

Mobile Security im Einklang mit DSGVO und BSI

Leitfaden zur DSGVO-konformen Smartphone- und Tablet-Nutzung nach BSI-Standards

Ein White Paper der Cortado Mobile Solutions GmbH



Inhalt

Einleitung	3
1 Höheres Cyberrisiko in verteilten Umgebungen.....	3
2 Auszüge aus der BSI-Studie	4
Angriffe während der Homeoffice-Zeit	4
Technologien zur Gefahrenabwehr	4
Gemischte IT-Ausstattung	6
Fünf einfache Maßnahmen für mehr IT-Sicherheit im Homeoffice	6
3 Sicherheit mobiler Endgeräte	7
4 Mobile Device Management	8
Automated Device Enrollment und Zero-Touch	8
5 Bedrohungen mit MDM abwehren	9
Fehlende Betriebssystem-Updates	9
Software-Schwachstellen in vorinstallierten Apps.....	9
Manipulation von Endgeräten/Schadprogramme	9
Webbasierte Angriffe auf mobile Browser	10
Missbrauch sensibler Daten im Sperrbildschirm	10
Gefahren durch private Nutzung mobiler Geräte.....	10
Gefahren durch BYOD	11
Deaktivieren von Sicherheitsfunktionen (Android)	11
Risikokonzentration durch ein Apple-ID für alle Apple Dienste (iOS)	11
6 Zusammenfassung.....	12

Einleitung

In seinem aktuellen **IT-Grundschutz-Kompendium** (Edition 2023) befasst sich das Bundesamt für Sicherheit in der Informationstechnik (BSI) u.a. mit Sicherheitsaspekten beim Umgang mit mobilen Endgeräten im geschäftlichen Einsatz. Das vorliegende White Paper beschreibt verschiedene Möglichkeiten der Implementierung der aktuellen BSI-Empfehlungen mit den Mitteln eines Mobile-Device-Management-Systems.

1 Höheres Cyberrisiko in verteilten Umgebungen

Die Corona-Pandemie hat in den vergangenen Jahren zu deutlichen Veränderungen im Arbeitsumfeld geführt. Unternehmen sahen sich gezwungen, angesichts der Homeoffice-Pflicht die Digitalisierung und eine grundsätzliche Modernisierung ihrer IT-Infrastruktur voranzutreiben. Gleichzeitig offenbarten sich mit der Heimarbeit neue Schwachstellen und Sicherheitslücken. Organisatorisch-technische Herausforderungen waren angesichts der verteilten Umgebungen mit Büro und Homeoffice zu meistern.

Sichere Infrastrukturen sind wichtiger als je zuvor, denn hybride Arbeitsmodelle sind auch nach der Pandemie Bestandteil in sehr vielen Unternehmen. Der Anteil an mobilen Geräten – vom Smartphone über das Tablet bis zum Notebook –, an denen Beschäftigte einen Großteil ihrer Arbeit erledigen, wird weiter ansteigen. Doch nach wie vor gibt es in vielen Unternehmen keine konkrete Vorstellung davon, wie diese Geräte in die Unternehmens-IT einzubinden sind bzw. wie ein Sicherheitskonzept grundsätzlich auszusehen hat, das mobile Geräte angemessen einbindet. Solche Konzepte hören längst nicht mehr beim Arbeitsplatz-PC auf, sondern müssen weitergedacht werden. Sowohl die Verwaltung rein geschäftlicher Endgeräte als auch solcher, die privat und geschäftlich genutzt werden, gilt es zu regeln.

Der starke Trend hin zur Mobilität wird sich in den kommenden Jahren fortsetzen. Bis Ende 2023 werden im Smartphone-Markt 1,5 Milliarden mobile Geräte¹ im Umlauf sein, mit überwältigender Dominanz (über 99 %) von Google und Apple. Mit Android laufen mittlerweile mehr als 7.000 unterschiedliche Gerätetypen von Hunderten von Herstellern. Gleichzeitig ist in den chinesischen Markt durch die Abspaltung des Google-Betriebssystems Bewegung gekommen; zusätzlich gibt es nationale Einzellösungen wie in Russland AuroraOS für Regierungseinrichtungen. Diese Erscheinungen sind aber zu vernachlässigen und angesichts der aktuellen geopolitischen Lage ohnehin noch einmal gesondert zu betrachten.

