SecurePIM
by virtual solution

MOBILE SECURITY
IN IHREM UNTERNEHMEN

Version 1.2
Stand: 19.12.14

INHALT

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

1. MOBILE SECURITY – AUCH IN IHREM UNTERNEHMEN

Immer häufiger werden mobile Endgeräte im Unternehmensumfeld eingesetzt. Der Grund ist naheliegend: Die Anwender wollen auch bei ihrer täglichen Arbeit nicht mehr auf die Vorteile verzichten, die ihnen Smartphones und Tablets bieten. Ein erfreulicher Trend, denn das Unternehmen profitiert nicht nur von einer besseren Vernetzung etwa des Außendienstes, sondern auch ganz allgemein durch Effizienzgewinne und eine höhere Mitarbeitermotivation. Erfreulicher Nebeneffekt ist eine deutlich bessere Erreichbarkeit der Mitarbeiter.

Diese Flexibilisierung der Arbeitswelt bringt es allerdings mit sich, dass berufliche Informationen und Anwendungen, die in der Vergangenheit nur am Arbeitsplatz oder an speziell abgesicherten Laptops verfügbar waren, zunehmend auf Geräten genutzt werden, deren Design und Software ursprünglich für einen Consumer-Markt konzipiert wurde. Nicht selten ist es möglich, über die mitgebrachten Smartphones Zugriff auf sensibelste Unternehmensdaten oder gar auf interne Unternehmensnetze zu erlangen.

Spätestens seit immer mehr Details aus der NSA-Affäre bekannt werden, muss jedem Beteiligtem zudem gegenwärtig sein, dass vorhandene Schwachstellen nicht nur ein potentielles Sicherheitsrisiko darstellen, sondern mit einer sehr großen Wahrscheinlichkeit auch tatsächlich in der Praxis genutzt werden. Es handelt sich um eine gerne verdrängte Tatsache, dass heute praktisch jede elektronische Kommunikation mitgelesen, ausgewertet und analysiert wird, der interessierte Dienste habhaft werden. Jede einzelne E-Mail, jede einzelne Nachricht, die wir privat oder beruflich versenden, wird mitgelesen. Jedes Telefonat, das wir führen, wird mitgehört. Die Leistungsfähigkeit der eingesetzten Server und Datenbanken ist heute so hoch, dass sogar die massenhafte Sammlung und systematische Auswertung solch enormer Datenmengen problemlos und nahezu in Echtzeit möglich ist.

Aber damit nicht genug. Angelockt von den enormen Renditen im Bereich der Industriespionage versuchen weltweit tausende kriminelle Angreifer Zugriff auf Unternehmensinformationen zu erhalten. Dank ausführlicher Dokumentationen und Software-Baukästen aus dem Web sinken die Einstiegshürden in dieses kriminelle Gewerbe zudem kontinuierlich. Auch kleinere Ziele werden dadurch zu einem lukrativen Ziel für Industriespionage.

WUSSTEN SIE EIGENTLICH, DASS …

+ … innerhalb von sechs Monaten 55.000 Mobiltelefone in Londoner Taxis verloren wurden?
+ … die Messaging-Anwendung WhatsApp alle Kontakte, die auf Ihrem Mobilgerät gespeichert sind, automatisch auf einen Server im Ausland kopiert?
+ … der deutsche Bundesnachrichtendienst einer der ganz wenigen Auslands-Geheimdienste weltweit ist, der keinen klaren Auftrag zur Förderung der einheimischen Wirtschaft hat?
+ … eine E-Mail auf dem Weg zum Empfänger im Klartext über Dutzende unbekannter Server läuft und für jeden Administrator einsehbar ist?
+ … die iOS KeyChain, die zentrale Stelle zur Speicherung von Zertifikaten und Passwörtern auf Apple-Geräten, nach einer Untersuchung des Frauenhofer Instituts nicht sicher ist?
+ … der Zugang in Ihre Firma vermutlich sorgfältig abgesichert ist, während es mit jedem Smartphone Ihrer Mitarbeiter ebenfalls möglich ist, in Ihr Unternehmen einzudringen? Das bedeutet, dass hunderte potentieller Unternehmenszugänge ganz leicht in die Hände Dritter gelangen können.

