SecurePIM
by Virtual Solution

MOBILE SICHERHEIT TROTZ BYOD: **GESCHÄFTSDATEN IN SECURITY-CONTAINERN SCHÜTZEN**

Mitarbeiter bringen das eigene Smartphone mit zur Arbeit, verschicken davon E-Mails mit angehängten Vertragsunterlagen, greifen aus dem Zug auf das Unternehmensnetzwerk zu und haben dabei noch die private Facebook-App geöffnet. Wie gelingt es den IT-Verantwortlichen in einem solchen Szenario Geschäftsdaten, wie zum Beispiel sensible Kundendaten, vor dem Zugriff Dritter zu schützen und dabei keine datenschutzrechtlichen Grenzen zu überschreiten? Vor allem im BYOD-Umfeld ist es mit Mobile Device Management-Lösungen nicht getan. Um Geschäftsdaten auch bei Geräteverlust oder Diebstahl umfassend zu schützen und Mitarbeitern zugleich höchste Usability zu garantieren, bietet sich die Arbeit mit Sicherheitscontainern an – am besten in Form von Apps.

Und hier kommen wir ins Spiel. SecurePIM ist eine Applikation des Herstellers Virtual Solution AG. Eine Mobile App, deren Leistungsmerkmale die geforderten Eigenschaften aufweist. Die Sicherheits-App trägt das Gütesiegel „100 Prozent Security made in Germany“. So arbeitet die Virtual Solution AG beispielweise auch gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) an Lösungen für den Einsatz von mobilen Endgeräten in hochsicheren Einsatzbereichen.

Jedes vierte Unternehmen geht aktuell davon aus, dass der klassische Büroarbeitsplatz mit Anwesenheitspflicht zunehmend an Bedeutung verliert. Das ist das Ergebnis einer aktuellen Befragung unter 1.500 Geschäftsführern und Personalleitern im Auftrag der BITKOM. Mobilität ist längst im Geschäftsalltag angekommen. Sowohl Arbeitnehmer als auch -geber sind von den Vorteilen flexibler Arbeitsplatzmodelle überzeugt. Mitarbeiter profitieren beispielsweise von einer besseren Vereinbarkeit von Beruf und Familie, einer größeren Zeitersparnis und gesteigerter Motivation, weil sie Ort und Zeit ihrer Arbeit frei wählen können. Unternehmen erzielen geringere Bürokosten, eine höhere Arbeitsplatz-Attraktivität sowie verstärkte Produktivität und Effektivität ihrer Mitarbeiter.

Die Arbeitnehmerentwicklung

früher		heute
Geregelte Arbeitszeit (09.00 Uhr - 17.00 Uhr)		**Flexible Arbeitszeiten**
Arbeit im Firmenbüro		**Flexibler Arbeitsplatz**
Aufgaben-orientiert		**Zielorientiert**
Vorgegebene Aufstiegs-möglichkeiten		**Individuelle Aufstiegs-möglichkeiten**
Betriebseigene Geräte nutzen (COD)		**BYOD**

Probleme & Gefahren

Voraussetzung ist der Einsatz mobiler Endgeräte – entweder unternehmenseigener Smartphones und Tablets oder privater Endgeräte der Mitarbeiter, ein Nutzungsmodell, das auch als „Bring Your Own Device“ (BYOD) bekannt ist. Beide Modelle stellen IT-Verantwortliche vor große Herausforderungen, wenn es darum geht, die Kontrolle über die vielen verschiedenen Endgeräte und die darauf gespeicherten Daten zu behalten. Besonders schwierig gestaltet sich in diesem Zusammenhang der Umgang mit sensiblen Kundendaten, die eines besonderen Schutzes bedürfen. Unternehmen, deren Mitarbeiter ihre eigenen Endgeräte nutzen, gehen neben den typischen Risiken, wie Geräteverlust, Diebstahl oder Cyberangriff, noch eine weitere Gefahr ein: Private Apps, wie Whatsapp oder Facebook, lesen nicht selten andere Anwendungen, wie zum Beispiel das Telefonbuch, aus. Das Ergebnis einer Erhebung des Global Privacy Enforcement Network (GPEN) aus dem vergangenen Jahr ist erschreckend: 75 Prozent aller Apps greifen auf mindestens eine sensible Gerätefunktion zu.

