Konfigurationen zu verändern oder Zugriffsrechte zu definieren. Zudem will er verlorene oder gestohlene Geräte aus der Ferne (remote) sperren oder deren Inhalte löschen.

Die Herausforderung wird jedoch komplexer, wenn Mitarbeiter ihre privaten Smartphones oder Tablets auch beruflich einsetzen (BYOD) oder ihre Firmen-Geräte auch privat nutzen dürfen (COPE). Dann müssen die privaten und geschäftlichen Daten strikt getrennt sein. Schließlich wollen Mitarbeiter nicht die Kontrolle über ihre privaten Urlaubsfotos oder Social-Media-Aktivitäten an die IT-Abteilung ihrer Firma abgeben. Der Administrator wiederum will nicht, dass sensible Firmendaten im selben Verzeichnis liegen wie persönliche Dokumente oder Videos des Mitarbeiters oder dass private Apps Zugriff auf dienstliche Informationen (z. B. Kontaktdaten) haben.

Mobile Application Management löst das Problem nur teilweise. Diese Lösungen regeln, welcher Nutzer gemäß seiner Rolle im Unternehmen auf welche Anwendungen zugreifen darf und sorgen dafür, dass die Installation und der Zugriff auf Apps nur nach den Unternehmensrichtlinien erfolgen. Weiterhin unterstützt MAM den Administrator bei der Bereitstellung, Lizenzierung und dem Application Lifecycle Management der mobilen Software. Zudem ist es damit möglich, den Austausch betrieblicher Daten zwischen mobilen Apps zu kontrollieren und einzuschränken.

Doch die reine Verwaltung von Apps oder Endgeräten bietet noch keine Sicherheit und löst nicht das Problem der Trennung von privaten und geschäftlichen Daten. Das Modell der Zukunft für die sichere mobile Kommunikation auf Smartphone und Tablet sind Container.

[1] Quelle: www.securelist.com (https://de.securelist.com/mobile-malware-evolution-2016/72443/)
[2] Quelle: Kapersky Lab

CONTAINER

Container verschlüsseln Inhalte und trennen berufliche von privaten Daten

Container legen den Fokus auf den Schutz der Informationen und Daten auf dem mobilen Endgerät und sind unabhängig von der Sicherheit des darunterliegenden Betriebssystems. Entsprechende Lösungen packen Unternehmensdaten, E-Mails, Kontakte, Kalender, Notizen oder auch Dokumente in einen sicheren und verschlüsselten Bereich (Container). Damit lassen sich die Daten eines Unternehmens auf dem mobilen Gerät in einer geschützten, abgeschotteten Umgebung bearbeiten und verwalten. Daten werden vor unbefugten Zugriffen, Verlust oder Manipulation geschützt und können nicht unkontrolliert ab- oder einfließen.

Container gewährleisten zudem die strikte Trennung von firmeninternen und privaten Daten. Das heißt: Ein Nutzer kann aus dem Unternehmens-Bereich heraus nicht auf seine privaten Apps zugreifen. So verhindert eine Container-Lösung beispielsweise, dass Firmeninformationen per Copy & Paste auf Facebook oder Twitter landen. Zugleich wird aber auch die Privatsphäre der Mitarbeiter geschützt.

Um die Sicherheit der Datenübertragung zu gewährleisten verschlüsseln die meisten Container-Lösungen die Datenübertragung. Somit sind die Daten sowohl im Container auf dem Endgerät geschützt als auch bei der Übertragung.

Container vereinen die unterschiedlichen Ansprüche von Anwendern, IT-Abteilungen und CISOs

Container bieten Vorteile für drei Nutzergruppen, deren Bedürfnisse teils stark voneinander abweichen: Anwender, IT-Administratoren und Compliance-Verantwortliche beziehungsweise CISOs (Chief Information Security Officer).

