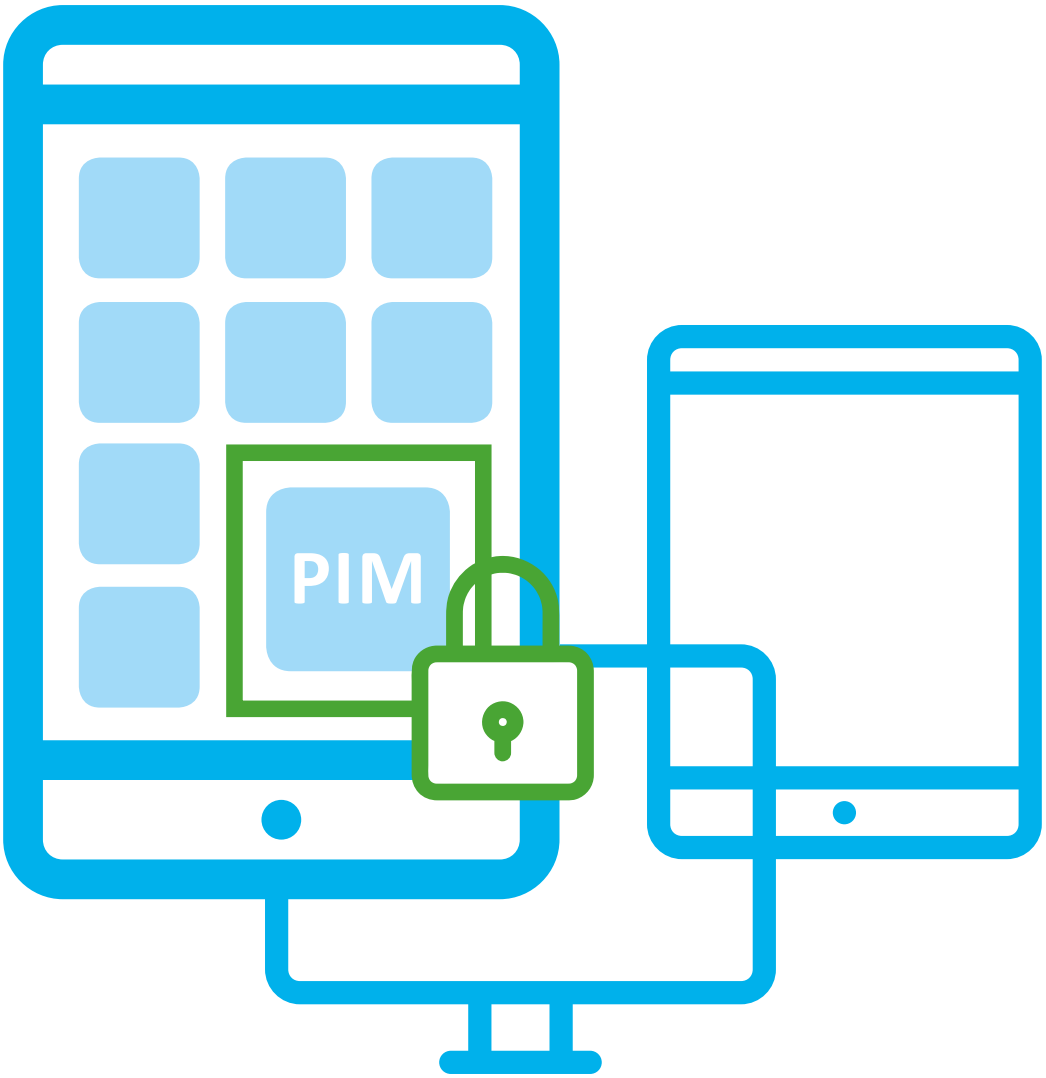
Virtual Solution



DATENSICHERHEIT FÜR SMARTPHONE & CO.

Bestandteile eines Mobile Security Konzeptes

Verlorene oder gestohlene Handys, Sicherheitslücken, Malware, Man-in-the-Middle-Attacken – die Einfallstore für Angriffe auf mobile Geräte und Daten sind vielfältig. Smartphones oder Tablets werden für Hacker immer attraktiver, da sie vermehrt Funktionen für geschäftskritische Prozesse bieten und mit dem Backend des Unternehmens verbunden sind. Mobile Datensicherheit, aber auch Datenschutz auf Smartphones werden vor diesem Hintergrund vitale Aspekte für das Arbeiten mit mobilen Geräten. Dieses White Paper beleuchtet drei grundlegende Sicherheitsstrategien: den Einsatz von im Gerät integrierten Sicherheitsfunktionen, die über das Betriebssystem des mobilen Device zugänglich sind, Systeme für Mobile Device Management (MDM) bzw. eine fortgeschrittene Variante davon und flexible Container mit Verschlüsselung.