Doch geschäftliche Dokumente, berufliche E-Mails, Termine sowie Businesskontakte müssen nicht nur aus Datenschutzgründen, sondern häufig auch aus Compliance-Gründen strikt von privaten Daten getrennt werden. Diese hochsensiblen und unternehmensrelevanten Daten liegen bei der Sicherheits-App SecurePIM in einem vollkommen undurchdringlichen Container. Dieser Sicherheitscontainer stellt sowohl auf Android- als auch auf iOS-Geräten die notwendige Sicherheit her und erfährt zugleich eine hohe Akzeptanz durch eine äußerst benutzerfreundliche Bedienung. Vergessen Sie die Ansicht, dass Security und Usability einander ausschließen.

MDM-Lösungen stoßen im BYOD-Umfeld an ihre Grenzen

Oft sind den Unternehmen jedoch juristisch die Hände gebunden, wenn es darum geht, Daten auf privaten Endgeräten zu schützen. Ein mitgebrachtes Gerät bleibt Eigentum des Mitarbeiters. Wenn sich der Arbeitgeber Zugriff verschaffen will, muss er dafür die entsprechende Rechtsgrundlage schaffen. Damit ergeben sich für IT-Administratoren eine Reihe von Fragen: Wie kann ich den Verlust unternehmensinterner Daten verhindern? Und wie können private und geschäftliche Daten voneinander getrennt werden, ohne dass die IT-Datenschutzregelungen verletzt werden?

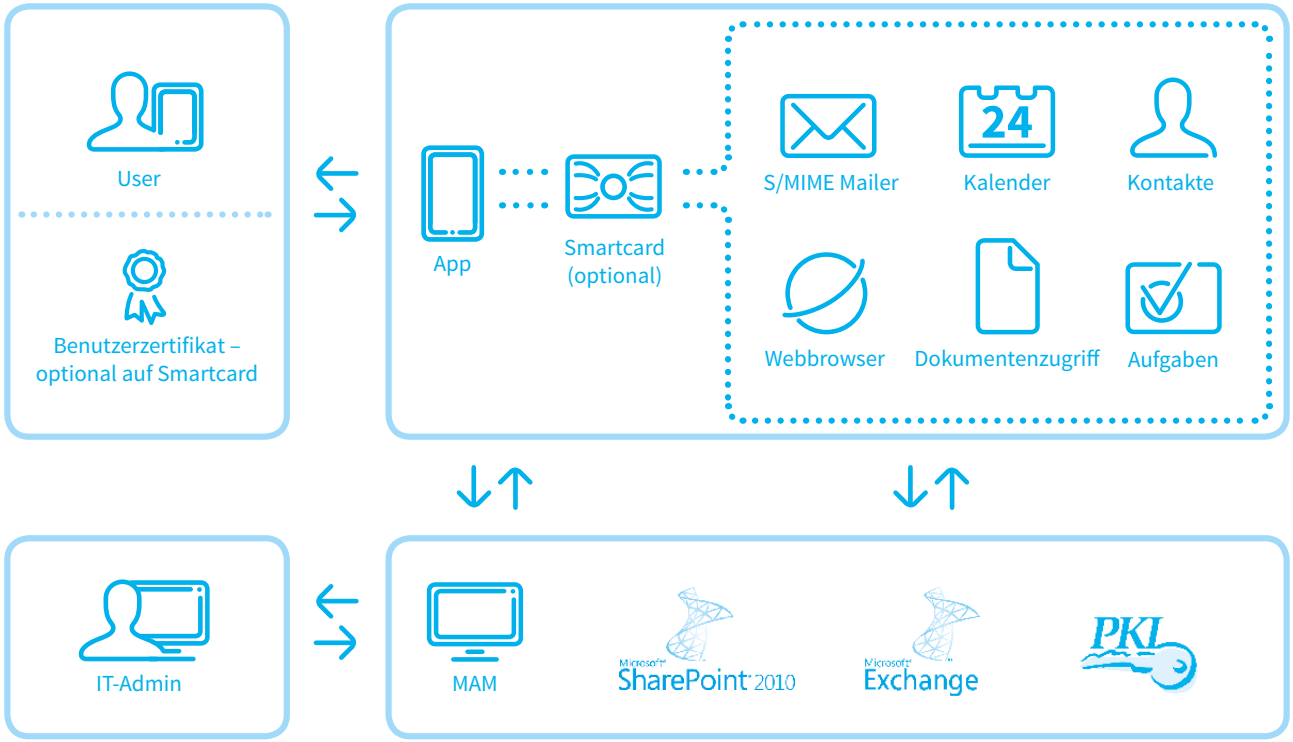
Vielen Unternehmen fehlt es an entsprechenden Lösungen für mobile Sicherheit. Das zeigt auch die aktuelle IDC-Studie „Enterprise Mobility in Deutschland 2014/2015“. Der Studie zufolge setzen derzeit gerade einmal 57 Prozent aller deutschen Unternehmen, die sich in irgendeiner Art und Weise mit dem Thema Enterprise Mobility beschäftigen, tatsächlich eine MDM-Lösung (Mobile Device Management) ein. MDM-Lösungen dienen in erster Linie der zentralen Verwaltung der mobilen Geräte. Sie bilden ab, welcher Benutzer welches Gerät mit welcher Softwareversion und welchen Apps verwendet. So können mithilfe eines solchen Systems an zentraler Stelle bestimmte Geräteeinstellungen vorgenommen werden. Allerdings gilt es zu beachten, dass MDM-Systeme nur die Funktionen verwalten können, die vom Gerätehersteller vorgesehen sind. Das heißt: Das Sicherheitsniveau lässt sich nicht beliebig steigern. Hinzu kommt, dass MDM-Lösungen im BYOD-Umfeld aufgrund der rechtlichen Rahmenbedingungen ohnehin ausscheiden, denn private Endgeräte dürfen nicht vom Unternehmen verwaltet werden.

