MATERNA
Virtual Solution

Container-Technologie

Zukunftssichere Lösung für IT-Sicherheit bei Smartphones und Tablets

Materna Virtual Solution GmbH · Januar 2023

MATERNA
Virtual Solution

Mobilgeräte – Einfallstor für Cyberangriffe? Bollwerk gegen Hacker:innen!

Smartphones oder Tablets geraten zunehmend ins Fadenkreuz von Hacker:innen. Wenig überraschend, bieten sie doch Funktionen für geschäftskritische Prozesse und sind mit dem Backend von Organisationen verbunden. In Anbetracht dessen ist es fast unverständlich, dass laut Bundesamt für Sicherheit in der Informationstechnik (BSI) die Hälfte aller in einer Studie befragten Unternehmen weniger als 10 Prozent ihrer IT-Ausgaben in Cybersicherheit investieren[1]. Zum Vergleich: Das BSI empfiehlt mindestens 20 Prozent in den Schutz der eigenen IT zu investieren.

Doch oft vernachlässigen Organisationen die Absicherung ihrer Mobilgeräte! Es besteht Nachholbedarf, damit Smartphones und Tablets nicht zum Einfallstor für Cyberangriffe werden. Lesen Sie auf den folgenden 16 Seiten, wie Sie Kommunikation sowie Daten auf Smartphones und Tablets effektiv mit modernen Sicherheitstechnologien schützen!

Nach diesem Whitepaper kennen Sie

- aktuelle Daten zum Thema Homeoffice, mobiler Arbeitsplatz & Cyber-Sicherheit
- die Gründe, weshalb IT-Sicherheit im Entscheider:innen-Kopf beginnt
- Möglichkeiten moderner IT-Sicherheit für Smartphones & Tablets
- das Sicherheitsmodell der Zukunft: Container-Technologie
- wesentliche Auswahlkriterien für Container-Lösungen

1 IT-Sicherheit im Home Office – Unter besonderer Berücksichtigung der Covid-19 Situation, BSI, 2020, S. 8.

MATERNA
Virtual Solution

Inhalt

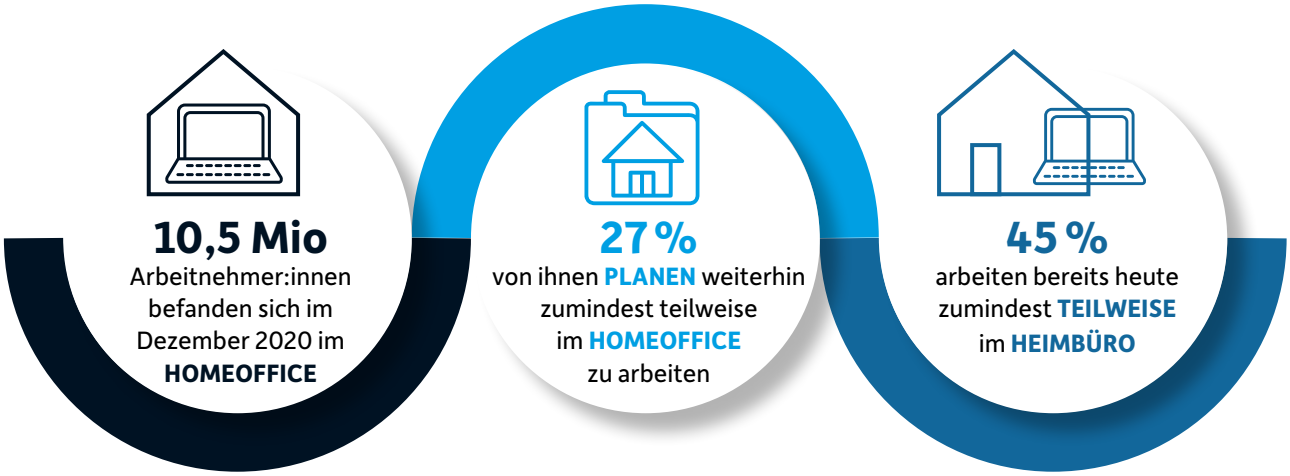
Seite

MATERNA
Virtual Solution

Homeoffice – von der Ausnahme zum neuen Normalzustand

Was sich vor den Pandemiejahren 2020/2021 bereits abzeichnete, ist nun ein Fakt: Angestellte in Organisationen müssen und wollen im Homeoffice sowie von unterwegs produktiv sein. Eine Bitkom-Studie belegt, dass Ende 2020 nahezu jede(r) vierte(r) Arbeitnehmer:in im heimischen Büro tätig war. Nicht wenige planen, dort bis auf Weiteres auch zu verbleiben.