Container bestechen durch ihre einfache Einführung, Verwaltung und hohe Nutzerfreundlichkeit, während MDM erweiterte Funktionalität, aber auch wesentlich höhere Aufwände erzeugt. Auf der Betriebssystem-Ebene ist mit MDM nur ein Basis-schutz möglich.

DATENSICHERHEIT FÜR SMARTPHONE & CO.

Bestandteile eines Mobile Security Konzeptes

Mobiles Arbeiten erzeugt neue Herausforderungen für die Informationssicherheit, denn mit der Nutzung mobiler Endgeräte steigen die Risiken, dass Unbefugte Zugriff auf Unternehmensinterna erlangen.

Um das passende Schutzniveau für die Unternehmensinformationen herzustellen, können Unternehmen aus verschiedenen Sicherheitskonzepten wählen. Das gewählte Konzept muss vier Anforderungen erfüllen: Es muss Unternehmensdaten bei der Speicherung auf dem Gerät schützen. Es muss den Transfer der Daten absichern. Er muss die Privatsphäre der Mitarbeiter respektieren und es muss die Vorgaben der EU-DSGVO erfüllen.

Eine Vielzahl von Parametern entscheidet über die Wahl des zum Unternehmen passenden Sicherheitskonzepts. Die wichtigsten Parameter sind Kosten, Realisierungszeiträume, Administrationsaufwände, Flexibilität, Nutzerfreundlichkeit und Funktionsumfang. Darüber hinaus muss die gewählte Lösung auch zu den Ansprüchen und Mobilitätsstrategien des jeweiligen Unternehmens passen.

Mobilität als Business-Faktor

Der mobile Zugriff auf Services hat unsere Gesellschaft in den letzten Jahren fundamental verändert. In Deutschland nutzen aktuellen Studien zufolge 57 Millionen Menschen Smartphones; drei von vier Nutzern (73 Prozent) können sich ein Leben ohne Smartphone nicht mehr vorstellen. Und der Boom ist ungebrochen: Für 2019 erwartet der Bitkom ein anhaltend starkes Wachstum im Markt für Smartphones, Apps, Telekommunikationsdienste und Mobilfunknetze in Deutschland auf 34,3 Milliarden €.[1]

Was im privaten Umfeld bereits etabliert ist, hat längst schon seinen Siegeszug im geschäftlichen Umfeld angetreten: Vom kleinen Handwerksunternehmen bis zum Großkonzern gewinnen Firmen Mehrwerte durch erhöhte Produktivität und Mitarbeitererreichbarkeit. Aber mobiles Arbeiten bedeutet auch, dass sich die Außengrenze des Unternehmens weiter in den öffentlichen Raum verschiebt: Mitarbeiter greifen ortsunabhängig via Smartphone oder Tablet auf Informationen, geschäftliche Anwendungen oder Kundendaten zu. Gleichzeitig verwenden Mitarbeiter ihre Smartphones sowohl privat als auch beruflich, unabhängig von Eigentumsverhältnissen (Unternehmen/Mitarbeiter) oder Nutzungsmodellen (BYOD – bring your own device, COPE – company owned, personally enabled etc).

Laut Unisys[2] nutzen 31 Prozent aller deutschen Arbeitnehmer ihr privates Smartphone für dienstliche Aufgaben, weitere 23 Prozent bekommen ein Smartphone vom Arbeitgeber gestellt. Während die Nutzung von Mobilgeräten, die das Unternehmen zur Verfügung stellt, noch einigermaßen kontrolliert werden kann, sieht das bei privaten Geräten anders aus. So geben 69 Prozent der in der Unisys-Studie Befragten, die ihr privates Smartphone nutzen, an, dass sie Apps und Websites nutzen, die nicht durch ihre Unternehmens-IT autorisiert sind. Der Hauptgrund dafür ist, dass diese Apps und Websites besser sind, d.h. in der Regel eine bessere User Experience bieten, als die vom Unternehmen bereitgestellten Apps.