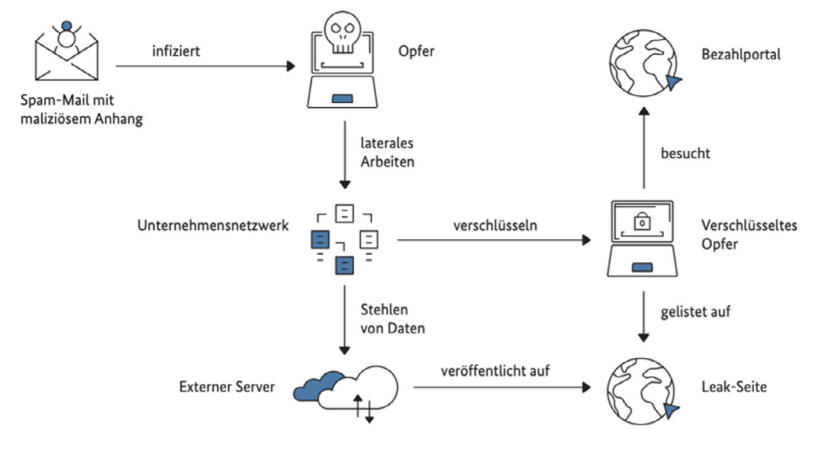
Tatsache ist, dass immer mehr Unternehmen mobile Endgeräte einsetzen, um ihren Beschäftigten ein flexibleres Arbeiten zu ermöglichen. Werden diese in Homeoffices eingesetzt, erwachsen daraus neue Risiken, denn Heimarbeitsplätze stellen für die Cybersicherheit eine besondere Herausforderung dar.

¹ IDC, Worldwide Business Use Smartphone Forecast Update, 2019–2023

2 Auszüge aus der BSI-Studie

Jedes Jahr veröffentlicht das BSI „Die Lage der IT-Sicherheit in Deutschland“. Auch in dem Bericht vom Oktober 2022 bleibt die Cyber-Erpressung eine der größten Bedrohungen und nimmt sogar weiter zu. Ziel der Angreifer ist dabei die Verschlüsselung oder Exfiltration von Daten, um dann von den betroffenen Unternehmen Löse- oder Schweigegeldzahlungen zu erpressen. Dass dies nicht nur für Unternehmen, sondern eben auch für öffentliche Verwaltungen schnell zum Problem werden kann, zeigt der folgenschwere Angriff auf die Landeskreisverwaltung Sachsen-Anhalt, welche als Konsequenz den Katastrophenfall ausrufen musste.

Diese Grafik des BSI zeigt einen beispielhaften Angriffsablauf:



Beispielhafter Ablauf eines Ransomware-Angriffs mit Löse- und Schweigegelderpressung (schematische Darstellung) Quelle: BSI

Eine weitere Studie des BSI zeigt, wie Unternehmen mit dem Thema „Cybersicherheit und verteilte Arbeitsplätze“ umgehen. Dazu wurden zwischen Oktober und November 2020 1.000 Personen aus kleinen, mittleren und großen Unternehmen in Deutschland befragt. Fazit: Sicherheit wird vernachlässigt.

Angriffe während der Homeoffice-Zeit

Acht Prozent der befragten Unternehmen hatten mit Cyberangriffen auf ihre IT-Infrastruktur zu kämpfen und mussten entsprechend reagieren, bei den Großunternehmen waren es sogar 24 Prozent. Ein Viertel der Angriffe wurde als existenzbedrohend eingestuft, da sehr schwere Schäden verursacht wurden, insbesondere bei Kleinstunternehmen.

Technologien zur Gefahrenabwehr

Folgende Komponenten empfiehlt das BSI, um in hybriden Arbeitsumgebungen zu einem höheren Schutzniveau zu kommen. Sie werden von Unternehmen unterschiedlich umgesetzt.