Während auf der einen Seite das Gefühl einer diffusen Unsicherheit wächst, herrscht auf der anderen Seite eine große Unklarheit über das richtige Vorgehen. Dieses Whitepaper will die wichtigsten Fragen zum Thema beantworten und darüber aufklären, welche neuen Gefahrenquellen sich durch den Einsatz mobiler Endgeräte ergeben, welche Angriffsszenarien realistisch sind und wie sich Unternehmen effektiv schützen.

Fünf typische Aussagen, die Sie bestimmt schon gehört haben, aber keinesfalls glauben sollten:

1.1 „Das betrifft nur Großunternehmen“

Eine weit verbreitete Einstellung lautet: Sicherheitsrisiken stellen nur in der Theorie eine Bedrohung dar. In der Realität bestätigt sich diese Meinung fatalerweise oft sogar recht lange – bis eben doch etwas passiert. Diese Haltung führt dazu, dass in vielen Unternehmen Sicherheitsprobleme sogar bekannt sind, es sich aber immer wieder Ausflüchte finden, warum die Lücken nicht – oder zumindest nicht jetzt – beseitigt werden muss. Unnötig zu erwähnen, welche schwerwiegenden Folgen sich aus dieser Fahrlässigkeit ergeben können. Die Liste fataler Fehleinschätzungen ist lang und reicht vom schwäbischen Mittelständler, der sein innovatives Produkt auf einer Messe beim asiatischen Hersteller zum halben Preis entdeckt, über die vom Wettbewerber gewonnene Ausschreibung, bei der die gleiche Idee einige Prozent günstiger angeboten wurden, bis hin zu Fällen gezielten Datendiebstahls, die Unternehmen in existenzielle Krisen gestürzt haben. Da die betroffenen Unternehmen meist schweigen, werden nur die seltensten Fälle bekannt.

1.2 „Wir blockieren die Nutzung von Smartphones und Tablets“

Auf diese Aussage sollten Sie sich niemals verlassen. Denn egal ob die Nutzung privater Mobilgeräte mit technischen oder organisatorischen Maßnahmen unterbunden werden: Ihre Mitarbeiter werden Mittel und Wege finden, die Blockade zu umgehen. Etwa indem sie die wichtige Mail an ihr privates E-Mail-Konto senden oder – noch schlimmer – den Vertrag, den sie auf dem Heimweg in der Bahn noch prüfen wollen, in der Dropbox ablegen. Deswegen sollten sich alle Unternehmen mit dem Thema „Mobile Security“ auseinandersetzen. Die Option, es zu unterlassen, bietet sich nicht. Ihre Mitarbeiter werden ihre Mobilgeräte im Unternehmen einsetzen, egal ob Sie darauf vorbereitet sind oder nicht. „Bring your Own Device“ ist keine Unternehmensstrategie, die Sie nach belieben einführen können, sondern ein Trend, dem sich Ihr Unternehmen stellen muss.

1.3 „Das neue iPhone hat jetzt einen Fingerabdruck-Scanner“

Richtig. Und dieser gaukelt zusätzliche Sicherheit vor. Tatsächlich ist das Sicherheitsniveau eines Fingerabdruck-Scanner aber geringer, als das des PIN-Verfahrens. Genau genommen hat Apple das Verfahren nur eingeführt, um ein gewisses Minimum an Sicherheit für die zahlreichen Nutzer zu bieten, die das PIN-Verfahren aus Bequemlichkeit gar nicht nutzen. Wie leicht sich das System mit künstlich erstellten Fingerprints überlisten lässt, demonstrierte der Chaos Computer Club (CCC) bereits wenige Tage nach Erscheinen des iPhone 5S. Hinzu kommen die grundsätzlichen Probleme biometrischer Verfahren: Eine PIN kann geändert, eine Smartcard getauscht, ein Zertifikat für ungültig erklärt werden – der Fingerabdruck ist jedoch unveränderlich, leicht zu „stehlen“ und zu kopieren. Ist ein Angreifer erst einmal in Besitz eines Abdrucks, kann er die Identität uneingeschränkt und unwiderruflich nutzen.

Mit Ausnahme von Blackberry sind alle gängigen Mobilgeräte für den Endanwender gemacht. Die eingebauten Sicherheitsmaßnahmen wurden nie dafür entwickelt, um sensible Unternehmensdaten in aller Welt umherzutragen.