Doch Mitarbeitende einfach ins Homeoffice zu entsenden und sicherheitstechnisch auf das Beste zu hoffen, ist ein Wagnis. Das legen auch aktuelle Zahlen von 2020/21 nahe, nach denen neun von zehn Unternehmen in Deutschland von Datenklau, Spionage oder Sabotage[2] betroffen waren.



siehe https://www.bitkom.org/Presse/Presseinformation/Mehr-als-10-Millionen-arbeiten-ausschliesslich-im-Homeoffice

2 https://t3n.de/news/unternehmen-schaden-cyberangriffe-bitkom-1396377/

Der Schaden, der dabei pro Jahr entstand, betrug sage und schreibe 220 Milliarden[3] (!) Euro. Eine Summe, die schon fast unglaublich erscheint, vor allem weil hauptsächlich Informations- und Produktionssysteme betroffen waren. Also genau jene Systeme, die einen wesentlichen Anteil zur Wertschöpfung in Organisationen beitragen.

»Mitarbeiterinnen und Mitarbeiter einfach zum Arbeiten nach Hause zu schicken, genügt nicht!«

Bitkom-Präsident Achim Berg[3]

Doch wie gewährleistet man die Integration von Smartphones und Tablets in die vorhandene Infrastruktur – ohne Verletzung der Informationssicherheit? Und das nicht nur im Homeoffice, sondern auch im Außeneinsatz, wo Mitarbeiter:innen auf den mobilen Zugriff auf die Netzwerke ihrer Organisation sowie auf webbasierte Apps angewiesen sind.

Für IT-Abteilungen ist das eine große Herausforderung, unabhängig davon, ob die Organisation ein mobiles Gerät (COPE) zur Verfügung stellt oder die Mitarbeiter:innen ihre privaten Mobilgeräte beruflich nutzen (BYOD). Neben der eigentlichen Verwaltung der Geräte stellt sich vor allem die Frage nach Sicherheit und Datenschutz. Dabei gibt es gleich mehrere Aspekte, auf die es zu achten gilt:

1) Mobile Endgeräte können leicht verloren gehen
Für diesen Fall muss sichergestellt sein, dass keine unbefugte Person Zugriff auf die Firmen- bzw. Behördeninformationen bekommt und die Daten auf einem Ersatzgerät schnell wieder verfügbar sind.

2) Mobile Geräte enthalten oft persönliche Inhalte der Mitarbeiter:innen
Fotos oder Kontakte zum Beispiel. Es besteht also die Gefahr, dass IT-Administrator:innen auf private Daten der Mitarbeitenden zugreifen können. Das gilt es zu unterbinden, wenn man die Auflagen der Aufsichtsbehörden erfüllen will.

3) Die Grenze zwischen privater und beruflicher/dienstlicher Nutzung erkennen
Betrieblich genutzte Smartphones enthalten sensible Unternehmens- bzw. Behördendaten. Mitarbeiter:innen müssen dafür sensibilisiert sein, damit sie keine unerlaubten Anwendungen auf ihren Geräten installieren, die gut getarnte Malware beinhalten oder Daten abgreifen.

Fazit: Viele Organisationen sichern ihre stationären Geräte in den Büros mittlerweile solide ab. In Homeoffice und Außendienst sieht das nach wie vor anders aus. Damit stehen sie nicht allein: Selbst Digitalvisionäre wie Amazon-Gründer Jeff Bezos, die es eigentlich besser wissen müssten, sind nicht vor unerwünschten Zugriffen auf ihre Smartphones gefeit[4]. Gerade Verantwortliche in Organisationen müssen sich also bewusst machen, dass Cyberangriffe keine Sci-Fi-Horrorszenarien sind, sondern bittere Realität im Hier und Jetzt. Und letztlich auch entsprechend handeln.