Mobilität erzeugt neue Sicherheitsherausforderungen

Mobilität bedeutet damit aus Unternehmenssicht nicht nur Flexibilität und Produktivitätsgewinn, sondern stellt auch ein nicht zu unterschätzendes Risiko für das Unternehmen dar. Unabhängig vom Angriffsvektor hat laut Cisco[3] jedes zweite mittelständische Unternehmen bereits einen Datendiebstahl hinnehmen müssen. In dieser Situation sind IT-Verantwortliche gefordert, solide Konzepte für den Schutz von Unternehmensdaten zu entwickeln. Gleichwohl haben die Verantwortlichen erkannt, dass ihre Sicherheitsansätze den Ansprüchen des modernen Arbeitsumfelds entgegenkommen müssen – besonders im Hinblick auf das mobile Arbeiten. 56 Prozent aller Befragten in der Cisco-Studie erachten den Schutz mobiler Devices vor Cyberattacken als herausfordernd.

[1] Smartphone-Markt wächst um 3 Prozent auf 34 Milliarden Euro, Bitkom, 2019; www.bitkom.org/Presse/Presseinformation/Smartphone-Markt-waechst-um-3-Prozent-auf-34-Milliarden-Euro

[2] The New Digital Workplace Divide, Unisys, 2018; www.app5.unisys.com/library/cmsmail/Digital%20Divide/DWD%20Germany%20FINAL_singles.pdf

[3] Small and Mighty – How Small and Midmarket Businesses Can Fortify Their Defense Against Today's Threats, Cisco, 2019; www.cisco.com/c/dam/en/us/products/collateral/security/small-mighty-threat.pdf

DATENSICHERHEIT FÜR SMARTPHONE & CO.

Bestandteile eines Mobile Security Konzeptes

Wesentliche Aspekte eines mobilen Schutzkonzepts

Im Wesentlichen müssen bei der Entwicklung eines mobilen Sicherheitskonzepts vier Aspekte berücksichtigt werden. Die ersten beiden Aspekte adressieren die Technik: Der Schutz der Daten auf dem Gerät und der Schutz der Daten beim Transfer. Als drittes muss der Zugriff auf interne Ressourcen (wie Applikationen, Systeme etc.) gesichert werden. Gleichberechtigt daneben muss das Schutzkonzept die Privatsphäre des Mitarbeiters respektieren und die Einhaltung gesetzlicher Vorschriften gewährleisten.

Viele mobile Sicherheitskonzepte scheitern am Widerstand der Mitarbeiter. Diese pochen zu Recht auf ihre Privatsphäre – und Mitbestimmungsgremien setzen diese Ansprüche wirkungsvoll durch. Zudem steht der Gesetzgeber auf der Seite der Arbeitnehmer: Die aktuelle Rechtsprechung[4] sieht vor, dass beispielsweise E-Mails nur dann vom Arbeitgeber mitgelesen werden dürfen, wenn die private Nutzung des Mail-Postfachs ausdrücklich verboten ist. Und selbst wenn diese Voraussetzung erfüllt ist, dürfen Arbeitgeber ihre Arbeitnehmer nicht dauerhaft überwachen.

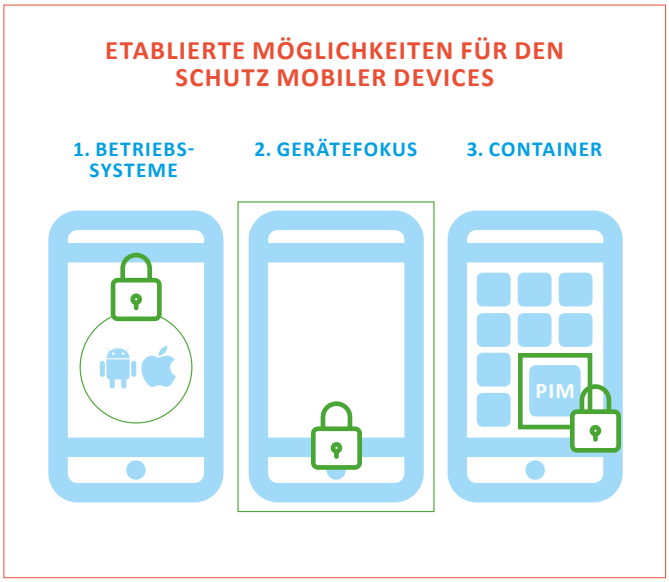
Vier Ziele des mobilen Sicherheitskonzeptes