1.4 „Verschlüsselung ist kompliziert und wenig alltagstauglich“

Richtig ist, dass Datensicherheit nur durch eine Kombination von verschiedenen Maßnahmen erreicht werden kann. Ein wichtiger Baustein ist die Verschlüsselung von Daten. Es stimmt auch, dass die Einführung von (beispielsweise) E-Mail-Verschlüsselung einen gewissen initialen technischen und organisatorischen Aufwand erfordert. Richtig ist aber auch, dass die anschließende Nutzung im Alltag völlig unkompliziert im Hintergrund abläuft.

1.5 „Die anderen machen es genauso“

Datensicherheit muss individuell bewertet werden. Auch in Ihrem Unternehmen kann es Bereiche geben, in denen die Bordmittel aktueller Smartphones eine ausreichende Sicherheit bieten. Es kann aber auch sein, dass das eine verlorene Handy eines bestimmten Kollegen für die Firma eine Katastrophe bedeuten würde. Aus diesem Grunde lassen sich die verschiedenen Vorgehensweisen nicht über einen Kamm scheren. Standardvorgehensweisen für die geschäftliche Nutzung mobiler Endgeräte und die zugehörigen Werkzeuge sind gerade im Entstehen.

2. RISIKEN
GANZ KONKRET

Bezüglich des Einsatzes mobiler Endgeräte in Unternehmen besteht eine ganze Reihe technischer Herausforderungen. Der IT-Grundschutzkatalog des Bundesamtes für Sicherheit in der Informationstechnologie (BSI) bietet eine umfassende Strukturierung möglicher Bedrohungen im IT-Umfeld. Aus unternehmerischer Sicht sind bei mobilen Endgeräten insbesondere die folgenden Themenbereiche relevant:

2.1 Verlust von sensiblen Unternehmensdaten

Smartphones werden unterwegs genutzt und gehen leicht verloren. Bei einem Laptop ist das Verlustrisiko dagegen allein aufgrund seines Formfaktors deutlich geringer, bei einem Arbeitsplatzrechner nahe Null. Unternehmen müssen daher davon ausgehen, dass die mobilen Geräte der Mitarbeiter früher oder später in die Hände von Dritten gelangen. Eine informelle Umfrage unter Mitarbeitern, wer schon einmal ein Handy verloren hat, fördert meist erschreckendes zutage. Übrigens: Es reicht schon aus, dass das Mobilgerät 20 Minuten in fremde Händen gerät, um den kompletten Inhalt von dem Gerät zu laden. Der Mitarbeiter merkt bei einem gezielten Angriff nicht einmal etwas davon.

2.2 Gezielte Wirtschaftsspionage

Das BSI listet in seinem Grundschutzkatalog aktuell 162 „vorsätzliche Handlungen“, mit denen sich IT-Systeme kompromittieren lassen. Vielen Unternehmen scheint dieses Gefahrenpotential zunächst wenig praxisrelevant. Spätestens seit PRISM, Tempora & Co. wissen wir jedoch, dass diese Techniken tatsächlich ganz konkret angewendet werden, um jeden Tag Millionen von Nachrichten mitzulesen. Jedes Unternehmen, das interessante Produkte und Dienstleistungen am Markt anbietet, muss davon ausgehen, dass Dritte versuchen, auf relevante Informationen zuzugreifen.

Der deutsche Verfassungschutz warnt inzwischen vor einer massiven Zunahme von Angriffen und nennt in seiner Broschüre „Wirtschaftspionage – Risiko für Unternehmen, Wissenschaft und Forschung“ zahlreiche konkreten Angriffsszenarien.

2.3 Einhaltung rechtlicher Rahmenbedingungen

Daneben stoßen Unternehmen aber auch auf rechtliche Probleme. Auf den meisten Geräten der Mitarbeiter befinden sich eine Mischung aus privaten Daten, Firmendaten und Daten der Kunden. Zunächst besteht ein rein wirtschaftliches Interesse des Unternehmens, seine Firmendaten zu schützen. Zugleich muss das Unternehmen aber auch eine ganze Reihe rechtlicher Rahmenbedingungen zum Datenschutz beachten, die unabhängig davon gelten, ob sich die Daten im Unternehmensnetz oder auf einem mobilen Gerät befinden.

Am sensibelsten ist dabei der Umgang mit personenbezogenen Daten. Rechtlich steht das Unternehmen in der Verantwortung, wenn ein Mitarbeiter mit Einverständnis des Unternehmens ein Gerät geschäftlich nutzt und dabei private Daten des Mitarbeiters oder Daten von Kunden in die Hände Dritter gelangen.