3 https://t3n.de/news/unternehmen-schaden-cyberangriffe-bitkom-1396377/
4 https://www.wiwo.de/technologie/digitale-welt/cybersecurity-mein-tipp-an-bezos-dienstliches-und-privates-auf-dem-smartphone-trennen/25467556.html

Sicherheitsthemen sind Entscheider:innenthemen!

Wenn doch alle Zahlen und Zeichen auf einen bewussteren Umgang mit Cybergefahren deuten, warum werden diese Themen nach wie vor stiefmütterlich behandelt? Größtenteils, so legt es zumindest die »Mobile Security«-Studie der Computerwoche nahe, ist das Risikobewusstsein bei Entscheider:innen erschreckend gering. Nicht, was den Datendiebstahl angeht, aber inwiefern Applikationen und Geräte ihren Anteil daran haben. Während die Hälfte der befragten 600 IT- und Geschäftsentscheider:innen Datenklau als größtes Sicherheitsrisiko für ihr Unternehmen identifiziert, betrachtet nur ein Bruchteil von ihnen mobile Apps und Geräte als Teil des Problems.

Die Studie kommt zu dem Schluss, dass es in den Entscheider:innenebenen in deutschen Organisationen schlicht am Risikobewusstsein mangelt. Doch auch fehlende Fachkenntnisse und organisatorische Defizite spielen eine Rolle. Sicherheitsthemen sind jedoch ganz klar Entscheider:innenthemen Nur wenn sie selbst ein klares Bild von IT-Risiken und ein Konzept für den Schutz der Unternehmens- bzw. Behördendaten haben, können sie es auch ihren Mitarbeiter:innen vorgeben und leben.

53 % **der befragten Entscheider:innen betrachten Datenklau als größtes Risiko**[5]

Nur 10 % **der Befragten auf Geschäftsleitungsebene sehen in mobilen Apps ein großes Risiko**[6]

5 https://www.tecchannel.de/a/mobile-security-unternehmen-unterschaetzen-die-risiken
6 https://www.tecchannel.de/a/mobile-security-unternehmen-unterschaetzen-die-risiken

Mobile IT-Sicherheit, ein Status quo der Möglichkeiten

Organisationen lösen die Herausforderung der IT-Sicherheit bei Smartphones und Tablets traditionell mit einer vollständigen Kontrolle über das Endgerät, dem Mobile Device Management (MDM). Primäres Ziel: Die vielen unterschiedlichen Geräte zentral verwalten, einheitliche Sicherheitseinstellungen und Richtlinien für Smartphones oder Tablets festlegen, Konfigurationen und Zugriffsrechte definieren. Zudem sperrt man verlorene oder gestohlene Geräte aus der Ferne oder löscht deren Inhalte.

Mehr mobile Geräte, mehr Risiken

Soweit so gut. Die Herausforderungen werden jedoch komplexer, wenn Mitarbeitende ihre Firmengeräte auch privat nutzen dürfen (COPE) oder ihre privaten Smartphones oder Tablets auch beruflich einsetzen (BYOD). Laut DSGVO müssen die privaten und geschäftlichen Daten strikt voneinander getrennt sein. Schließlich wollen Mitarbeiter:innen nicht die Kontrolle über ihre privaten Urlaubsfotos oder Social-Media-Aktivitäten an die IT-Abteilung ihrer Firma abgeben. Administrator:innen möchten wiederum vermeiden, dass sensible Daten im selben Verzeichnis liegen wie persönliche Dokumente oder Videos der Mitarbeitenden. Und schon gar nicht, dass private Apps Zugriff auf dienstliche/betriebliche Informationen, z. B. Kontaktdaten haben. Hier aber stößt MDM an seine Grenzen!

