Virtual Solution

EINE EINFACHE UND SICHERE LÖSUNG FÜR
BRING YOUR OWN DEVICE

Der stationäre Arbeitsplatz wird zum Auslaufmodell. In Deutschland ist mittlerweile die Mehrheit der Beschäftigten vorwiegend oder sogar ausschließlich mobil an wechselnden Arbeitsplätzen tätig – Tendenz weiter steigend. Viele Mitarbeiter setzen dabei eigene Smartphones oder Tablets auch beruflich ein. Zudem stellt der Trend zu „Bring Your Own Device“ (BYOD) die IT-Abteilung vor große Herausforderungen hinsichtlich Management, Datenschutz und vor allem Sicherheit. Schließlich geraten mobile Geräte zunehmend ins Visier von Hackern. Wichtige Themen sind hier die klare Trennung von geschäftlichen und privaten Daten, der Schutz vor unberechtigtem Zugriff oder Verschlüsselung. Container-Lösungen erfüllen all diese Anforderungen. Mit Hilfe von Containern können Unternehmen ihre Apps und Daten auf dem mobilen Gerät in einer geschützten, abgeschotteten Umgebung betreiben und verwalten - egal ob es privat ist (BYOD) oder von der Firma gestellt wird (COPE). Dadurch verhindern sie, dass Daten unkontrolliert ab- oder einfließen beziehungsweise manipuliert werden können.

BRING YOUR OWN DEVICE

EINE EINFACHE UND SICHERE LÖSUNG FÜR BRING YOUR OWN DEVICE

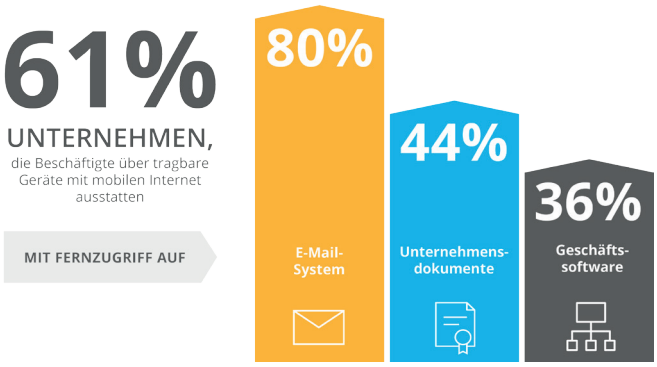
Mobil statt stationär: Mobile Worker stellen die Mehrheit

Außendienstmitarbeiter greifen von unterwegs via Smartphone auf ihre Daten und geschäftlichen Anwendungen zu, Ärzte erscheinen zur Visite mit Tablets am Patientenbett und Service-Techniker nutzen robuste Smartphones für die Verwaltung ihrer Aufträge - mobiles Arbeiten ist der neue Mainstream. Das belegt auch die 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) Mitte 2016 vorgestellt hat.

Zentrales Ergebnis: Heute sind bereits mehr als die Hälfte der Beschäftigten (54 Prozent) vorwiegend oder sogar ausschließlich mobil an wechselnden Arbeitsplätzen tätig, sei es im Home-Office, an wechselnden Orten innerhalb des Unternehmens, auf Geschäftsreisen, im Café oder im Zug. Das heißt, Beschäftigte, die vorwiegend an einem einzigen, stationären Arbeitsplatz sitzen, stellen mit 46 Prozent mittlerweile die Minderheit.

Vorreiter sind die großen Unternehmen

Auch die Zahlen des Statistischen Bundesamts zeigen, dass mobiles Arbeiten in Deutschland weiter zunimmt. Demnach stellen mittlerweile 61 Prozent der deutschen Unternehmen ihren Beschäftigten tragbare Geräte mit mobilem Internetzugang zur Verfügung (2015: 57 Prozent) - Tendenz weiter steigend. Der Reifegrad korreliert dabei mit der Unternehmensgröße. Während 60 Prozent der kleinen Unternehmen mit bis zu neun Angestellten die Voraussetzungen für mobiles Arbeiten schaffen, sind es bei größeren Unternehmen (250 und mehr Mitarbeiter) bereits 94 Prozent. Schließlich bieten mobile Arbeitsplätze Arbeitnehmern neue Möglichkeiten und Freiheiten, ihr Berufsleben ihrem individuellen Rhythmus anzupassen und so effektiver zu gestalten - und damit auch mit ihrem Privatleben in Einklang zu bringen.