Noch schwieriger wird die juristische Bewertung in einem sogenannten „Bring Your Own Device“-Umfeld. Ein mitgebrachtes Gerät bleibt Eigentum des Mitarbeiters. Wenn sich ein Arbeitgeber Zugriff darauf verschaffen will, muss er dafür eine Rechtsgrundlage schaffen. Tut er dies nicht, könnte das als Verletzung der Vertraulichkeit des Wortes (StGB §§ 201), Verletzung des höchstpersönlichen Lebensbereichs durch Bilddaten (§ 201a StGB), die Verletzung des Briefgeheimnisses (§ 202 StGB), das Ausspähen und/oder Abfangen von Daten (§ 202 a und b StGB) und das Verletzen des Post- oder Fernmeldegeheimnis (§ 206 StGB) sowie gegen die informationelle Selbstbestimmung des Mitarbeiters (leitet sich direkt aus dem Grundgesetz ab) gewertet werden.

Das Unternehmen hat dafür Sorge zu tragen, dass eine Verletzung dieser Bestimmungen nicht erfolgen kann und muss alle technischen und organisatorischen Vorrausetzungen dafür schaffen. Kommt es dieser Pflicht nicht nach, kann dem Unternehmen grob fahrlässiges oder sogar vorsätzliches Verhalten vorgehalten werden. In dem Fall müssen das Unternehmen und unter Umständen auch die Organvertreter persönlich mit Schadensersatzforderungen beziehungsweise auch mit Gefängnisstrafen rechnen. Der Schaden für den Ruf und die Reputation kommt dann noch dazu.

Das Unternehmen muss Verfahren definieren, um die persönlichen Daten des Mitarbeiters zu schützen. Das schließt – und an dieser Stelle wird es besonders schwierig – auch den vorsätzlichen Missbrauch durch einzelne Mitarbeiter ein. Das Unternehmen muss sicherstellt, dass sich auch die IT-Mitarbeiter, die für die Sicherheit im Unternehmen zuständig sind, keinen unbefugten Zugriff auf die persönlichen Daten der Mitarbeiter verschaffen können, wenn sie an einem mitgebrachten Gerät arbeiten.

3. TECHNISCHE HERAUSFORDERUNGEN

Schon diese Übersicht der zu berücksichtigenden Rahmenbedingungen macht deutlich, dass ein unstrukturiertes Vorgehen keinen Erfolg bringen wird. Aus den oben beschriebenen Risikoszenarien lassen sich aber auch einige konkrete technische Anforderungen ableiten, mit denen sich die Bedingungen erfüllen lassen. Diese Herausforderungen sind:

3.1 Nur autorisierter Zugriff

Ein wesentlicher Baustein für die Datensicherheit ist eine eindeutige Identifizierung des Benutzers. Es muss jederzeit feststellbar sein, wer auf bestimmte Informationen und Anwendungen zugreift. Diese sogenannte Authentifizierung erfolgt bei den meisten Geräten über eine PIN, die bei der Aktivierung des Geräts eingegeben wird.

Kennt ein Angreifer diese PIN, hat er vollen Zugriff auf das System. Ein vierstelliger iPhone-PIN kann mit einem aktuellen MacBook in weniger als 20 Minuten identifiziert und damit voller Zugriff auf das Gerät erlangt werden. Dabei wird am Telefon selbst nichts verändert (Stichwort „Jailbreak“), der Einbruch beziehungsweise der Datendiebstahl ist für den Besitzer des Gerätes nicht einmal nachvollziehbar.

Weitere Maßnahmen moderner Smartphones, wie etwa Gesichtserkennung oder Fingerabdruckscanner bieten keine zusätzliche Sicherheit. Typischerweise dienen diese eher als minimale Schutz für Benutzer, denen selbst eine kurze PIN-Eingabe zu aufwendig ist und die ihr Gerät ohne jede Authentifizierung einsetzen.

3.2 Sicherheit der Daten

Die auf dem Gerät lokal vorhanden Daten müssen vor unbefugtem Zugriff geschützt sein. Dies gilt unabhängig davon, ob ein zufälliger Finder oder ein Dieb physikalisch Zugriff auf das Gerät hat oder ein Angreifer auf anderem Wege, etwa mittels einer manipulierten App, versucht Daten zu kompromittieren.

Die bestehenden Sicherheitsmaßnahmen stellen nur einen begrenzten Schutz dar. Die Verschlüsselung auf Apple-Geräten („NSFileProtection“), die seit iOS6 existiert und seit iOS7 standardmäßig aktiviert ist, basiert auf der persönlichen PIN des Benutzers.