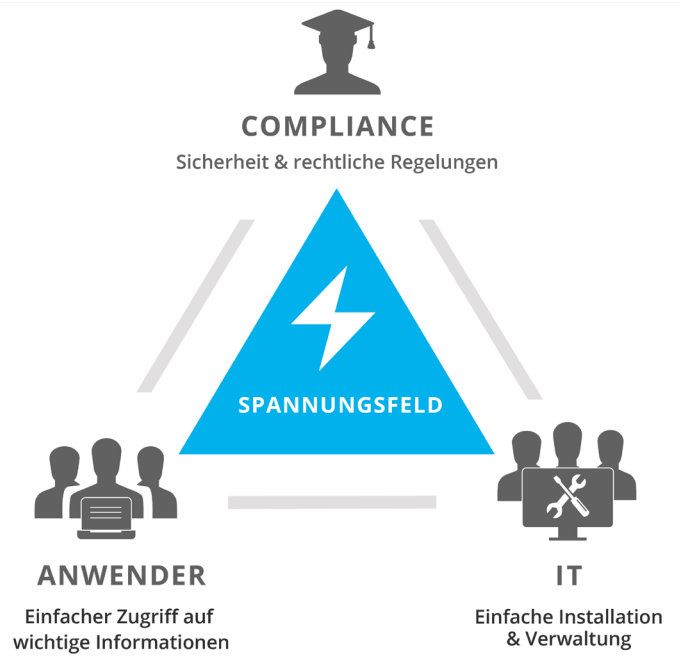
Die **Anwender** profitieren zunächst von der einfachen und schnellen Installation der Container-App. Sie laden sich die App aus dem App Store oder Google Play herunter und loggen sich mit ihren Anmeldeinformationen und/oder ihrem Registrierungscode ein. Dank einer intuitiven Benutzeroberfläche finden sie sich sofort ohne spezielles Training zurecht. Nach dem Öffnen der Container-App befindet sich der Mitarbeiter automatisch im beruflichen, geschützten Bereich, keine andere App kann mehr auf die Daten zugreifen. Damit können sie mit ihrem Smartphone auch von unterwegs sicher und produktiv arbeiten sowie ihre mobilen Geräte problemlos privat nutzen, da die IT-Abteilung nur den Container mit den Unternehmensdaten kontrolliert und nicht auf die privaten Daten zugreifen kann.

CONTAINER

Der **IT-Administrator** verwaltet die Container entweder über ein Management-Portal des Container-Anbieters oder eine bestehende MDM-Lösung. Darüber kann er Sicherheitsregeln wie etwa Vorgaben für die Länge von Passwörtern, den Einsatz von Smartcards oder Regeln für das Sperren von Geräten oder das Löschen von Inhalten aus der Ferne (Remote Wipe) schnell und einfach festlegen. Natürlich ist es möglich, diese Policies je nach Sicherheits-Anforderungen des Unternehmens flexibel anzupassen. So kann der Admin beispielsweise den Einsatz von Sprach-Assistenten wie Siri, Fingerabdruck-Sensoren für die Authentifizierung oder die teilweise Verknüpfung von beruflichen und privaten Kontakten aus dem Adressbuch erlauben. Damit keine sensiblen Inhalte im RAM des Geräts gespeichert werden, kann er auch die Copy & Paste-, Autovervollständigungs- oder Autokorrektur-Funktionen ausschalten.

Die IT-Abteilung bestimmt über die Management-Konsole zentral, wer entsprechend seiner Rolle mit seinem mobilen Endgerät Zugriff auf welche Unternehmensdaten erhält. Dabei kann er auch Rechte für bestimmte Anwendergruppen festlegen. Wenn der Mitarbeiter das Unternehmen verlässt, das Gerät verloren geht oder gestohlen wird, lassen sich die Unternehmensdaten im Container umgehend löschen. Administratoren erhalten dadurch vollständige Kontrolle über die Firmeninformationen, ohne die Privatsphäre der Mitarbeiter zu verletzen.

Auch **die Sicherheits- und Compliance-Verantwortlichen** profitieren von Container-Lösungen, da sie damit Compliance-Anforderungen und Richtlinien auf dem mobilen Gerät einfacher durchsetzen können. Dank moderner Kryptografie-Technologien sind die Daten im Container und auch bei der Übertragung zuverlässig verschlüsselt. Damit lassen sich Man-in-The-Middle-Attacken verhindern. Und der wohl größte Vorteil: Die Firmendaten und private Informationen werden auf demselben Endgerät strikt voneinander getrennt. Damit eignen sich Container für COPE- und BYOD-Szenarien sowie Unternehmen, die sehr großen Wert auf die mobile Sicherheit ihrer Daten und den Schutz der Privatsphäre von Mitarbeitern und Kunden legen.