Statistisches Bundesamt, IKT in Unternehmen 2016

Allerdings schränken Unternehmen die Nutzung und Funktionen mobiler Geräte im Vergleich zu einem festen Arbeitsplatz (noch) ein. 80 Prozent der Unternehmen gewähren ihren Mitarbeitern den Zugriff auf E-Mails, 44 Prozent erlauben den Zugang zu Unternehmensdokumenten und deren Bearbeitung. In etwas mehr als einem Drittel der Firmen (36 Prozent) dürfen die Beschäftigten auf ihren Smartphones oder Tablets auch mit firmeninterner Geschäfts-Software arbeiten.

Die Integration mobiler Geräte in die IT-Infrastruktur stellt allerdings eine der größten Herausforderungen für Unternehmen dar. Ein wichtiger Trend ist Bring Your Own Device (BYOD), sprich die berufliche Nutzung privater Smartphones oder Tablets. Alternative Ansätze sind COPE (Corporate Owned, Personally Enabled) oder CYOD (Choose Your Own Device) – siehe Kasten.

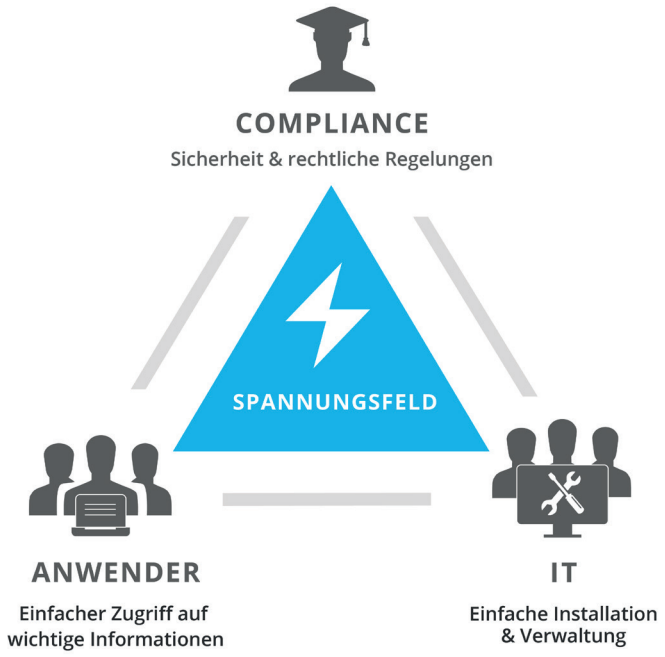
BYOD als Herausforderung für die IT-Abteilung

Den Anfang für BYOD machte vor Jahren meist der Geschäftsführer, der mit seinem neuen Smartphone auf seine E-Mails zugreifen wollte. Dann kamen die Vertriebsmitarbeiter im Außendienst auf die IT-Abteilung zu, um die aktuellen Verkaufszahlen auch beim Kunden vor Ort abzurufen. Und mit der Zeit waren es immer mehr Mitarbeiter, die ihre privaten Geräte mit in die Firma brachten und Zugriff auf die Unternehmens-IT verlangten.

BRING YOUR OWN DEVICE

Viele IT-Administratoren kennen dieses Szenario - und zerbrechen sich darüber die Köpfe. Sollen sie private Smartphones, Tablets oder Netbooks akzeptieren oder aussperren? Die Bedenken der IT-Abteilung liegen auf der Hand. Sie hat zunächst schlicht und einfach Angst, die Kontrolle über die unternehmenseigenen Daten zu verlieren. Die Vielzahl privater Endgeräte widerspricht dem Bedürfnis nach Standardisierung. Schließlich muss die IT alle gängigen mobilen Betriebssysteme unterstützen, von Apple iOS über Google Android und Blackberry bis hin zu Microsoft Windows 10 (Mobile). Mit der privaten Nutzung verschwimmen zudem die Grenzen zwischen privaten und Unternehmensdaten. Weitere Probleme können bei der Verwaltung der Geräte sowie auch bei Berechtigungen und dem Einsatz von Sicherheitsprodukten entstehen, ganz zu schweigen vom Support am Service Desk.