1. Schutz der Unternehmensdaten
2. Schutz vor Zugriff auf interne Ressourcen
3. Schutz der Privatsphäre der Mitarbeiter
4. Einhaltung der gesetzlichen Vorschriften

Auf der anderen Seite müssen Schutzkonzepte aber auch die Belange von Unternehmen adressieren. Mit der Einführung der EU-DSGVO haben sich die Vorgaben an Firmen in puncto Datenschutz konkretisiert. Beim Abfluss von personenbezogenen Daten haben Organisationen eine Meldepflicht und müssen mit erheblichen Strafzahlungen rechnen. Dabei muss es nicht einmal zu einem konkreten Datenschutz-Vorfall kommen: Sogar das Fehlen eines technisch-organisatorischen Sicherheitskonzepts für Datenschutz und Datensicherheit kann Strafzahlungen nach sich ziehen. Eine einfache Übertragung der Verantwortlichkeit für den Schutz der anvertrauten Daten auf den Mitarbeiter verfängt hier nicht – das Unternehmen bleibt in jedem Fall verantwortlich.

Gängige Schutzkonzepte

Auf dem Markt lassen sich drei grundlegende Ansätze für mobile Sicherheitskonzepte beobachten: Die Nutzung von Betriebssystem-Optionen, der Einsatz zusätzlicher mobiler Managementsysteme und Container. In der Realität werden diese Ansätze auch kombiniert.



[4] E-Mail-Überwachung im Büro – Was darf der Arbeitgeber? RA Axel Pöppel, www.ra-poeppel.de/e-mail-ueberwachung-im-buero-was-darf-der-arbeitgeber/

DATENSICHERHEIT FÜR SMARTPHONE & CO.

Bestandteile eines Mobile Security Konzeptes

Einsatz der Möglichkeiten des Betriebssystems

Am naheliegendsten ist die Nutzung der vom Geräte-Provider bzw. im Betriebssystem (OS) bereitgestellten Security-Features. Das Betriebssystem ggfs. in Verbindung mit zusätzlich Verwaltungsdiensten erlaubt die Einrichtung grundlegender Sicherheitsmechanismen.

Dazu gehören die Einrichtung einer PIN (oder biometrischer Identifikation) für den Zugriff auf das Gerät bzw. Apps sowie die Einhaltung von Richtlinien für komplexe Passwörter und deren regelmäßige Aktualisierung. Auch die Kontrolle der drahtlosen Zugriffe (WLAN, Bluetooth) auf Netzwerke bis hin zur Verschlüsselung von Daten auf dem Gerät lassen sich über Betriebssystem-Funktionalitäten organisieren. Regelmäßige OS-Updates sind ein weiterer Bestandteil dieses Schutzkonzepts.

Apple ist durch seinen Walled-Garden-Ansatz in der Lage, sein iOS strikt zu kontrollieren und regelmäßige OS-Updates zeitnah durchzusetzen. Außerdem unterstützt das Betriebssystem das Kryptografieverfahren AES-256 auf Hardware-Ebene. Das Verfahren erlaubt eine vollständige Storage-Verschlüsselung und eine schnelle Remote-Löschung. Sandboxes limitieren die Zugriffe einzelner Apps auf Daten bzw. andere Apps; die Systempartition mit dem Root-Verzeichnis ist schreibgeschützt, was eine solide Sicherheitsmaßnahme gegen Malware-Angriffe darstellt.

Auch Android bietet einige wichtige Basis-Sicherheitsfunktionen. Doch bei Android erweist sich der Open-Source-Gedanke als Achillesferse: Dadurch, dass Device Provider Anpassungen am Betriebssystem vornehmen, verzögert sich der Rollout von OS-Updates, die von Google zentral bereitgestellt werden. Dies erhöht die Chance auf Zero-Day-Exploits.