Mobile Security im Einklang mit DSGVO und BSI

1. Einrichten von Virtual Private Networks (VPN)
2. Verschlüsselung von Datenträgern
3. Mehr-Faktor-Authentisierung
4. Segmentierung und Absicherung von Netzen
5. Mobile Device Management (MDM)

VPN-Lösungen hatten bereits vor Corona 55 Prozent der befragten Unternehmen eingesetzt, elf Prozent hatten dies während der Krise nachgeholt. Ähnlich die Entwicklung bei der Verschlüsselung von Datenträgern (59 Prozent/fünf Prozent). Mehr-Faktor-Authentisierung war bei 42 Prozent vor der Krise bereits ein Thema, währenddessen setzten sich 10 Prozent damit auseinander. Die Segmentierung und Absicherung von Netzen liegen mit 43 Prozent bzw. acht Prozent nahezu gleichauf.

Nur 29 Prozent der Unternehmen hatten bereits vor 2020 mit dem Thema Mobile Device Management praktische Erfahrungen gesammelt, neun Prozent begannen während der Pandemie, sich damit zu beschäftigen. In diesem Technologiesegment besteht also noch deutlicher Aufholbedarf: Nur 38 Prozent der Endgeräte mit Verbindung zum Firmennetz sind überhaupt einer zentralen Verwaltung durch ein MDM unterworfen. Zwar planen zwölf Prozent dessen Einsatz, doch dies bedeutet nach wie vor: Für die Hälfte der Unternehmen ist Mobile Device Management auch mittelfristig kein Thema.

Angesichts der sich weiter perpetuierenden Homeoffice-Situation stehen damit Tausende von Unternehmen vor einem eklatanten Sicherheitsrisiko, das aus der Verwendung mobiler Geräte resultiert. Das BSI empfiehlt grundsätzlich, auf den Einsatz privater IT möglichst zu verzichten. Insbesondere die langfristige Perspektive für einen stärkeren Ausbau von Homeoffice-Plätzen zeige, wie wichtig passgenaue Sicherheitslösungen an dieser Stelle seien. In genau diese Lücke stößt MDM: Es erlaubt auch die sichere Nutzung von privaten Endgeräten im Unternehmen.



Gemischte IT-Ausstattung

39 Prozent der vom BSI befragten Unternehmen gaben an, dass bei ihnen auch private IT (sprich Smartphones/Notebooks) zum Einsatz kommt. Ein IT-Sicherheitskonzept darf sich daher nicht auf Unternehmens-IT fokussieren, sondern muss auch private IT einbeziehen und Regelungen für Bring Your Own Device (BYOD) beinhalten. Selbst wenn vom Handy aus nur einmal kurz einige geschäftliche E-Mails abgerufen werden – auch solche Betriebsmodi müssen berücksichtigt werden, werden jedoch bislang stark vernachlässigt.

Dies spiegelt sich in gefährlich niedrigen Budgets für Cybersicherheit wider. Das BSI empfiehlt, 20 Prozent des IT-Budgets für Cybersicherheit auszugeben. Laut Studie investieren aber 55 Prozent der Unternehmen nur bis zu zehn Prozent in diesen Bereich. Die Befragung ergab ferner: Für 68 Prozent der Unternehmen ist es eher oder sehr wichtig, dass IT-Lösungen oder Anlagen – insbesondere solche, die Teil einer Sicherheitsinfrastruktur sind – in Deutschland oder der EU entwickelt werden.

Fünf einfache Maßnahmen für mehr IT-Sicherheit im Homeoffice

Das Sicherheitsniveau in hybriden Arbeitsumgebungen mit mobilen Endgeräten im Einsatz lässt sich allgemeinen Empfehlungen zufolge durch fünf einfache Maßnahmen erhöhen.