CONTAINER

Tipps: Darauf sollten Unternehmen bei der Auswahl einer Container-Lösung achten

Bei der Auswahl einer Container-Lösung sollten Unternehmen folgende Punkte beachten:

Einfach zu bedienende App

Die Container-Lösung sollte als App für das jeweilige mobile Betriebssystem (Apple iOS, Google Android etc.) des Smartphones oder Tablets optimiert sein und sich möglichst nah an die Usability von Native Apps orientieren. Container Apps sind fest auf dem Mobilgerät installiert, arbeiten aber auch offline. Sie nutzen die Funktionen des mobilen Geräts wie GPS-Modul, Kamera oder Mikrofon. Letzteres ist beispielsweise relevant, wenn Nutzer mit ihrer Smartphone-Kamera auch sicherheitskritische Inhalte erfassen wollen. Dazu gehören etwa Flipcharts, Beweissicherungsfotos oder Scans von Dokumenten.

Die Container-App SecurePIM beispielsweise bietet die Funktion Secure Camera. Diese greift direkt auf die Hardware des Geräts zu, nutzt weder die vorinstallierte Kamera-App noch speichert sie die Bilder in das Smartphone eigene Fotoalbum. Stattdessen legt Secure Camera die Fotos in einem gesicherten Container ab. Damit können Nutzer nun auch mit ihrem Smartphone in kritischen Anwendungsbereichen sicher fotografieren.

Direkte Verbindung zwischen Smartphone und Server

Die Verbindung zwischen dem Client und dem Mail-Server sollte direkt und ohne Umleitung über ein Network Operations Center (NOC) erfolgen, um eine hohe Verfügbarkeit und Geschwindigkeit bei der Datenübertragung zu gewährleisten. Eine Container-App sollte daher etwa den Microsoft Exchange-Server mit ActiveSync unterstützen, IBM Domino oder Z-Push, eine PHP-basierte OpenSource-Implementation des ActiveSync-Protokolls.

Einsatz von Krypto-Standards

Der Anbieter einer Container-Lösung sollte keine eigenen Verschlüsselungs-Algorithmen entwickeln, sondern auf bewährte Krypto-Standards wie S/MIME, AES-256, SHA-256 oder Elliptic Curve setzen. Nicht optimal ist RSA-2048, das vom Bundesamt für Sicherheit in der Informationstechnik als nicht mehr sicher klassifiziert wird. Auch der logische Nachfolger, RSA-4096, ist mit Vorsicht zu genießen. Bedingt durch die hohe Schlüssellänge steigen Speicherverbrauch und Prozessornutzung stark an. Besonders bei schwächeren Geräten wie Smartphones kann die allgemeine Leistung des Geräts und die Usability gestört werden. SecurePIM setzt daher auf das Krypto-Verfahren Elliptic Curve mit einer Schlüssellänge von 256 Bit, das die CPU des mobilen Geräts kaum fordert und wegen des Einsatzes von elliptischen Kurven statt Primzahl-Faktorisierung als ähnlich sicher wie RSA-4096 gilt.

Usability

Die Usability beziehungsweise Benutzerfreundlichkeit ist ein weiteres wichtiges Kriterium beim Kauf einer Container-Lösung für Smartphones und Tablets. Die App sollte einfach zu installieren und verwalten sein sowie die Leistung des mobilen Geräts nicht beeinträchtigen. Nur Sicherheit, die den Nutzer nicht einschränkt, wird sich durchsetzen.

Option: SmartCard für Hardware-basierte Sicherheit

Für Unternehmen oder auch Behörden, die höhere Sicherheitsanforderungen haben, reicht die Authentifizierung per Passwort oder Touch-ID oft nicht aus. Sie setzen daher zusätzlich auf Hardware-basierte Sicherheit via SmartCards. Eine Container-Lösung sollte SmartCards als zusätzliche Sicherheits-Option unterstützen und sicherheitsrelevante Prozesse wie die Entschlüsselung von Daten vom potenziell unsicheren Consumer-Gerät auf die SmartCard verlagern können. Ein Beispiel: Die SmartCard speichert einen nicht duplizierbaren Schlüssel. Der IT-Administrator bemerkt, wenn dieser Schlüssel verloren geht und kann so den unberechtigten Zugriff auf das Unternehmensnetz verhindern.