Gut zu wissen: Um mehr über die Sicherheitsrisiken zu erfahren, lesen Sie auch den Blog-Beitrag: **»So wehren Sie die gefährlichsten Angriffsmethoden auf Smartphones & Tablets ab«.**

Konzepte für den Einsatz mobiler Geräte in Organisationen

Company-Owned-Personally-Enabled (COPE)
COPE bezeichnet die Möglichkeit der Nutzung von Unternehmens- bzw. Behörden-Hardware für private Zwecke. Damit kann zum Beispiel die Überlassung eines betrieblichen/dienstlichen Smartphones auch für Privatgespräche gemeint sein. Dies hat zum Beispiel den Vorteil, dass Beschäftigte unterwegs kein zweites Gerät mit sich herumtragen müssen.

Bring-Your-Own-Device (BYOD)
BYOD bezeichnet die Nutzung von privaten Endgeräten für berufliche Zwecke. Dies umfasst den beruflichen Einsatz sowohl privater Hardware wie z. B. Smartphones samt kommerzieller und privater Software wie z. B. WhatsApp. BYOD beschreibt einerseits das Verhalten der Nutzerinnen und Nutzer, andererseits aber auch eine organisatorische Strategie. Auch hier ist der wichtigste, nutzer:innenfreundliche Vorteil »nur EIN Smartphone«.

Mobile Device Management ist nicht (immer) die beste Lösung

MDM-Lösungen regeln, welche Nutzer:innen gemäß ihrer Rolle in der Organisation auf welche Anwendungen zugreifen darf. Sie sorgen dafür, dass die Installation und der Zugriff auf Apps nur nach den jeweiligen Richtlinien erfolgen. Sie unterstützen Administrator:innen bei der Bereitstellung, Lizenzierung und dem Application Lifecycle Management der mobilen Software. Zudem ist es damit möglich, den Austausch betrieblicher/dienstlicher Daten zwischen mobilen Apps zu kontrollieren und einzuschränken.

Kurzum: Mit einem MDM erhalten Administrator:innen die volle Kontrolle über das komplette Gerät. Doch die reine Verwaltung von Apps oder Endgeräten bietet noch lange keine Sicherheit und löst nicht das Problem der Trennung von privaten und geschäftlichen Daten, wie es die Aufsichtsbehörden vorsehen. Zusätzlich wird die Einführung eines MDMs von Betriebs- und Personalrät:innen meist sehr kritisch – und damit langwierig – geprüft. Das Modell der Zukunft ist ein anderes.

MATERNA
Virtual Solution

Sieben gute Gründe für die Container-Technologie

Schützen, was wertvoll ist – Sicherheits-Modell der Zukunft

Das Modell der Zukunft für die sichere mobile Kommunikation auf Smartphone und Tablet ist die Container-Technologie. Hier sind alle internen Daten – egal, ob auf dem Endgerät, dem Netzwerk oder bei der Übertragung – in einem abgeschotteten und verschlüsselten Bereich. Die Daten von Behörden bzw. Unternehmen befinden sich dann auf dem mobilen Gerät in einer geschützten Umgebung. Privat oder von der Firma gestellt ist dabei unerheblich. Die Container-Technologie gewährleistet zudem die in der DSGVO geforderte strikte Trennung von firmeninternen und privaten Daten. So ist die Privatsphäre ebenso geschützt wie wertvolle Daten der Organisation.

Wie Container-Lösungen funktionieren

Container-Technologie legt den Fokus auf den Schutz der Informationen und Daten auf dem mobilen Endgerät und erweitert das Betriebssystem quasi um eine zusätzliche Sicherheitsschicht. Entsprechende Lösungen ermöglichen die Nutzung von E-Mails, Messenger, Kontakten, Kalender, Netzwerk- und Fachanwendungszugriff, Dokumenten oder auch Notizen und Aufgaben in einem sicheren und verschlüsselten Bereich, dem sogenannten Container. Damit lassen sich die Daten auf dem mobilen Gerät in einer geschützten, abgeschotteten Umgebung bearbeiten und verwalten. Sie sind so vor unbefugten Zugriffen, Verlust oder Manipulation sicher und können nicht unkontrolliert ab- oder einfließen.