Geschäftsdaten in der App:
Unternehmen setzen auf abgetrennte Sicherheitscontainer

Um diese Nachteile klassischer MDM-Systeme zu umgehen, setzen Unternehmen heutzutage auf sogenannte Sicherheitscontainer. Auf dem jeweiligen Endgerät wird ein abgetrennter Bereich eingerichtet, in dem die Unternehmensdaten den Richtlinien entsprechend verwaltet und vor allem geschützt werden. Die Kontrolle für diesen Bereich hat die Unternehmens-IT. Um den Wechsel zwischen dem geschäftlichen und dem privaten Bereich für den Anwender so einfach wie möglich zu gestalten, bietet sich der Einsatz von Sicherheits-Apps an, in denen alle geschäftlichen Dokumente, E-Mails, Kontakte und Termine vereint sind. Damit sind auch hochsensible Firmendaten, Tasks und der Web-Browser vor dem Zugriff Dritter geschützt und Mitarbeiter können ohne Sicherheitsrisiko beispielsweise auf die interne CRM-Lösung ihres Unternehmens zugreifen.

Diese Sicherheits-Apps ermöglichen darüber hinaus skalierbare Security-Stufen. Die zur Autorisierung des Benutzers erforderlichen Maßnahmen können von den Unternehmen selbst festgelegt werden, dabei kann es sich zum Beispiel um Passwörter handeln, die gewisse Anforderungen erfüllen müssen, oder um Smartcards, welche die höchste Sicherheitsstufe garantieren. Durch eine solche externe Authentifizierungskomponente sind Unternehmensdaten auch sicher, wenn das Gerät verloren geht oder gestohlen wird, denn ohne sie ist kein Zugriff auf den Sicherheitscontainer möglich. Zudem lassen sich eine solche App und die darin gespeicherten Daten auch per Fernzugriff schnell und einfach löschen. Professionelle App-Lösungen gehen noch einen Schritt weiter und verschlüsseln automatisch alle Daten, die mit der App verschickt oder empfangen und in diesem Bereich abgelegt werden. Im Zuge der Datenübertragung werden zudem CRL-Checks durchgeführt, bei mangelnder Gültigkeit der Zertifikate wird der Zugriff gesperrt.

Systemarchitektur



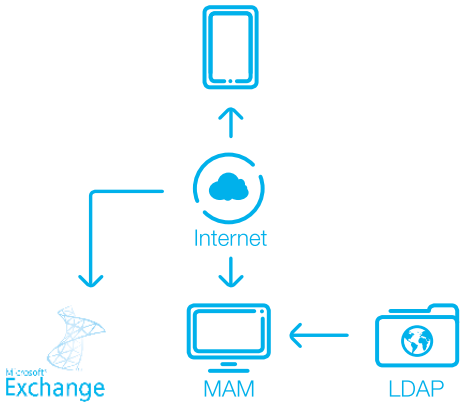
Worauf sollten Unternehmen bei der Auswahl einer Lösung für mobile Sicherheit achten?