Virtual Solution

CONTAINER

SecurePIM von Virtual Solution: Sicheres mobiles Arbeiten

SecurePIM ermöglicht es Mitarbeitern von überall und jederzeit produktiv zu sein. Die Container-App packt E-Mails, Chatverläufe, Kontakte, Kalender, Notizen, Aufgaben, Dokumente und Intranet-Zugang auf dem Smartphone oder Tablet in einen sicheren und verschlüsselten Container, der mit einem Passwort, PIN oder per Touch/FaceID geschützt ist. Der Sicherheitsexperte Virtual Solution arbeitet dabei mit modernsten Verschlüsselungstechnologien. Die S/MIME-Verschlüsselung ist eine der derzeit sichersten Verschlüsselungsverfahren und sorgt damit dafür, dass Daten sowohl auf dem Gerät als auch bei der Übertragung optimal geschützt sind. Alle sicherheitsrelevanten Bereiche der SecurePIM App und dem dazugehörigen Management-Portal hat das deutsche Unternehmen selbst entwickelt und ist deshalb zu 100 Prozent Sicherheit „Made in Germany".

Virtual Solution hat es sich zur Aufgabe gemacht Sicherheit und Benutzerfreundlichkeit zu vereinen. Deshalb orientiert sich SecurePIM in der Handhabung an gewohnten Oberflächen der jeweiligen Systeme (iOS oder Android). Die App ist dadurch einfach zu bedienen und der Benutzer wird bei seiner täglichen Arbeit nicht eingeschränkt – bei maximaler Sicherheit.

Auch Konfiguration und Rollout der App sind ganz einfach. Die Mitarbeiter laden sich die App aus dem App Store oder Google Play runter und loggen sich mit ihren Anmeldeinformationen ein. Die Installation eines MDM Profils ist nicht notwendig, kann aber problemlos integriert werden. Somit passt sich die Lösung an jede bestehende Infrastruktur an – auch wenn sich diese einmal ändert. Das SecurePIM Management Portal sorgt für zusätzliche Flexibilität, da es Administratoren erlaubt ganz einfach Sicherheitsregeln festzulegen. Passwortlänge und Funktionen wie das Verbot von einfachem Kopieren innerhalb der App, können im Portal angepasst werden.

Mit dem integrierten Messenger Modul bietet SecurePIM alles was Sie für sichere, bequeme und schnelle Zusammenarbeit brauchen. Der Vorteil: Sie behalten die volle Kontrolle über Ihre Firmendaten. Egal, ob auf dienstlichen oder privaten Smartphones.

Auf einen Blick: Vorteile des Container-Modells

- ✓ Einfacher Zugriff auf Firmendaten mit Smartphone oder Tablet im gewohnten Look-and-Feel
- ✓ Einfache Konfiguration und Rollout in jeder Infrastruktur
- ✓ Die Daten sind mit modernen Technologien verschlüsselt – im Container auf dem mobilen Gerät und auch bei der Übertragung
- ✓ Für COPE- und für BYOD-Szenarien geeignet
- ✓ Strikte Trennung von geschäftlichen und privaten Daten
- ✓ Vollumfängliche Kontrolle über Unternehmensinformationen, ohne die Privatsphäre der Mitarbeiter zu verletzen

ÜBER VIRTUAL SOLUTION

Virtual Solution entwickelt und vertreibt die Applikation SecurePIM und das Framework SERA (Secure Environment for Reliable Applications) für iOS- und Android-Geräte. SecurePIM ermöglicht Ihren Mitarbeitern den sicheren Zugriff auf E-Mails, Kalender und Dokumente sowie das sichere Chatten und Telefonieren auf Smartphones und Tablets.

Virtual Solution AG
Blutenburgstraße 18
D-80636 München

+49 (0)89 30 90 57-0

kontakt@virtual-solution.com
www.virtual-solution.com