Mittlerweile unterstützen die meisten Unternehmen BYOD-Programme für den Einsatz privater Smartphones oder Tablets im Unternehmen, da BYOD neben den Herausforderungen auch einige Vorteile bringt. So kann beispielsweise die Produktivität der Mitarbeiter erheblich steigen, weil mobile Geräte und Apps komfortabler und benutzerfreundlicher sind als PCs oder Unternehmenssoftware.



Insbesondere jüngere Mitarbeiter wollen auch beruflich und von unterwegs schnell und flexibel mit den ihnen bekannten Tools arbeiten, sei es auf dem Firmenrechner oder ihrem persönlichen Gerät. Die Erlaubnis private Endgeräte am Arbeitsplatz nutzen zu dürfen, kann Unternehmen auch vor dem Hintergrund der „Work-Life-Balance“ als Arbeitgeber attraktiver machen. In Zeiten des drohenden Fachkräftemangels ist das ein nicht zu unterschätzender Faktor.

Hoher Aufwand für die Verwaltung

Auf der einen Seite hoffen viele Unternehmen, mit Hilfe von BYOD Kosten zu sparen, da die Ausgaben für den Kauf der Hardware entfallen. Doch auf der anderen Seite steigt der Aufwand für Administration und Support. Durch die große Anzahl unterschiedlicher Geräte und Betriebssysteme sowie die oftmals gleichzeitig private und geschäftliche Nutzung ergeben sich eine Vielzahl neuer Anforderungen hinsichtlich Management, Datenschutz und Sicherheit. Auch die Einrichtung einer speziellen Mobile Device Management (MDM)-Software für die Aktivierung, Verwaltung und Absicherung der Geräte ist nicht unbedingt trivial.

Hier kann die IT-Abteilung den Unmut der Mitarbeiter hervorrufen, wenn sie über das MDM-Tool beispielsweise Funktionen zur Ortung der Geräte oder Remote Wipe (Löschung der Daten aus der Ferne) einsetzen will. Nicht jeder Mitarbeiter wird diesen (Kontroll-)Funktionen auf seinem privaten Gerät zustimmen. Etwas geschickter ist der Ansatz, nur die mobilen Anwendungen zu kontrollieren, die mit der Arbeit im Unternehmen zu tun haben.

Die Kombination aus privatem Endgerät und Kontrolle durch das Unternehmen stellt zudem eine Herausforderung beim Datenschutz dar und kann zu rechtlichen Problemen führen. BYOD-Geräte enthalten private Daten des Mitarbeiters wie Familienfotos oder Informationen aus sozialen Netzwerken. Daher besteht die Gefahr, dass die IT-Administratoren auf private Daten der Mitarbeiter zugreifen können. Die Mitarbeiter selbst dürften Probleme haben, die Grenze zwischen privater und beruflicher Nutzung zu erkennen. Denn betrieblich genutzte Smartphones enthalten auch kritische und sensible

BRING YOUR OWN DEVICE

Unternehmensdaten. Zudem nutzen Mitarbeiter zunehmend Cloud-Services für ihre tägliche Arbeit. Daher besteht bei BYOD die Gefahr, dass Benutzer nicht verifizierte Anwendungen auf ihren Geräten installieren, die gut getarnte Malware darstellen.