DSGVO-konformer Schutz

Container-Lösungen gewährleisten zudem die strikte Trennung von firmeninternen und privaten Daten, wie es die DSGVO vorsieht. Das heißt: Nutzer:innen können aus dem verschlüsselten Bereich heraus nicht auf ihre privaten Apps zugreifen. So verhindert eine Container-Lösung beispielsweise, dass interne Informationen per Copy & Paste auf Facebook oder Twitter landen. Zugleich bleibt die Privatsphäre der Mitarbeiter:innen geschützt. Um die Sicherheit der Datenübertragung zu gewährleisten, verschlüsseln Container-Lösungen ihre Übertragung in der Regel Ende-zu-Ende.

Vorteile der Container-Lösungen im Überblick

+ Einfacher Zugriff auf Organisationsdaten mit Smartphone oder Tablet
+ Unkomplizierte Konfiguration und zügiger Roll-out in jeder Infrastruktur
+ Modernste Datenverschlüsselungstechnologie auf dem Mobilgerät und bei Übertragung
+ Geeignet für COPE- und für BYOD-Szenarien
+ Strikte Trennung von geschäftlichen/dienstlichen und privaten Daten
+ Volle Kontrolle über Organisationsinformationen, ohne die Privatsphäre der Mitarbeiter:innen zu verletzen
+ Effiziente zentrale Verwaltung, aber kein Eingriff in die Gerätekonfiguration

MATERNA
Virtual Solution

Wer profitiert in Ihrer Organisation von der Container-Technologie?

Container-Lösungen erleichtern gleich drei Nutzer:innengruppen den Arbeitsalltag:

1. **Anwender:innen**
2. **IT-Administrator:innen und**
3. **Compliance-Verantwortliche beziehungsweise CISOs.**

Anwender:innen arbeiten sicher, intuitiv und produktiv von überall

Ihre Nutzer:innen profitieren zunächst von der einfachen und schnellen Installation. Sie laden sich die entsprechende Anwendung aus dem App Store oder bei 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 oder aufwendigen Support zurecht. Nach dem Öffnen der App befinden sich die Nutzer:innen 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. Die IT-Abteilung kontrolliert dabei nur den Bereich mit den Unternehmens- bzw. Behördendaten, ohne auf Privates zugreifen zu können.

IT-Administrator:innen behalten die berufliche Datenhoheit

Administrator:innen verwalten die Container-Lösung entweder über ein Management-Portal des Herstellers oder eine bestehende MDM-Lösung. Darüber können sie 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 schnell und einfach festlegen. Natürlich ist es möglich, diese Policies je nach Sicherheitsanforderungen des Unternehmens/der Behörde flexibel anzupassen. So können Administrator:innen beispielsweise den Einsatz von Sprach-Assistenten wie Siri, Fingerabdrucksensoren 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, können Administrator:innen auch die Copy & Paste-, Autovervollständigungs- oder Autokorrekturfunktionen ausschalten.

Die IT-Abteilung bestimmt zentral über die Management-Konsole, wer entsprechend seiner Rolle mit seinem mobilen Endgerät Zugriff auf Organisationsdaten erhält. Dabei kann sie auch Rechte für bestimmte Anwender:innengruppen festlegen. Wenn Mitarbeiter:innen das Unternehmen/die Behörde verlassen, das Gerät verloren geht oder gestohlen wird, lassen sich der Zugang auf und die beruflichen oder dienstlichen Daten in der Container-Lösung sofort löschen. Administrator:innen erhalten so die volle Kontrolle über die Informationen, ohne die Privatsphäre der Mitarbeitenden zu verletzen.

Sicherheits- und Compliance-Verantwortliche setzen Richtlinien konsequent um

Gerade CISOs 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 innerhalb der Container-Lösung und auch bei der Übertragung State of the Art verschlüsselt. Mit entsprechenden Gateways sind auch die zentralen Kommunikationsserver über Mobilgeräte nicht mehr direkt aus dem Internet erreichbar und Man-in-The-Middle-Attacken lassen sich wirkungsvoll verhindern.

Der wohl größte Vorteil: Die beruflichen Daten und private Informationen sind auf ein und demselben Endgerät strikt voneinander getrennt. Damit eignen sich Container-Lösungen für COPE- und BYOD-Szenarien sowie Organisationen, die sehr großen Wert auf die mobile Sicherheit ihrer Daten und den Schutz der Privatsphäre von Mitarbeiter:innen, Kund:innen oder Bürger:innen legen. Und Betriebs- oder Personalräte erteilen bei der Einführung meist sehr zügig ihre Zustimmung.