Unterschiedliche Betriebssysteme erhöhen die Management-Aufwände

Die Unterschiedlichkeit der Betriebssysteme ist eine der essenziellen Komponenten, die beim Management von mobilen Devices berücksichtigt werden muss. IT-Abteilungen, deren mobile Sicherheitskonzepte auf den Sicherheitsfunktionen der Betriebssysteme beruhen, beschreiten einen lizenzseitig kostengünstigen Weg, der zudem schnell aus eigener Hand realisiert werden kann. Dieser Ansatz eignet sich daher vor allem, wenn Unternehmen einen einheitlichen Standard für mobile Devices verfolgen, beispielweise ausschließlich auf iPhones setzen.

Sollen in einem Unternehmen aber verschiedene Devices genutzt werden, steigt der administrative Aufwand stark an. Eine BYOD-Policy lässt sich nur mit extremem Aufwand umsetzen, da u. a. auch das entsprechende Fachwissen bzgl. der spezifischen Fähigkeiten jedes OS auf aktuellem Niveau gehalten werden muss. Ein ungelöstes Problem bei diesem Ansatz bleibt darüber hinaus der Zugriff öffentlicher Apps (wie WhatsApp) auf die Kontaktliste, die beim geschäftlichen Einsatz des Geräts auch Kontakte von Business-Partnern enthält. Der Abfluss solch personenbezogener Informationen kann in Strafzahlungen nach EU-DSGVO münden.

FAZIT: EINSATZ DES BETRIEBSSYSTEMS

PRO

- ⊕ Kostengünstige Lösung für standardisierten Geräte-Pool

CONTRA

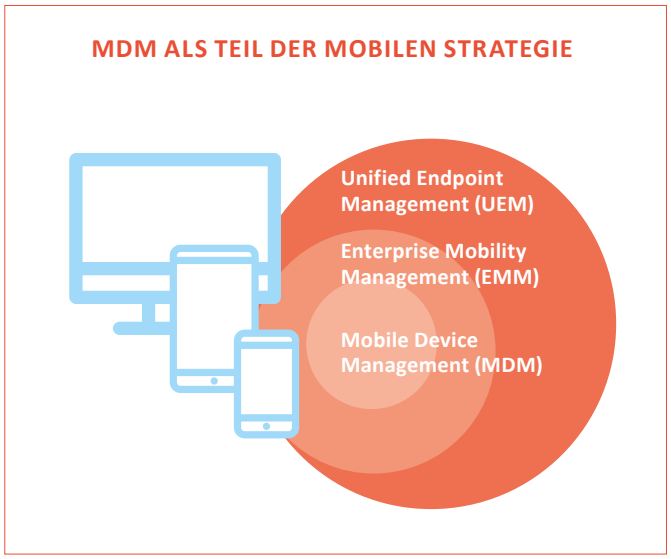
- ⊖ Verzögerte Updates (Gefahr von Zero-Day-Exploits)
- ⊖ BYOD nur mit großem Aufwand umsetzbar
- ⊖ Abfluss personenbezogener Daten durch unsichere, öffentliche Apps möglich (EU-DSGVO-Konflikte)
- ⊖ Kontinuierliche Schulungsaufwände für Admin-Personal

DATENSICHERHEIT FÜR SMARTPHONE & CO.

Bestandteile eines Mobile Security Konzeptes

Nutzung eines MDM/UEM/EMM-Systems

Die Verwaltung von mobilen Endgeräten begann vor Jahren als Mobile Device Management (MDM). Die Bezeichnung illustriert, dass die Maxime dieser Systeme war, im Wesentlichen das Device zu schützen bzw. zu verwalten. Dazu gehörte auch der Schutz der Daten auf dem mobilen Endgerät sowie einige einfache Kontrollen der mobilen Apps. Zu den zentralen Funktionen von MDM-Systemen zählen auch die Durchsetzung von Passwort-Policies, die zentrale Installation von Apps, die Remote-Löschung von (kompletten) Devices und die Konfiguration von Unternehmens-Profilen.



Mit dem Nachfolger, dem Enterprise Mobility Management (EMM), erhielten die IT-Teams verfeinerte und erweiterte Möglichkeiten des Managements – und zugleich die Option, Devices über verschiedene Betriebssysteme hinweg zu managen. EMM ist eine Kombination aus Mobile Device Management, Mobile Application Management und Mobile Content Management. EMM erlaubt das Durchsetzen von Multi-Faktor-Authentifizierung sowie die Einrichtung von Enterprise File Sync und Share. Devices erhielten Browser mit sicherer Konfiguration, die Implementierung von bedingten Zugriffsrichtlinien wurde möglich (entsprechend spezifischer User-Rechte).