Angriffe auf mobile Geräte nehmen zu

Eines ist klar: Die mobilen Bedrohungen nehmen zu und werden komplexer. Ein Beispiel sind gezielte Angriffe auf iPhones mit der Spionagesoftware Pegasus, eine der größten mobilen Bedrohungen im Jahr 2016. Pegasus nutzte drei Zero-Day-Schwachstellen („Trident“) aus und rootete unbemerkt die Geräte der Opfer. Hacker konnten dadurch auf Nachrichten, Anrufe, E-Mails oder Protokolle von Apps wie Gmail, Facebook, Skype, WhatsApp oder Kalender zugreifen. Auch Ransomware für mobile Endgeräte nimmt stark zu. Hier verschlüsseln Angreifer Daten auf dem Smartphone, um Lösegeld für deren Freigabe zu erpressen. So stieg die Zahl der Ransomware-Attacken dem Security Report 2016 von Check Point Software Technologies zufolge von Juli auf August 2016 um 30 Prozent - Tendenz steigend.

Mobile Geräte wie Smartphones oder Tablets geraten nicht zuletzt deswegen immer stärker ins Fadenkreuz von Hackern, weil sie vermehrt Funktionen für geschäftskritische Prozesse bieten und mit dem Backend des Unternehmens verbunden sind. So zeigt die aktuelle Studie „Mobile Security in Deutschland 2017“ der Marktforscher von IDC, dass sich im Jahr 2016 die Sicherheitslage gegenüber 2015 verschärft hat. Demnach 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.

Auch der finanzielle Schaden durch Sicherheitsbrüche mit mobilen Technologien ist immens. Anwaltskosten, Strafzahlungen oder Geschäftseinbußen treiben die Kosten in die Höhe. 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.

Mobile Security: Geräte, Apps & Daten schützen

Daher müssen Unternehmen die mobilen Geräte ihrer Mitarbeiter viel besser absichern als bisher. Kaspersky Lab hat 2016 in einer Umfrage festgestellt, dass 2016 weltweit nur 53 Prozent aller Smartphones in Firmen über Sicherheitslösungen gegen Cyberangriffe verfügten. Es ist Zeit zu handeln. Doch mit dem Schutz der physischen Endgeräte alleine ist es nicht getan. Durch BYOD verschiebt sich der Security-Fokus vom Gerät hin zu den Apps und den Inhalten. Denn viele Mitarbeiter, die ihre privaten Geräte dienstlich nutzen, wollen die Kontrolle über diese nicht an den Arbeitgeber abgeben. Außerdem stellen Unternehmen zunehmend auch freien Mitarbeitern, Partnern oder externen Dienstleistern individuelle Apps und Daten zur Verfügung.

Für die zentrale Verwaltung ihrer Endgeräte setzen viele Unternehmen auf Mobile-Device-Management (MDM)-Lösungen. Mit diesen ist es neben der Inventarisierung auch möglich, zentral Sicherheitseinstellungen und Richtlinien für Smartphones und Tablets festzulegen, Konfigurationen zu verändern oder Zugriffsrechte zu definieren. Verlorene oder gestohlene Geräte lassen sich sperren oder aus der Ferne zurücksetzen. Zum Funktionsumfang gehören auch Maßnahmen gegen Missbrauch wie das Deaktivieren der Kamera, das Setzen von Passwörtern oder die Abwehr von Jailbreaks.

Etwas komplexer ist die Verwaltung der mobilen Apps. Lösungen für Mobile Application Management (MAM) regeln, auf welche Anwendungen die Nutzer zugreifen dürfen, seien es Unternehmens-Apps oder Apps aus öffentlichen App-Stores. MAM gewährleistet, dass die Installation und der Zugriff auf alle Apps nur nach den Unternehmensrichtlinien erfolgen. Unternehmen können dadurch auch einzelne Applikationen und deren Daten verteilen, ohne direkten Zugriff auf das Gerät haben zu müssen.

MDM und MAM bilden die zentralen Säulen von Enterprise Mobility Management (EMM), einem umfassenden Ansatz für das Management und die Sicherung mobiler Geräte, Anwendungen und Informationen sowie deren Integration in die Firmen-IT. EMM-Lösungen sind aber für viele (kleine und

BRING YOUR OWN DEVICE

mittlere) Unternehmen überdimensioniert und kostspielig. Außerdem sind EMM-Lösungen komplex zu verwalten. Die einfache und sichere Alternative für mobile Kommunikation der Zukunft bilden Container-Lösungen.