MATERNA
Virtual Solution

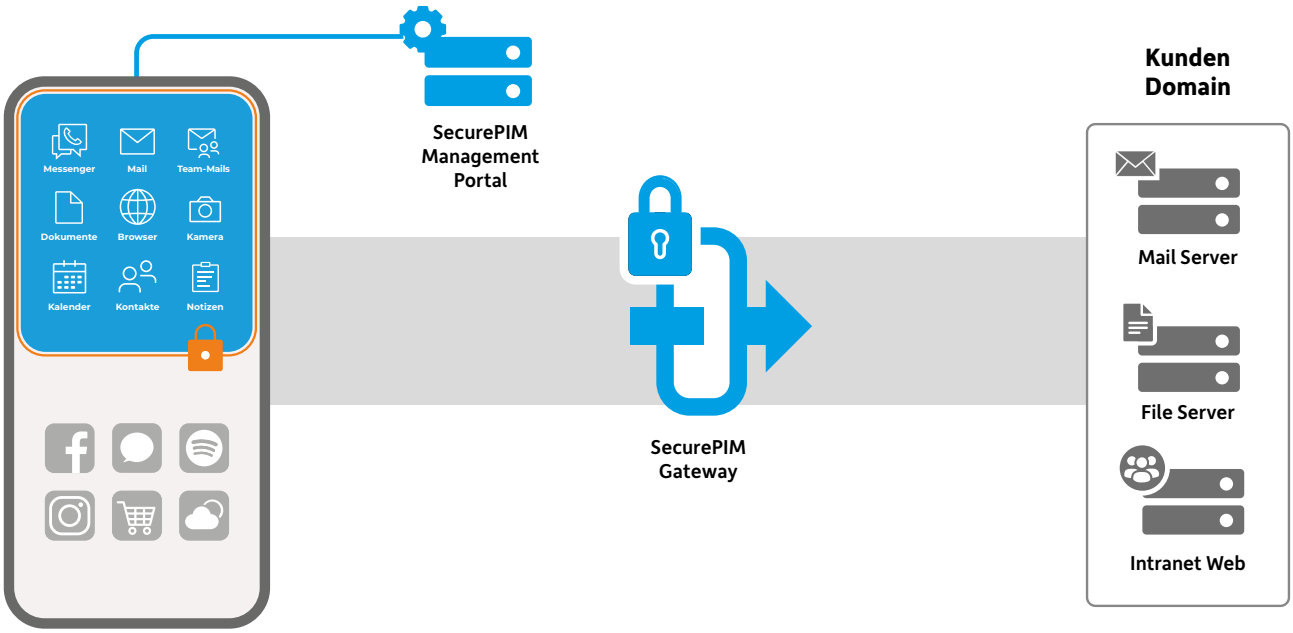
Container-Lösungen schützen effektiv – wenn es die richtigen sind

Bei der Auswahl einer Container-Lösung sollten IT-Entscheider:innen ein genaues Augenmerk auf einige wichtige Aspekte haben. Eine geeignete Anwendung sollte nicht nur auf einem unabhängig geprüften Sicherheits-Framework basieren. Sie sollte auch:

+ einfach zu bedienen sein
+ eine performante Verbindung zwischen Client und Server herstellen können – ganz ohne VPN
+ die neuesten kryptografischen Standards einsetzen und
+ die Option für hardwarebasierte Sicherheit mit Smartcards unterstützen

Intuitive Usability erleichtert Einsatz und Nutzung von Container-Lösungen

Sicherheit hin oder her – was nicht intuitiv und komfortabel ist, werden Nutzer:innen nicht verwenden. Deshalb unsere Empfehlung: Achten Sie darauf, dass Ihre Container-Lösung als App sowohl für iOS- als auch Android-Geräte optimiert und zugelassen ist. Die Nutzer:innenoberflächen sollten sich nach Möglichkeit an nativen Apps orientieren. Auf diese Weise profitieren viele Mitarbeiter:innen und die IT-Abteilung auch bei hybriden OS-Landschaften und Mischmodellen (COPE & BYOD).