Dabei ist zu beachten, dass die zentralen Schlüssel und Zertifikate in der sogenannten iOS KeyChain gespeichert werden. Diese weist jedoch erhebliche Sicherheitsmängel auf, wie das Fraunhofer Institut eindrucksvoll nachgewiesen hat (siehe iOS Keychain Weakness FAQ von Jens Heider und Rachid El Khayari – http://sit.sit.fraunhofer.de/studies/en/sc-iphone-passwords-faq.pdf).

3.3 Sichere Kommunikation

Mobile Endgeräte dienen in allererster Linie der Kommunikation. Von der einfachen Sprachkommunikation über den Versand von E-Mails an Kollegen und Geschäftspartner bis zum Zugriff auf interne Systeme im Unternehmen. Neben den lokal vorhandenen Daten muss daher auch die Kommunikation abgesichert werden, sowohl um die übertragenen Daten zu schützen, als auch um sicherzustellen, dass ein kompromittierter mobiler Datenkanal keinen unbefugten Zugang ins Unternehmensnetz ermöglicht. So verbinden sich Mitarbeiter gerade im Ausland oft mit öffentlichen WLANs, um teure Roaminggebühren zu sparen. Unter Gesichtspunkten der IT-Sicherheit stellt dies ein Worst Case Szenario dar. Zur Absicherung der Kommunikation bieten die Hersteller kaum entsprechende Lösungen. Ein auf die Sicherheitsbedürfnisse eines Unternehmens zugeschnittener Ansatz muss neben dem Mobilgerät auch die Zugänge ins Unternehmen berücksichtigen.

3.4 Trennung von geschäftlichen und privaten Daten

Insbesondere aus datenschutzrechtlichen Gründen müssen geschäftliche und private Daten streng getrennt werden. Dies gilt unabhängig davon, ob ein privates Gerät geschäftlich genutzt („Bring your own Device“) oder ein vom Unternehmen gestelltes Gerät für eine private Nutzung freigegeben wird („Corporate Owned - Personally Enabled“). Zu den rechtlichen Konsequenzen einer gemischten Nutzung gibt es umfangreiche Ausarbeitungen, deren Kernaussage im Wesentlichen lautet, dass sich eine Verwaltung privater Geräte durch das Unternehmen verbietet. Die meisten Lösungen, die Unternehmen heute für eine Verwaltung und Absicherung der Geräte verwenden, unterscheiden jedoch nicht zwischen den beiden Nutzungsebenen und können nur das gesamte Gerät verwalten. Daher muss in der Praxis immer ein Firmengerät parallel betrieben und mitgeführt werden.

Aus Sicht der Anwender ein ganz und gar unbefriedigendes Ergebnis. Ihre Motivation, dauerhaft mit zwei Geräten herumzulaufen, dürfte äußerst gering sein. Eine Trennung geschäftlicher und privater Daten bietet zum heutigen Zeitpunkt einzig Blackberry mit seiner neuen Plattform 10.

3.5 Integration bestehende Security Infrastruktur

Smartphones stellen IT-Abteilungen vor eine ganze Reihe von Herausforderungen. Neue Konzepte und Vorgehensweisen müssen geprüft, neue Produkte und Tools evaluiert und eingeführt werden. Dabei sollten bestehende Unternehmensrichtlinien und Anforderungen, die typischerweise sehr langfristig angelegt sind, berücksichtigt werden. Vorhandene Mechanismen und Tools wie etwa eine Public Key Infrastruktur müssen soweit möglich integriert werden.

3.6 User Experience

Vor allem aber: Unter den Security-Anforderungen darf keinesfalls die Usability leiden. Die einfache und flexible Bedienung sowie die zeit- und ortsungebundene Zugriffsmöglichkeit auf digitale Informationen haben den Siegeszug von Smartphones und Tablets erst eingeleitet. Wenn es der IT nicht gelingt, eine hohe Sicherheit bei gleichzeitiger Bewahrung der Usability-Vorteile zu erreichen, werden die Benutzer erneut Mittel und Wege finden, mit ungeeigneten Maßnahmen die Sicherheitsvorkehrungen zu umgehen, um sich die Arbeit zu erleichtern.