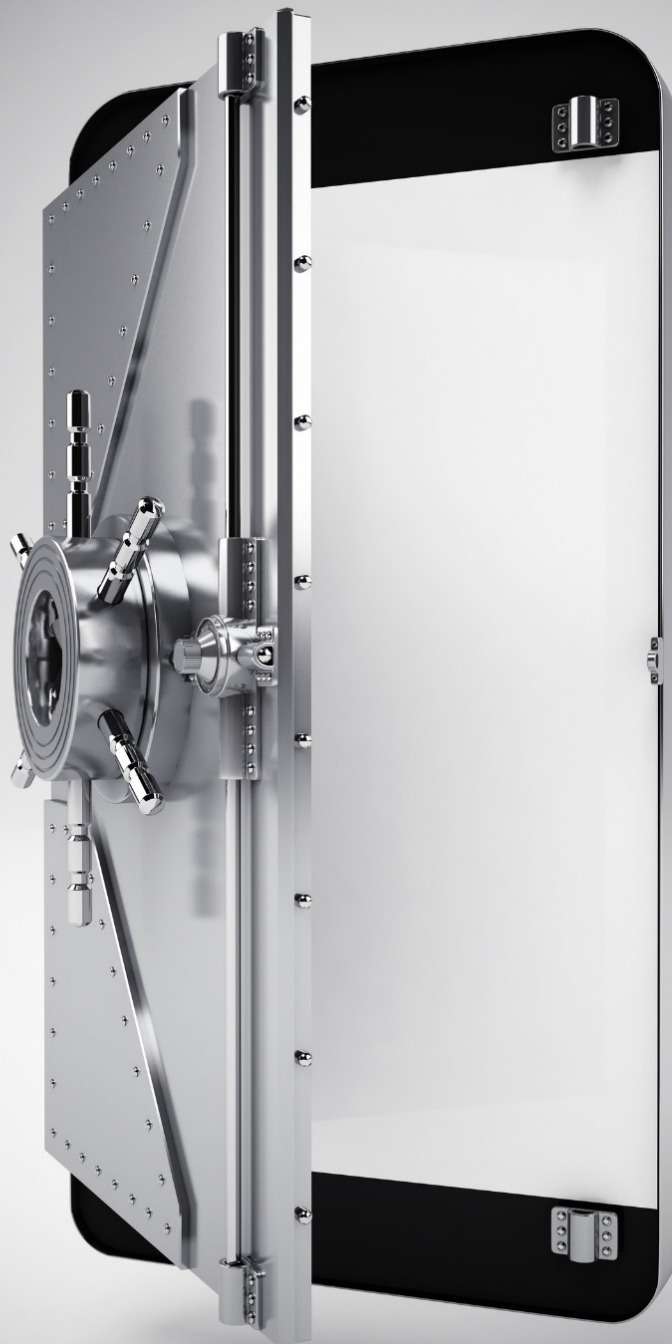
1. Einrichtung eines VPN
2. Einsatz von Mehr-Faktor-Authentisierung
3. Nutzung eines MDM-Systems
4. Regelmäßige Updates
5. Hinzuziehen qualifizierter Dienstleister

Das BSI rät zusätzlich, mindestens 20 Prozent der IT-Ausgaben für Security zu verwenden sowie den BSI-IT-Grundschutzkatalog zu berücksichtigen.



3 Sicherheit mobiler Endgeräte

Bedrohungen entstehen auf mehreren Ebenen des Sicherheitskonzeptaufbaus bei mobilen Betriebssystemen (der sog. „Chain of Trust“) – beginnend bei Firmware und Kernel der Hardware über Datei- und Betriebssystem, Apps und Sandboxes bis zum User Interface. Jede Schicht baut dabei auf der anderen auf und die Kette ist nur dann intakt, wenn zwischen jeder Schicht Integrität besteht. Auf jeder Stufe lassen sich unterschiedliche Angriffsvektoren ausmachen, wobei man zwischen Angriffen auf Hardware (Zugriff auf Speicher, SIM-Karte etc.), auf Software (Exploits) sowie dem Risikofaktor „User“ (d.h. Administratoren, Support oder auch Sachbearbeitende, die Anwendungen falsch benutzen oder auch falsch einstellen) unterscheidet. MDM minimiert die Sicherheitsrisiken, denen Unternehmen durch diese Vektoren ausgesetzt sind.