Direkte Verbindung zwischen Smartphone und Server für schnelle Datenübertragung

Die Verbindung zwischen dem Client und dem Mail-Server sollte direkt und ohne Umleitung über ein Network Operations Center erfolgen, um eine hohe Verfügbarkeit und Geschwindigkeit bei der Datenübertragung zu gewährleisten. Eine Container-App sollte daher etwa den Microsoft Exchange Server mit ActiveSync oder HCL Domino unterstützen und über ein sicheres Gateway Verbindung zu Fileshare sowie Intranet aufbauen. So können Mitabeiter:innen effizient arbeiten, da der unkomplizierte Zugriff von überall sichergestellt ist. Ganz ohne VPN.

Einsatz von zertifizierten Krypto-Standards für optimalen Datenschutz

Der Anbieter einer Container-Lösung sollte keine eigenen Verschlüsselungsalgorithmen entwickeln, sondern auf bewährte Krypto-Standards wie S/MIME, AES-256, SHA-256 oder Elliptic Curve setzen. Aufgepasst: RSA-2048 wird vom Bundesamt für Sicherheit in der Informationstechnik als nicht mehr sicher klassifiziert. Und auch der Nachfolger RSA-4096 eignet sich aus anderen Gründen nicht: Bedingt durch die hohe Schlüssellänge steigen Speicherverbrauch und Prozessornutzung stark an. Gerade bei Geräten wie Smartphones können die allgemeine Leistung und Usability leiden.

Smartcard-Option für hardwarebasierte Sicherheit

Für Behörden oder auch Unternehmen, die höhere Sicherheitsanforderungen haben, reicht die Authentifizierung per Passwort oder biometrische Verfahren oft nicht aus. Sie setzen daher zusätzlich auf externe Sicherheitselemente, insbesondere Smartcards. Eine Container-Lösung sollte Smartcards als zusätzliche Sicherheitsoption unterstützen und sicherheitsrelevante Prozesse wie die Entschlüsselung von Daten auf die Smartcard verlagern können.

Ein Beispiel: Die Smartcard speichert einen nicht duplizierbaren Schlüssel. Die IT-Administrator:innen bemerken, wenn dieser Schlüssel verloren geht und können so den unberechtigten Zugriff auf das Organisationsnetz verhindern.

MATERNA
Virtual Solution

SecurePIM von Materna Virtual Solution: Alles sicher in einer App

SecurePIM ermöglicht es Mitarbeiter:innen, überall und jederzeit produktiv zu sein. Die Kommunikationslösung schottet E-Mails, Messaging, Kontakte, Kalender, Netzwerk- und Intranet-Zugriff, Dokumente, Notizen und Aufgaben auf mobilen iOS- sowie Android-Geräten in einem verschlüsselten Containerbereich ab. Die Authentifizierung erfolgt via Passwort, PIN oder biometrische Verfahren. Für höchste Sicherheitsansprüche natürlich auch mit Smartcards.

Gut für Nutzer:innen & Adminstrator:innen

SecurePIM bietet alle relevanten Funktionen in einer abgeschotteten App. Das freut Anwender:innen, denn sie arbeiten effizient und ohne Technologiebrüche mit dem Betriebssystem ihrer Wahl. Ein Beispiel: Sie können aus dem Chat heraus direkt auf Dokumente im Netzwerk zugreifen, diese bearbeiten und dann per E-Mail versenden. IT-Profis verhindern so wirksam eine riskante Schatten-IT und können eine plattformübergreifende, ressourcenschonende Verwaltung sicherstellen. Auch Konfiguration und Roll-out sind einfach – dank Selbstbedienung der Nutzer:innen aus dem App Store oder Google Play. Die Installation eines MDM-Profils ist nicht notwendig, die Kombination mit einem vorhandenen MDM-System aber problemlos möglich. So lässt sich die Lösung in nahezu jede Infrastruktur schnell integrieren.