4. LÖSUNGSANSÄTZE

Die Security-Probleme durch den Einsatz von Tablets und Smartphones sind noch recht jung. Mit Ausnahme von Blackberry berücksichtigen die allermeisten Hersteller die Unternehmensanforderungen kaum, sondern adressieren hauptsächlich private Konsumenten und deren Anforderungen. Aus diesen Gründen bilden sich derzeit eine ganze Reihe von Lösungsansätzen heraus, die in Verbindung mit entsprechenden Produkten die genannten Aufgaben lösen sollen. Insbesondere die beiden Ansätze „Mobile Device Management“ und „Security Container“ gelten als vielversprechend und setzen sich derzeit am Markt durch. Es gibt aber auch eine Reihe weiterer, zum Teil einfacherer Lösungsansätze.

4.1 Blockieren oder Filtern

Der radikalste Ansatz liegt darin, Nutzung von Smartphones und Tablets komplett zu blockieren. Durch entsprechende serverseitige Filter kann dies auch in Abstufungen erfolgen. Auf diese Weise lassen sich lediglich einzelne Inhalte, etwa E-Mail-Anhänge, gezielt sperren. Vordergründig ein sicherer Ansatz, allerdings bietet er keinerlei Mehrwert für Nutzer und es besteht immer die Gefahr, dass Schutzmechanismen durch Anwender umgangen werden. Damit landen sensible Informationen möglicherweise in privaten E-Mail- oder Dropbox-Accounts und sind damit gänzlich außerhalb der Kontrolle des Unternehmens.

4.2 Remote Access ohne Speicherung lokaler Daten

Bei dieser Vorgehensweise verhindern Online-Lösungen, das sensible Daten lokal auf dem Gerät gespeichert werden. Der Zugriff auf Unternehmensdaten erfolgt dabei ähnlich einer Remote-Desktop-Lösung, das Mobilgerät wird letztlich lediglich als Tatstatur und Bildschirm genutzt. Auf diese Weise kann sicher ausgeschlossen werden, dass lokal vorhandener Informationen in fremde Hände gelangen. Voraussetzung ist allerdings, dass

keinerlei temporäre Dateien lokal gespeichert werden und die Datenübertragung stark verschlüsselt ist. Allerdings leidet die Usability bei einer solchen Lösung erheblich: Ohne lokale Datenhaltung ist eine permanente und stabile Internetverbindung erforderlich. In Zügen oder Flugzeugen kann in der Regel gar nicht oder nur sehr eingeschränkt gearbeitet werden. Typische Benutzererfahrung einer echten App lassen sich mit Remote-Lösungen zudem nur schwer umsetzen, da die Remote-Lösung nur eingeschränkten Zugriff auf die im Gerät verbauten Sensoren erhält und die Geschwindigkeit der Anwendung von der Internetverbindung abhängt.

4.3 Mobile Device Management

Lösungen zum Mobile Device Management (MDM) haben sich in den letzten beiden Jahren stark verbreitet und werden bereits in vielen Unternehmen eingesetzt. Die wesentliche Zielsetzung dieser Lösungen liegt in einer zentralen Verwaltung der mobilen Endgeräte. Ein Unternehmen ist so immer Bilde, welcher Benutzer welches Gerät, mit welcher Softwareversion und welchen Apps verwendet. MDM-Lösungen übernehmen typischerweise die Verteilung von Software und erlauben es, gewisse Einstellungen am Gerät vorzunehmen. Allerdings gibt es hier wichtige Einschränkungen zu machen: Grundsätzlich können MDM-Lösungen nur die Funktionen verwalten können, die vom Gerätehersteller vorgesehen sind. Ein höheres Sicherheitsniveau als vom Hersteller vorgesehen, lässt sich mit MDM-Werkzeugen daher nicht erreichen.

Für Unternehmen, in denen eine große Zahl mobiler Endgeräte verwaltet werden, empfiehlt sich fraglos der Einsatz einer MDM-Lösung. Allerdings gilt es zu bedenken, dass MDM keine Security-Lösung darstellt, auch wenn der eine oder Hersteller sein Produkt um zusätzliche Funktionalitäten in diesem Umfeld erweitert. In „Bring Your Own Device"-Szenarien scheidet MDM allein aufgrund rechtlicher Rahmenbedingungen gänzlich aus, da das private Gerät eines Mitarbeiters nicht unter die Verwaltung des Unternehmens gebracht werden darf.