4 Mobile Device Management

Unter Mobile Device Management versteht man ein System zur Verwaltung und automatisierten Durchsetzung unternehmensweit einheitlicher Vorgaben auf Endgeräten, unter anderem für

- › Geräteadministration (z.B. Kamera ein/aus)
- › Einstellung von Profilen (z.B. WiFi, Exchange, VPN, Zertifikate)
- › Anwendungsmanagement (verteilen und konfigurieren von APP's)
- › Umsetzung von Compliance-Richtlinien (z.B. Passcodelinien)
- › Fernlöschung und Fernsperrung

Eine MDM-Lösung kann im Rahmen vorgegebener Richtlinien diverse Einstellungen auf dem Gerät einschränken, etwa WiFi/Bluetooth-Funktionalität, Accountverwaltung, Sicherheit (Passcode, Sperrbildschirm), Nutzung von App-Stores, Browsereinstellungen (Cookies, Popups), Assistenten oder Cloud-Synchronisation. Sie nimmt des Weiteren häufig sogenannte Profil-Konfigurationen auf den Geräten vor, zumeist in den Bereichen WiFi, Zertifikate, E-Mail-Konten und VPN.

Anwendungsmanagement betrifft sämtliche Aktivitäten rund um die App-Verwaltung. Hier werden verwaltete, erzwungene und optionale Apps festgelegt, ihre Installation, Deinstallation sowie Updates angestoßen und Vorkonfigurationen für die App getroffen (z.B. Serveradresse + Username).

Mobile Device Management sorgt dafür, dass die Compliance-Vorgaben des Unternehmens eingehalten werden. So können Geräte gesperrt werden (kein Zugriff mehr auf Unternehmensressourcen), wenn z.B. Vorgaben zur Passcode-Komplexität (Länge der PIN) nicht eingehalten werden, Geräte den regelmäßigen Kontakt zum MDM-System verlieren, verpflichtende Apps nicht installiert oder Betriebssystem-Updates abgelehnt bzw. zu häufig verschoben werden.

Automated Device Enrollment und Zero-Touch

Große Stückzahlen von Geräten können über ein MDM-System einfach eingerichtet bzw. über zertifizierte Reseller/Distributoren erworben werden. Sie werden dann beim Einschalten automatisiert initial vorkonfiguriert und in das MDM eingebracht, ohne dass noch jemand Hand anlegen muss.



5 Bedrohungen mit MDM abwehren

Das IT-Grundschutz-Kompendium des BSI (Edition 2023) befasst sich mit den Bedrohungsszenarien für mobile Geräte eingehend in den Abschnitten SYS.3.2.1 (Allgemeine Smartphones und Tablets), 3.2.2 (MDM), 3.2.3 (iOS for Enterprise) und 3.2.4 (Android). Eine Auswahl der gängigsten Szenarien und wie man ihnen mit MDM begegnet wird im Folgenden dargestellt.

Fehlende Betriebssystem-Updates

OS-Exploits sind etwa möglich, indem jemand über eine präparierte SMS die Kontrolle über Geräte erlangt oder Roots (Erlangen erweiterter [Administrator-]Rechte auf Android-Geräten) bzw. Jailbreaks (Veränderung des iOS zum Einbau bestimmter Funktionen) durchführt. Wie man dieser Problematik begegnet, hängt vom Betriebsmodus ab. Bei BYOD-Devices, d.h. auf privaten Mitarbeitergeräten, lässt sich ein OS-Update nicht erzwingen, jedoch kann man den separaten Arbeitsbereich auf dem Gerät sperren. Gibt es spezielle Apps, in denen Lücken auftreten, können diese deinstalliert oder ausgesperrt werden. Anders sieht es bei voll verwalteten Geräten aus, also reinen Firmenhandys. Hier haben Unternehmen die volle Möglichkeit, Updates einzuplanen und zu erzwingen. So sind die Geräte immer auf dem neuesten Patch-Level.