Aktuell entwickeln sich EMM-Systeme weiter zu Unified-Endpoint-Management-Systemen (UEM), die in der Lage sind, sowohl mobile Endgeräte als auch Desktop-Systeme zu konfigurieren und zu aktualisieren. Perspektivisch sollen UEM-Systeme auch erlauben, neue Endpunkte im Internet of Things zu verwalten.

Komplette Gerätekontrolle vs. Nutzeransprüche

Die Einführung eines MDM-, EMM- oder UEM-Systems ist ein professioneller Ansatz, um einen „Fuhrpark“ von Devices zu managen. Dieser Ansatz bietet sich vor allem für große Unternehmen und eine Vielzahl von zu verwaltenden Geräten an, denn der Aufwand für den Rollout und die dauerhafte Administration ist beträchtlich. Unabdingbar ist der Einsatz eines solchen Systems für Unternehmen, die eigene Apps auf die mobilen Geräte ausrollen wollen. Die Administratoren erhalten vollen Zugriff auf das Gerät. Der Zugriff geht also über die Business-Daten und -Apps hinaus und deckt auch die private Nutzung des Geräts ab (Device-zentrierter Ansatz). Bei Geräten mit Mischnutzung kann das im Zweifelsfall bedeuten, dass auch private Daten mit einem Remote Swipe gelöscht werden.

Eine weitere Schwachstelle des Konzepts kann sich ergeben, wenn externe Partner/Mitarbeiter in das Management eingebunden werden sollen. Freelancer, die für mehrere Unternehmen einer Branche arbeiten, werden große Vorbehalte für den Einsatz eines MDM auf ihrem Gerät haben, da Administratoren damit Einblick in Daten erhalten könnten, die nicht für ihr Unternehmen bestimmt sind. Ebenso wenig werden Freelancer Interesse daran haben, dass die Inhalte ihres Device ggfs. komplett gelöscht werden.

Neben diesen Defiziten für die Nutzer sollten auch die Aufwände für Installation und dauerhaften Betrieb eines MDM-Systems nicht unterschätzt werden. Diese Aufwände schlagen sich in zusätzlichen Kostenblöcken nieder, die das Unternehmen über die hohen Lizenzkosten hinaus erbringen muss.

DATENSICHERHEIT FÜR SMARTPHONE & CO.

Bestandteile eines Mobile Security Konzeptes

FAZIT: EINSATZ EINES MDM-SYSTEMS

PRO

- ⊕ Umfassende Lösung mit reicher Funktionalität
- ⊕ Ermöglicht eigene AppStores
- ⊕ Durchsetzung von Policies

CONTRA

- ⊖ Hohe Kosten
- ⊖ Komplexität erzeugt hohe Aufwände bei Einführung
- ⊖ Potenzieller Eingriff in Privatsphäre bis hin zur Löschung persönlicher Daten

Container als flexible Lösung für mobile Sicherheit

Eine Alternative oder Ergänzung zu den beschriebenen Konzepten ist der Rückgriff auf eine datenzentrierte Lösung. Im Gegensatz zu einer Device-zentrierten Lösung fokussiert sich der Ansatz ausschließlich auf den Schutz der Unternehmensdaten. Das Konzept erfüllt sowohl Datenschutz-Anforderungen als auch Erwartungen an den Schutz der Privatsphäre. Container ermöglichen sicheres mobiles Arbeiten – unabhängig davon, ob das mobile Device aktiv gemanagt wird oder nicht.

Trennung von Business- und privaten Daten

Beim datenzentrierten Ansatz wird auf dem mobile Device ein remote administrierbarer Container installiert. Damit wird der Business-Teil strikt vom privaten Teil des Geräts getrennt. Ein prominentes Beispiel für den Einsatz von Containern ist Samsungs Knox. Hierbei wird der Container-Einsatz aber auf Geräte eines bestimmten Herstellers limitiert. Wenn Unternehmen Container unabhängig von Endgeräten nutzen wollen, ist ein OS-agnostischer Container-Ansatz der einzig sinnvolle.