Hinsichtlich der Entscheidung für eine konkrete Sicherheitslösung sollten die Verantwortlichen folgende sechs Kriterien beachten:

+ **Usability:** Die beste Lösung nützt nichts, wenn sie von den Anwendern nicht eingesetzt wird. Um die Mitarbeiterakzeptanz zu steigern, sollten die Verantwortlichen eine App wählen, die bedienerfreundlich ist. Am besten entscheidet man sich für Anwendungen die über ein iOS bzw. Android-typisches User interface (UI) verfügen, das bereits aus dem privaten Umfeld der Nutzer gelernt ist. Mit SecurePIM stehen Ihnen alle Business-Funktionen in nur einer App zur Verfügung. Greifen Sie zentral auf Firmen-E-Mails, Kontakte, Termine und Dokumente zu, ohne die App wechseln zu müssen.

+ **Integration:** Wichtig ist, dass sich die Sicherheitslösung nahtlos in die bestehende Public-Key-Infrastruktur (PKI) des Unternehmens integrieren lässt. Schlüssel, Kennwörter etc. können weiterhin verwendet werden, was den Administrationsaufwand bei der Einführung erheblich reduziert. SecurePIM kann einfach, schnell und nahtlos in die IT-Landschaft Ihres Unternehmens integriert werden.

Integration



+ **Server-Lösung:** Außerdem sollte es sich bei einer Lösung für mobile Sicherheit immer um eine Server-Lösung handeln. Im Gegensatz zur Cloud-Alternative bleiben die Daten Eigentum des Unternehmens. Im Ernstfall lassen sich alle Unternehmensdaten, die in SecurePIM abgelegt sind, unverzüglich sperren. Die privaten Daten des Geräts bleiben davon unberührt.

+ **Made in Germany:** Bei der Zusammenarbeit mit einem Dienstleister sollten die Verantwortlichen sicherstellen, dass dieser keine Daten im amerikanischen Raum speichert. Die Server sollten in deutschen Rechenzentren stehen, wodurch auch die deutschen Datenschutzrichtlinien gelten. Die SecurePIM App ist eine Entwicklung des deutschen Softwareunternehmens Virtual Solution AG. Sämtliche sicherheitsrelevante Bereiche der App und des zugehörigen Management-Portals sind exklusiv vom Hersteller in Eigenentwicklung erstellt und damit zu 100 Prozent „Security made in Germany“.

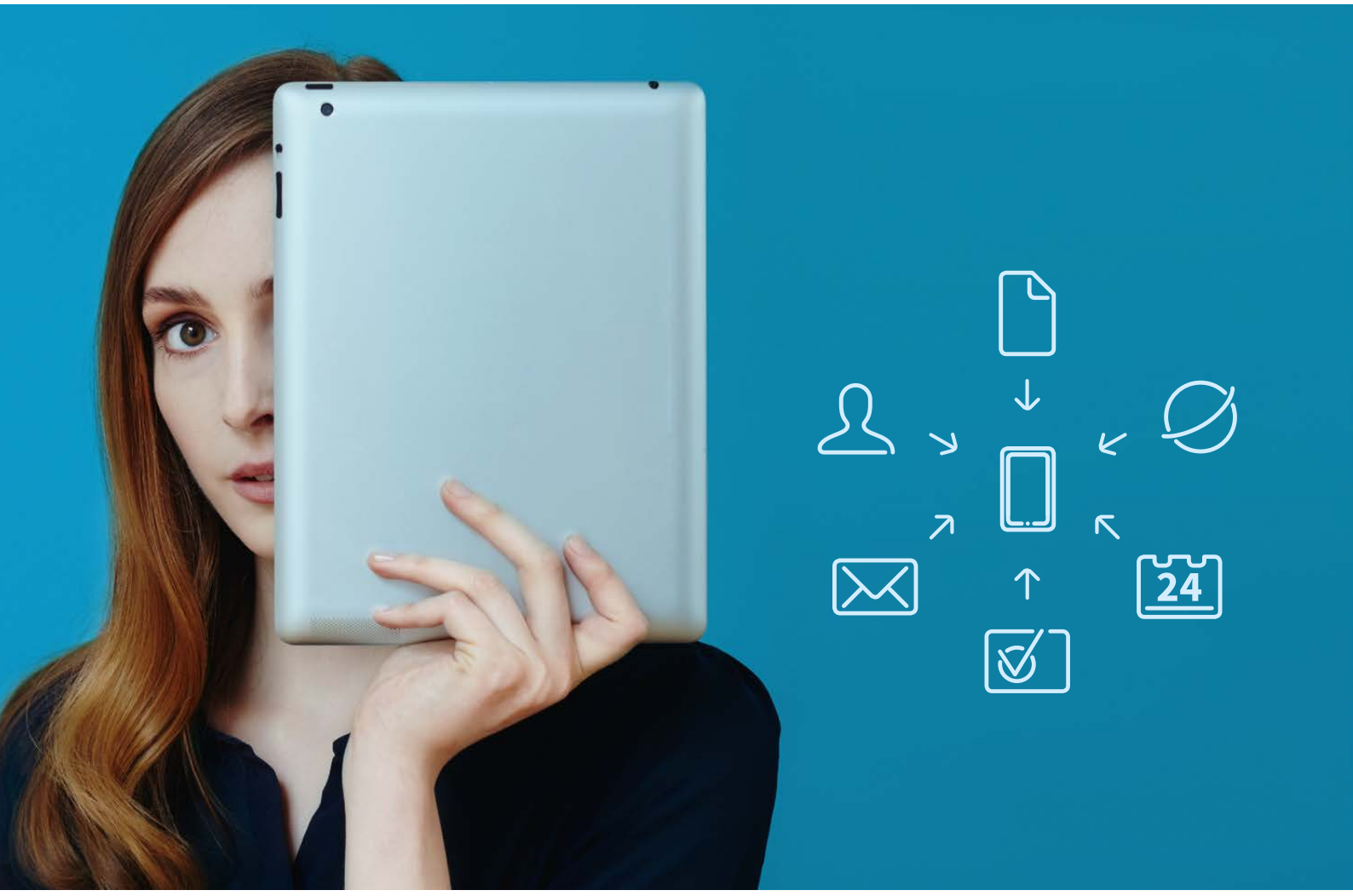
+ **Skalierbare Security:** Wer sich für die Nutzung einer Sicherheitslösung entscheidet, sollte sich nicht an die Gerätefunktionalität binden, sondern herstellerunabhängig verschiedene Sicherheitsstufen und Sicherheitsverfahren wählen können. Je nach Anforderung lässt sich das das Sicherheitslevel von SecurePIM anpassen. TLS-Authentifizierung, Containerverschlüsselung und S/MIME-Verschlüsselung können wahlweise über Smartcard oder Benutzerzertifikat erfolgen. Auf den Mobilgeräten gespeicherte Daten werden dabei immer mit EINEM mindestens 2096 Bit langen Schlüssel chiffriert.