4.4 Secure Container

Ein besserer Lösungsansatz der sich am Markt zunehmend durchsetzt, sind sogenannte „Secure Container". Dabei wird auf einem Gerät ein eigener geschützter Bereich für die unternehmensbezogenen Informationen geschaffen. In diesem Bereich werden E-Mails, Kontakte, Kalender und Dokumente verwaltet und aus diesem Bereich kann gesichert auf Unternehmensanwendungen zugegriffen werden. Da dieser Bereich vom Rest des Geräts komplett abgeschirmt wird, ist eine uneingeschränkte persönliche Nutzung ohne weitere Risiken für das Unternehmen jederzeit möglich.

Dabei werden die lokal gespeicherten Informationen, die sich innerhalb des „Secure Containers" befinden, ebenso wie der Kommunikationskanal ins Unternehmen stark verschlüsselt. Die zur Autorisierung des Benutzers erforderlichen Methoden können durch das Unternehmen festgelegt werden und reichen von Passwörtern, die gewisse Anforderungen erfüllen müssen, bis hin zu Smartcards. Selbst wenn das Mobilgerät des Mitarbeiters komplett ungesichert bliebe, könnte eine dritte Person ohne genau festgelegte Authentifizierung nicht auf den Secure Container zugreifen.

Um ein höchstmögliches Sicherheitsniveau zu erreichen, kann die Absicherung der Informationen auch über eine Smartcard erfolgen. Dabei handelt es sich um ein geschlossenes Sicherheitssystem, das nicht unter der Kontrolle des Smartphone- oder Tablet-Herstellers steht. Wenn die Entschlüsselung der lokal gespeicherten Informationen über eine Smartcard erfolgt, können die Daten nach heutigem Stand der Technik daher nicht kompromittiert werden. Das gilt aufgrund der spezialisierten Sicherheitsarchitektur selbst für den Fall, dass sich die Smartcard in den Händen eines Angreifers befindet.

Von entscheidender Bedeutung ist auch, dass der Secure Container auf dem mobilen Endgerät vollständig durch das Unternehmen kontrolliert wird. Die Unternehmens-IT kann selbst festlegen, welche Sicherheitsanforderungen an eine Autorisierung oder Verschlüsselung, möglicherweise differenziert nach Benutzergruppen, gestellt werden. Sie kann bestimmen, welche Dokumentenmanagementsysteme, welcher E-Mail-Accounts oder Intranet-Anwendungen aus dem Container heraus genutzt werden dürfen. Auf diese Weise lässt sich sehr einfach festlegen, dass Anwender nur mittels verschlüsselter E-Mails untereinander kommunizieren.

All dies bedeutet aber nicht, dass die Unternehmens-IT selbst Zugriff auf die Daten erlangen könnte. Vielmehr ist sichergestellt, dass die im Unternehmen geltenden Anforderungen und Richtlinien auch für die auf dem

mobilen Endgerät genutzten Informationen und Prozesse gelten. Gleichzeitig werden diese lokal vorhandenen Informationen sowie die durch die Mobilgeräte eröffneten Zugänge ins Unternehmen bestmöglich gegen unbefugten Zugriff durch Dritte geschützt.

Letztlich wird das Unternehmensnetzwerk auf das Smartphone oder Tablet erweitert, weshalb man auch von einem „Secure Connected Container" spricht. Der Benutzer kann das Gerät uneingeschränkt persönlich nutzen, die Unternehmensdaten werden jedoch mit höchstmöglicher Sicherheit geschützt.

Mehrwert gegenüber Apple Standardmechanismen

Mit Ausnahme von Blackberry sieht heute kein Hersteller eine getrennte Datenhaltung von privaten und geschäftlichen Daten vor. Apples iOS-Betriebssystem darf heute gegenüber Googles Android und Microsofts Mobile Phone als besonders sicher gelten. Bislang sind im Apple-Umfeld kaum Viren bekannt. Und trotzdem öffnet auch iOS noch beträchtliche Lücken:

+ Selbst wenn die NSFileProtection zur Verschlüsselung lokaler Daten für einzelne Apps auf iOS-Systemen aktiviert ist, kann diese, sobald die PIN des Benutzers bekannt ist, umgangen werden.

+ Unabhängig davon entzieht es sich jeglicher Kontrolle, wo temporäre Dateien mit möglicherweise sensiblen Daten auf dem Gerät abgelegt werden.

+ Besonders dramatisch: Schlüssel und Zertifikate – die zentralen Bestandteile für praktische alle Sicherheitsmechanismen von der E-Mail-Verschlüsselung bis hin zur Absicherung ab- und eingehender Verbindungen – liegen in der iOS Keychain, die jederzeit kompromittiert werden kann.