Container trennen private und berufliche Daten

Beim Container-Ansatz steht der Schutz der Informationen und Daten im Vordergrund. Anstatt das Gerät zu kontrollieren, liegt der Fokus auf der Sicherheit der Daten auf dem mobilen Endgerät, egal ob es privat ist (BYOD) oder von der Firma gestellt wird (COPE). Mit Hilfe von Containern lassen sich die Apps und Daten eines Unternehmens auf dem mobilen Gerät in einer geschützten, abgeschotteten Umgebung betreiben und verwalten. Dadurch wird verhindert, dass Daten unkontrolliert ab- oder einfließen beziehungsweise manipuliert werden.

Container ermöglichen die klare Trennung von privaten und geschäftlichen Daten und Apps. Welches Unternehmen sieht es gerne, dass sensible Firmendaten im selben Verzeichnis liegen wie die Urlaubsfotos des Mitarbeiters? Zugleich wird durch die strikte Trennung auch die Privatsphäre der Mitarbeiter geschützt.

Eine sicher konfigurierte Container-Lösung verhindert beispielsweise, dass Firmeninformationen per Copy & Paste auf Social-Media-Kanälen wie Facebook oder Twitter landen. Das heißt: Ein Nutzer kann aus dem Unternehmens-Bereich heraus nicht auf seine privaten Apps zugreifen. Mögliche Schwachstellen am Gerät oder Fehler des Anwenders lassen sich dadurch weitestgehend ausschalten.

COPE und CYOD: Alternativen zu BYOD

BYOD ist nicht der einzige Ansatz für die Integration mobiler Geräte wie Smartphones oder Tablets in das Unternehmens-Netzwerk. Alternativen sind COPE (Corporate Owned, Personally Enabled) oder CYOD (Choose Your Own Device).

Beim **COPE-Ansatz** stellt das Unternehmen den Mitarbeitern ein Smartphone oder Tablet zur Verfügung, es handelt sich also nicht um das privat gekaufte Gerät. COPE erlaubt ausdrücklich, die Geräte sowohl für private als auch geschäftliche Aufgaben zu nutzen. Dafür ist der Mitarbeiter aber – zumindest bis zu einem gewissen Grad – für die Einrichtung und das laufende Handling selbst verantwortlich. Da das Unternehmen im Gegensatz zu BYOD Eigentümer des mobilen Geräts ist, vereinfacht sich die Administration der Geräte. Die IT-Abteilung kann das Ausrollen der Geräte und die Bereitstellung der Anwendungen standardisieren und zentral abwickeln sowie die Geräte besser kontrollieren als bei BYOD.

Der **CYOD-Ansatz** ähnelt COPE, erlaubt Mitarbeitern aber weniger Rechte für die Konfiguration des Geräts. Hier definiert das Unternehmen auch einen festen Pool an Geräten, aus dem die Mitarbeiter dann ein Smartphone oder Tablet wählen. Die Verwaltung der Geräte verbleibt aber ausschließlich beim Unternehmen; den Mitarbeitern wird aber gestattet, die Geräte auch für den privaten Bereich zu nutzen. Welche Daten darauf genutzt werden dürfen, wird im Rahmen der Rahmenvereinbarungen definiert.