Zwei Komponenten für noch mehr Flexibilität & Performance

Das SecurePIM Management Portal sorgt für zusätzliche Flexibilität, da es Administrator:innen erlaubt, Sicherheitsregeln einfach festzulegen und die Nutzer:innen zentral zu verwalten. Beispielsweise lassen sich Passwortlängen und Funktionen, wie das Verbot von einfachem Kopieren innerhalb der App zügig im Portal konfigurieren. Das SecurePIM Management Portal sorgt so dafür, dass Organisationen gesetzlich vorgegebene Compliance-Regeln einfach und zügig umsetzen können.

Das SecurePIM Gateway sichert die Verbindung der App zum zentralen Kommunikationsserver und ins organisationsinterne Netzwerk ab. Administrator:innen können es zügig installieren, einfach verwalten und so Betriebsaufwände senken. Das Beste: Dank Authentifizierung durch Zertifikate sind weder VPN noch MDM nötig. Das Mobilgerät wird so ein Teil des Firmennetzwerks – der Exchange-Server ist vom Internet abgeschottet und deutlich besser geschützt.

Warum Sie sich für SecurePIM entscheiden sollten:

+ **Hohe Nutzer:innenfreundlichkeit:** ohne großen Schulungs- und Verwaltungsaufwand für Mitarbeiter:innen und Administrator:innen
+ **BSI-geprüft:** alle SecurePIM-Varianten basieren auf SERA, einer vom BSI geprüften und zugelassenen Sicherheitsarchitektur
+ **Umfassender Geheimnisschutz nur mit SecurePIM:** Mobiles Arbeiten für Behörden und sicherheitsbetreute Industrie bis zu VS-NfD & NATO RESTRICTED
+ **Out-of-the-box DSGVO-konform:** Schützt persönliche Daten und vermeidet Strafzahlungen und Reputationsverlust bei DSGVO-Verstößen
+ **Zukunftssicher:** die plattformunabhängige Container-Technologie kann auch bei einem Gerätewechsel z. B. von iOS zu Android zum Einsatz kommen
+ **Flexibel:** der Mischbetrieb von BYOD- und COPE-Modellen ist durchgängig möglich

Sie möchten in Ihrer Bundes-, Landes- oder Kommunalbehörde sicher von unterwegs mit SecurePIM Government arbeiten? Oder wollen Sie Ihre Unternehmensdaten mit SecurePIM Enterprise vor unbefugten Zugriffen schützen? Lassen Sie uns über Ihre Anforderungen sprechen!

kontakt@virtual-solution.com
T +49 89 30 90 57-0

MATERNA
Virtual Solution

Über Materna Virtual Solution

Materna Virtual Solution, ein Unternehmen der Materna-Gruppe, ist ein auf sichere mobile Anwendungen spezialisierter Softwarehersteller mit Sitz in München und Entwicklungsstandort in Berlin.

Das Unternehmen entwickelt und vertreibt die Applikationen SecurePIM, SecureCOM und die Sicherheitsarchitektur SERA für iOS und Android. SecurePIM ermöglicht verschlüsseltes und benutzerfreundliches mobiles Arbeiten. Behörden können mit Smartphones und Tablets auf Geheimhaltungsstufe VERSCHLUSSSACHE – NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) und auf der Sicherheitsstufe NATO RESTRICTED kommunizieren.

Für Unternehmen stellt SecurePIM die Anforderungen der Datenschutzgrundverordnung (DSGVO) auf mobilen Geräten sicher und senkt damit die Risiken strafbewährter DSGVO-Verstöße und des Verlustes von Unternehmensdaten.

Materna Virtual Solution wurde 1996 gegründet und beschäftigt rund 100 Mitarbeiter:innen. Alle Produkte der Materna Virtual Solution tragen das Vertrauenszeichen »IT-Security made in Germany« des TeleTrust-IT-Bundesverbandes IT-Sicherheit e.V.

P-23.0022_Whitepaper_Container Technologie_de/de_v5_01/23

MATERNA
Virtual Solution

Materna Virtual Solution GmbH
Blutenburgstraße 18 · 80636 München · T +49 89 30 90 57-0
kontakt@virtual-solution.com · www.materna-virtual-solution.com