Generell wird es für einen großen einen Hersteller mit bedeutendem Marktanteil immer sehr schwierig sein, seine Systeme komplett abzusichern. Dies liegt weniger an mangelnder Sorgfalt des Herstellers, als an der hohen Motivation, dessen Systeme zu kompromittieren. Je verbreiteter ein Betriebssystem, desto größerer Aufwand kann betrieben werden, um es zu knacken. Dezentral implementierte Sicherheitslösungen sind dagegen aus wirtschaftlicher Sicht kaum zu überwindende Hürden.

Secure Container Lösungen bietet nach heutigem Stand der Technik die höchst-mögliche Sicherheit. Je nach Art der Containerlösung und zusätzlicher Absicherung (wie etwa über ein Secure-Element in Form einer Smartcard), besteht nach herrschender Meinung keine Möglichkeit die Daten innerhalb eines Secure Containers zu kompromittieren. Das gilt nach Aussage der Smartcard Hersteller auch für entsprechende ausgerüstete Dienste. Eine 2.048 BIT-Verschlüsselung mittels Smartcard kann nach heutigem Stand der Technik nicht kompromittiert werden. Potentielle Angriffe müssten bei einer derartigen Absicherung über den Prozess (etwa bei der Ausstellung der Smartcards) ansetzen.

5. SCHLUSSBEMERKUNG

Die Entwicklung geht klar in diese Richtung: Mittelfristig wird jede Information, jeder Prozess, der heute am Arbeitsplatzrechner genutzt wird, auch an mobilen Endgeräten verfügbar sein. Hochsicher und mit der Nutzerfreundlichkeit, die den mobilen Endgeräten zu ihrem Siegeszug verholfen haben. Unternehmensmitarbeiter wollen auf diese Vorzüge ebensowenig verzichten, wie sie dauerhaft mit zwei Geräten unterwegs sein wollen. Aus diesem Grund ist eine saubere Trennung von privater und geschäftlicher Nutzung wichtig – uns aus rechtlichen Gründen sogar unabdingbar.

Das entsprechenden Ansätzen, Produkten und Vorgehensweisen kann die Unternehmens-IT diesen Anforderungen Rechnung tragen. Voraussetzung ist eine Betrachtung der konkrete Anforderungen eines Unternehmens oder in anderen Worten die Erarbeitung einer Mobilstrategie.

SecurePIM
by virtual solution

Checkliste Mobile Security

+ Ist das Thema Sicherheit in Ihrem Unternehmen Chefsache?
  Wenn nein, sollten Sie regelmäßige Audits mit durchführen.

+ Welche Daten in ihrem Unternehmen sind besonders schützenswert?
  Dies können entweder Daten sein, die aufgrund juristischer Bestimmungen oder zur Aufrechterhaltung der eigenen Wettbewerbsfähigkeit geschützt werden müssen. Identifizieren Sie dieses Inventar.

+ Gibt es ein Sicherheitskonzept, mit dem diese Daten geschützt werden?
  Schließt dieses Konzept auch mobile Zugangswege ein?

+ Werden in Ihrem Unternehmen private mobile Endgeräte genutzt, um damit dienstliche Aufgaben zu erledigen? Ist dies im Sinne des Unternehmens wünschenswert? Gibt es dafür eine implizite oder explizite Erlaubnis?

+ Sind Ihren Mitarbeitern die Gefahren bewusst, die sich durch eine Nutzung mobiler Endgeräte ergeben?

+ Hat Ihre Unternehmens-IT einen Überblick darüber, mit welchen Endgeräten und Betriebssystem-Versionen auf Unternehmensdaten zugegriffen wird? Erfüllt Ihre Unternehmens-IT die Anforderungen, die der Datenschutz bei der Geräteverwaltung stellt?

+ Sind Sie in der Lage, bei einem Geräteverlust alle sensiblen Daten auf dem Gerät ihres Mitarbeiters vor fremden Zugriff zu schützen?

+ Können Sie sicherstellen, dass bei der Authentifizierung am Gerät Mindeststandards eingehalten werden?

+ Lassen sich auf den Geräten Ihrer Mitarbeiter private und dienstliche Daten und Anwendungen sauber trennen?

Sollten Sie auch nur eine der vorstehenden Fragen negativ beantworten müssen, ist die Einführung einer durchgängigen Mobile-Security-Strategie dringend angeraten.

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