Virtual Solution

BRING YOUR OWN DEVICE

Vorteile für Administratoren, Mitarbeiter und Compliance-Verantwortliche

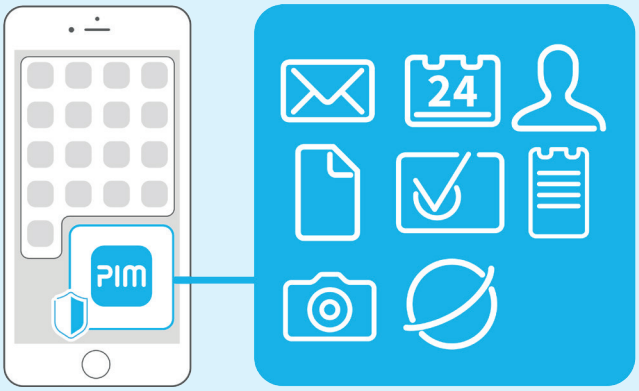
Das SecurePIM-Management-Portal erlaubt es Administratoren, Sicherheitsregeln wie etwa Vorgaben für die Länge von Passwörtern oder das Verbot von einfachem Kopieren innerhalb der SecurePIM-App ganz einfach festzulegen. In Kombination mit dem SecurePIM-Gateway bestimmen sie, wer mit seinem mobilen Endgerät Zugriff auf Unternehmensdaten erhält. Wenn der Mitarbeiter das Unternehmen verlässt oder das Gerät verloren geht, können die Unternehmensdaten im SecurePIM Container umgehend gelöscht werden. Administratoren erhalten dadurch vollständige Kontrolle über die Firmeninformationen, ohne die Privatsphäre der Mitarbeiter zu verletzen.

Das Rollout der App geht einfach und schnell. Mitarbeiter laden sich die App aus dem App Store (iOS) oder Google Play Store (Android) herunter und loggen sich mit ihren Anmeldeinformationen ein. Aufgrund der intuitiven Benutzeroberfläche finden sie sich ohne spezielle Einarbeitung sofort zurecht. Die Mitarbeiter können dann über SecurePIM mit Smartphone oder Tablet einfach auf Firmendaten zugreifen, von unterwegs arbeiten und natürlich ihre mobilen Geräte auch problemlos privat nutzen.

Auch die Sicherheits- und Compliance-Verantwortlichen profitieren von SecurePIM. Das Prinzip des gesicherten Containers ist sowohl für COPE- als auch für BYOD-Szenarien geeignet. Dank moderner Kryptografie-Technologien sind die Daten im Container, auf dem mobilen Gerät und auch bei der Übertragung zuverlässig verschlüsselt. Damit lassen sich Man-in-The-Middle-Attacken verhindern. Und der wohl entscheidende Vorteil: Die Firmendaten und privaten Daten werden auf demselben Endgerät strikt voneinander getrennt.

Sicherer Container mit SecurePIM

SecurePIM packt E-Mails, Kontakte, Kalender, Notizen, Aufgaben, Dokumente und Intranet auf dem Smartphone oder Tablet (iOS und Android) in einen verschlüsselten Container. Die Verschlüsselung erfolgt dabei hybrid mit RSA-4096 und AES-256. Die Software basiert auf demselben Sicherheitskern wie die einzige vom BSI (Bundesamt für Sicherheit in der Informationstechnik) zugelassene Lösung für iOS-basierte Mobilgeräte (VS – NfD „VERSCHLUSSSACHE - NUR FÜR DEN DIENSTGEBRAUCH“). SecurePIM lässt sich sowohl in der Cloud als auch On-Premise nutzen.



Mit der SecurePIM-App ist es zudem möglich, S/MIME-verschlüsselte E-Mails zu senden und zu empfangen. SecurePIM AutoPKI vereinfacht das Schlüssel- und Zertifikats-Management, da sie S/MIME-Schlüssel automatisch generiert und verschickt. Über SecurePIM Sync lassen sich E-Mails auch auf dem Desktop verschlüsseln.

Da die Virtual Solution AG sämtliche sicherheitsrelevante Bereiche der App und der zugehörigen Admin-Konsole selbst entwickelt hat, bietet SecurePIM zu 100 Prozent Sicherheit „Made in Germany“. Die Server stehen in deutschen Rechenzentren. Es gelten die deutschen Datenschutzrichtlinien.

Virtual Solution AG
Blutenburgstraße 18
D-80636 München

+49 (0)89 30 90 57-0

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

ÜBER VIRTUAL SOLUTION

Als IT-Sicherheitsspezialist entwickelt, produziert und vertreibt Virtual Solution mit seiner Applikation „SecurePIM“ und dem Framework „SERA“ Sicherheitslösungen rund um die sichere mobile Kommunikation für Behörden und Unternehmen für iOS und Android Geräte. Virtual Solution ist ein deutsches, international agierendes Unternehmen mit dem Ziel, die mobile Arbeitswelt der Zukunft benutzerfreundlich zu gestalten und zu sichern.