Software-Schwachstellen in vorinstallierten Apps

Angriffsszenario: Apps, die in Arbeitsbereichen mit Schwachstellen eingesetzt werden, eröffnen potenziell die Möglichkeit, auf Unternehmensdaten zuzugreifen. Dies wäre z.B. bei Apps mit externen Drittanbieter-Bibliotheken der Fall, die veraltet sind bzw. Schwachstellen enthalten, die der App-Hersteller noch nicht aktualisiert hat. Vorinstallierte Apps weisen zudem unter Umständen erhöhte Ausführungsrechte auf (zum Beispiel iOS Mail).

Schutzmaßnahmen mit MDM (gilt für BYOD wie für voll verwaltete Geräte gleichermaßen):

- Einrichten von Sperr- und Erlaubt-Listen für Apps
- Etablieren eines Review- und Freigabe-Prozesses im Anwendungsmanagement, der regelt, unter welchen Bedingungen Apps in den Enterprise App Store aufgenommen werden dürfen
- Einrichten eines Threat-Prevention-Systems (vergleichbar mit Reputation Services). Mit einer solchen Drittanbieter-Lösung lässt sich die Reputation von Apps anhand von Machine Learning bewerten und dafür sorgen, dass bestimmte Apps erst gar nicht auf den Geräten installiert werden.

Manipulation von Endgeräten/Schadprogramme

Angriffsszenarien sind hier Phishing oder Browser Exploits. Diese sind auf mobilen Browsern allerdings noch nicht so häufig zu beobachten wie bei klassischen Desktop-Systemen.

Schutzmöglichkeiten sind bei BYOD-Geräten begrenzt. Bestenfalls lassen sich über das Anwendungsmanagement die unterschiedlichen Browser auswählen, welche eingesetzt werden sollen und diese entsprechend

konfigurieren. Bei voll verwalteten Geräten sind die Möglichkeiten größer: Da iOS auch Managed Domains einsetzt, kann man über Web-Proxy unternehmenskritische Ressourcen sicher ansprechen. Ebenfalls einen Sicherheitsbeitrag leisten kann VPN, über das man bestimmte Netze ausschließlich anspricht.

Webbasierte Angriffe auf mobile Browser

Solche Angriffe treten bislang noch selten auf. Das Angriffsszenario besteht in der Installation von Proxys, Keyloggern, Drittanbieter-Tastaturen oder Apps mit Telefonie- und SMS-Zugriff. Schutzmaßnahmen (bei BYOD- und voll verwalteten Geräten) wären das Einsetzen globaler Web-Proxys, Anwendungsmanagement oder von Threat-Prevention-Systemen.

Missbrauch sensibler Daten im Sperrbildschirm

Auf dem Sperrbildschirm erscheinen auf den Systemen häufig Unternehmensdaten, die dort nicht hingehören: angefangen von E-Mails bis hin zu Kurznachrichten oder Dateinamen. Auch die Möglichkeit, Assistenten zu aktivieren, die Rechte auf dem System haben (Abrufen aktueller Termine oder Vorlesen von E-Mails) gehört zum Angriffsszenario. Schutzmaßnahme (BYOD- und voll verwaltete Geräte): Solche Informationen dürfen nicht angezeigt werden, Assistenten müssen deaktiviert werden.

Gefahren durch private Nutzung mobiler Geräte

Dadurch, dass geschäftliche Daten abfließen und Beschäftigte gleichzeitig mehr Software in ihre mobilen Geräte einbringen (worunter sich dann auch Schadsoftware oder unerlaubte Apps befinden können), eröffnet sich hier ein sehr breiter Angriffsvektor.

Bei BYOD-Geräten lässt sich als Schutzmaßnahme der Arbeitsbereich, der durch die Betriebssystem-Mechanismen stark geschützt ist, bei potenziellen Angriffen sperren. Über das Anwendungsmanagement kann man festlegen, welche Apps installiert werden dürfen. Mittels Container-Technologie und separaten Partitionen lassen sich private von geschäftlichen Apps und Daten trennen. In der Datenflusssteuerung kann zudem festgelegt werden, in welche Richtung Datenflüsse zwischen privatem und geschäftlichem Bereich zugelassen werden.