Im Container läuft eine Suite von Business Apps für das mobile Arbeiten (für E-Mail, Kalender, Kontakte etc.) separiert von den öffentlichen Apps, wie z. B. WhatsApp. In diesem Container werden auch alle Business-Daten verschlüsselt gespeichert und mittels PIN oder Password zusätzlich geschützt. Damit sind die Informationen vor unbefugtem Zugriff auf dem Endgerät geschützt. Daten werden zudem vor Verlust oder Manipulation geschützt und können nicht unkontrolliert ab- oder einfließen. Das Administrationspersonal des Unternehmens, hat nur Zugriff auf den Inhalt des Containers, nicht auf den Rest des Gerätes.

Container - leistungsfähige Sicherheitslösung für alle Devices

Container lassen sich unabhängig vom Nutzungsmodell des Device einsetzen, also auch wenn private Smartphones und Tablets im Rahmen eines BYOD-Programmes im Unternehmen genutzt werden. Das heißt: Ein Nutzer kann aus dem Unternehmensbereich heraus nicht auf seine privaten Apps zugreifen. So verhindert eine Container-Lösung beispielsweise, dass Firmeninformationen per Copy & Paste auf Facebook oder Twitter landen. Die öffentlichen Apps haben andererseits keinen Zugriff auf die Business-Daten.

Die Container-Lösung lässt sich zudem einsetzen, um „Extended Enterprises“ zu realisieren, in denen externe Mitarbeiter limitierten Zugriff auf Unternehmensinformationen und Systeme erhalten, um eine reibungslose Zusammenarbeit zu unterstützen. Die privaten Informationen oder Daten aus anderen Kundenprojekten, die auf dem Mobilgerät gespeichert sind, verbleiben unter der alleinigen Kontrolle des jeweiligen Besitzers des Endgeräts. Der Betreiber des Containers kann ausschließlich die Inhalte des Containers löschen, nicht die privaten Daten des Nutzers.

Verschlüsselung ist unabdingbar

Ein wichtiges Moment für sicheres mobiles Arbeiten ist eine starke Verschlüsselung – wie diese beispielsweise auch von der EU-DSGVO explizit gefordert wird. Die Verschlüsselung umfasst zwei Aspekte: Zum einen müssen Container selbst performante Sicherheitsmechanismen einsetzen. Dafür haben sich RSA-4096 und AES-256 als Basis durchgesetzt. Zum anderen muss auch der Transport von Daten verschlüsselt werden. Hierbei kommt idealerweise eine Ende-zu-Ende-Verschlüsslung der E-Mails mittels S/MIME zum Einsatz.

DATENSICHERHEIT FÜR SMARTPHONE & CO.

Bestandteile eines Mobile Security Konzeptes

Umfassender Schutz für Unternehmensdaten

Container bieten damit multiplen Schutz für Unternehmensinformationen: Auch im Fall eines Diebstahls hat der Dieb noch keinen Zugriff auf Business-Informationen. Denn diese sind durch eine weitere Schutzebene gesichert: Eine zusätzliche Authentifizierung ist nötig – die üblicherweise mit einer weiteren PIN oder einem Passwort realisiert wird. Bei hohen Sicherheitsansprüchen lässt sich der Zugriff auf den Container auch mittels zusätzlicher Smartcard absichern. Zudem werden die Daten im Container verschlüsselt vorgehalten.

Des Weiteren sind Container ein wirksamer Schutz vor dem Hintergrund einer grassierenden Schatten-IT, die durch mobile Devices gefördert wird. Insbesondere bleibt eine Vielzahl von kriminellen Angriffen auf mobile Devices ohne negative Auswirkungen für das Unternehmen. Die strikte Trennung von Business und privatem Bereich bietet der Malware keine Chance für den Zugriff auf sensible Informationen.

FAZIT: EINSATZ VON CONTAINERN

PRO

- ⊕ Einfach einzuführende Lösung
- ⊕ Kostengünstig
- ⊕ Device-unabhängiger Einsatz
- ⊕ Privatsphäre der Mitarbeiter bleibt geschützt
- ⊕ Durchsetzung von Policies
- ⊕ Erfüllung von internen Datensicherheitsansprüchen
- ⊕ Erfüllung von externen Datenschutzvorgaben (EU-DSGVO)
- ⊕ Einfache Administration
- ⊕ Hohe Usability
- ⊕ Hohes Sicherheitsniveau für Unternehmensdaten