+ **Zentrale Verwaltung:** Um den Administrationsaufwand weiterhin zu reduzieren, sollte die Verwaltung und Konfiguration der Sicherheitslösung zentral über ein Mobile-Application-Management-Portal möglich sein. Das Mobile-Application-Management-Portal ist zentraler Bestandteil von SecurePIM. Damit konfiguriert und verwaltet Ihre IT-Abteilung zentral die SecurePIM App auf allen mobilen Geräten jedes einzelnen Benutzers.

Fazit

Fest steht: Die Grenzen zwischen privater und geschäftlicher Nutzung mobiler Geräte schwinden. Mit ein und demselben Gerät greifen Mitarbeiter auf ihre Facebook-App zu und verschicken sensible Unternehmensdaten per E-Mail. Für IT-Administratoren wird es immer schwieriger, die Kontrolle zu behalten und Compliance-Richtlinien einzuhalten ohne gegen geltende Datenschutzbestimmungen zu verstoßen. Der Einsatz von Sicherheits-containern macht es möglich, geschäftliche und private Daten strikt voneinander zu trennen. Damit können IT-Verantwortliche die erforderlichen Autorisierungsmechanismen für den Zugriff auf den isolierten Unternehmenscontainer festlegen und die vorgeschriebenen Richtlinien für diesen Bereich durchsetzen. So sind Geschäftsdaten auch geschützt, wenn Endgeräte verloren gehen oder gestohlen werden. Eine professionelle Gesamtlösung bietet darüber hinaus die Möglichkeit, die Verwaltung und Konfiguration der App über ein zentrales Portal vorzunehmen. Das Ergebnis: Die IT-Verantwortlichen können sich auf ihre eigentlichen Aufgaben konzentrieren und Innovationen vorantreiben, die direkten Einfluss auf den Geschäftserfolg haben.

Besuchen Sie uns unter:
www.securepim.com



Virtual Solution AG
Vorstand: Andreas Eder, Dr. Raoul-Thomas Herborg
Aufsichtsratsvorsitzender: Dr. Boris Mariacher
Amtsgericht München HRB 202166, USt.-ID DE813833087

Blutenburgstraße 18
80636 München

T +49 – 89 – 30 90 57-0
F +49 – 89 – 30 90 57-200

mail@securepim.com
www.securepim.com

Kooperation

Allianz für Cyber-Sicherheit

SecurITy made in Germany