CONTRA

- ⊖ Keine eigenen AppStores
- ⊖ limitiertes Feature-Set

Mobilität braucht nutzerorientierte Sicherheit

Enterprise-Mobility-Konzepte brauchen Sicherheit und Flexibilität. Durch die ständig steigende Business-Dynamik müssen sie sich immer wieder an neue Rahmenbedingungen anpassen. Das gilt nicht nur für unternehmensweite Entwicklungen, sondern auch auf der Ebene der Nutzer bzw. Mitarbeiter. Dementsprechend müssen sich Lösungen für Sicherheit auch an die Bedürfnisse verschiedener Nutzer adaptieren lassen. Mitarbeiter wollen heute mit den neuesten Gerätemodellen arbeiten und am besten mit dem Betriebssystem ihrer Wahl (iOS oder Android). Sicherheit muss aber auch einfach sein – sowohl für den Nutzer als auch für den Betreiber. Komplizierte Konzepte werden sich nicht durchsetzen. Technisch bedeutet das, dass Sicherheitslösungen sich ohne große Projektaufwände in verschiedenste Infrastrukturen integrieren lassen.

Mit der Kombination von Flexibilität und Einfachheit stellen sich Unternehmen in punkto Sicherheit zukunftssicher auf.

Container App: Mobile Sicherheit maximieren mit nur einer Lösung

Ein Höchstmaß an Sicherheit und Flexibilität beim Arbeiten auf mobilen Endgeräten erhalten Unternehmen durch den Einsatz einer Container-App wie SecurePIM. Die App ermöglicht die einfache Realisierung umfassender Sicherheit. Da alle Daten innerhalb von SecurePIM verschlüsselt in einem „Sicherheitscontainer“ abgelegt werden, sind Informationen vor unbefugtem Zugriff auf dem Endgerät geschützt, sowohl unter iOS als auch unter Android. Die Datenübertragung erfolgt ebenfalls verschlüsselt. Daten werden vor Verlust oder Manipulation geschützt und können nicht unkontrolliert ab- oder einfließen. Damit werden auch die Ansprüche der EU-DSGVO erfüllt.

Die Container-App SecurePIM gewährleistet die strikte Trennung von firmeninternen und privaten Daten – sogar dann, wenn private Smartphones und Tablets im Rahmen eines BYOD-Programmes im Unternehmen genutzt werden. Zugleich wird aber auch die Privatsphäre der Mitarbeiter geschützt.

Virtual Solution

DATENSICHERHEIT FÜR SMARTPHONE & CO.

Bestandteile eines Mobile Security Konzeptes

Unternehmen, die bereits MDM-Systeme einsetzen oder in Zukunft einsetzen wollen, können SecurePIM einfach integrieren. Das MDM-System fungiert dann als Management-Portal für SecurePIM.

Alle sicherheitsrelevanten Bereiche der SecurePIM App und dem dazugehörigen Management Portal sind in Deutschland nach deutschen Datenschutzrichtlinien entwickelt worden. SecurePIM ist deshalb zu 100 Prozent Sicherheit „Made in Germany“. Das bestätigt auch die BSI-Zulassung bis VS NfD („Verschlusssache – nur für den Dienstgebrauch“).

Erfahren Sie mehr über SecurePIM!

CHECKLISTE
mobiles Sicherheitskonzept

Bei der Entwicklung eines Konzepts für mobile Sicherheit sollten IT-Verantwortliche folgende Sicherheitsmechanismen berücksichtigen:

- Zentrale Kontrolle über Unternehmensdaten inkl. der Möglichkeit der Fernlöschung
- Strikte Trennung von privaten und geschäftlichen Daten
- Schutz vor Manipulation von Daten und Business-Services
- Jailbreak-Detektion inkl. der Möglichkeit der Zugriffssperrung
- Starke PINs, Passwörter, Touch ID oder Face ID
- Sichere Browser
- State-of-the-Art Verschlüsselung
- Ende-zu-Ende-Verschlüsselung

ÜBER VIRTUAL SOLUTION

Virtual Solution hat es sich zur Aufgabe gemacht, Sicherheit und Benutzerfreundlichkeit in der mobilen Arbeitswelt der Zukunft zu verbinden. Bereits seit 1996 entwickelt und vertreibt das deutsche Unternehmen Sicherheitslösungen, die auf die Sicherheitsbedürfnisse einer zunehmend digitalisierten und mobilen Gesellschaft zugeschnitten sind.

Virtual Solution AG
Blutenburgstraße 18
D-80636 München

+49 (0)89 30 90 57-0

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