Voll verwaltete Geräte lassen sich durch Einsatz von VPN und Web-Proxys schützen. Allerdings wird die private Nutzung eher bei BYOD-Geräten der Fall sein. So genannte COPE-Geräte, die dem Unternehmen gehören, aber auch für privaten Einsatz freigegeben werden, kann man wiederum per VPN oder Web-Proxy schützen.

Gefahren durch BYOD

Angriffsszenario: Der Nutzer hat die Kontrolle über sein Gerät und damit das volle Portfolio an Möglichkeiten: Roots/Jailbreaks, Anzapfen geschäftlicher Datenquellen, Einbringen von Schadsoftware, Installieren unerlaubter Apps. Außerdem hat er Hardwarezugriff.

Schutz funktioniert hier nur mittels Mobile Device Management über die Betriebssystem-Mechanismen, die sich sowohl bei Android als auch bei iOS in den letzten Jahren deutlich verbessert haben. Bei ausreichender Trennung von Apps und Daten sowie einer guten Datenflusssteuerung kommt man bereits zu einem hohen Schutzniveau, mit dem man guten Gewissens BYOD-Geräte einsetzen kann.

Deaktivieren von Sicherheitsfunktionen (Android)

Angriffsszenario ist hier das bekannte Entsperren des Bootloaders zur Installation eines Custom ROMs. Werden die Entwickleroptionen via MDM deaktiviert, ist dies allerdings inzwischen nicht mehr so einfach durchzuführen. Zusätzlich ist es durch Einsatz der Android Factory Reset Protection heute möglich – analog zu Apple – nach Diebstahl oder Verkauf des Gerätes die Eingabe des bisherigen Google Kontos zu verlangen, bevor man sich überhaupt mit einem anderen Konto anmelden kann.

Risikokonzentration durch ein Apple-ID für alle Apple Dienste (iOS)

Hier besteht das Angriffsszenario aus dem unbefugten Zugriff auf iCloud-Daten durch nicht ausreichend abgesicherte Apple-IDs im geschäftlichen Einsatz. Setzen also Beschäftigte Apple-IDs im geschäftlichen Umfeld ein und wählen dort schwache Passwörter, gibt es potenziell ein Problem. Schutzmaßnahme (BYOD- und voll verwaltete Geräte) ist die Nutzung von verwalteten Apple IDs mit dem Apple Business Manager und konfigurierter föderativer Authentifizierung. Auf diese Art gelangt man zu besserer Kontrolle über die Qualität der Authentifizierung. Über die Anbindung des Azure AD oder Zwei-Faktor-Authentisierung lässt sich zudem der Zugang der verwalteten Apple IDs besser absichern.



6 Zusammenfassung

Die Digitalisierung der Arbeitswelt unter Einbeziehung mobiler Endgeräte schreitet immer weiter voran. Im Zuge dessen erhöht sich auch die Gefährdung durch Cyberangriffe auf Unternehmen. MDM kann hier, so auch die Einschätzung des BSI, einen wichtigen Baustein eines IT-Sicherheitskonzeptes darstellen. An BOYD als Betriebsmodell kommt heute kein Unternehmen vorbei, denn die wenigsten haben während der Homeoffice-Zeit für all ihre Beschäftigten eigene Geräte angeschafft. Deshalb ist es notwendig und ratsam, eine Security-Strategie für gemeinschaftlich privat sowie geschäftlich genutzte Geräte zu entwickeln. Liegt diese vor, können auch private Geräte sicher und effektiv für Unternehmenszwecke eingesetzt werden.

Der IT-Grundschutzkatalog des BSI liefert einen guten Leitfaden dafür, was ein hohes Schutzniveau ausmacht. Konkrete Empfehlungen gibt es vom BSI nicht, allerdings gibt es Umsetzungsempfehlungen für iOS (SYS.3.2.3 iOS for Enterprise) und Android (SYS.3.2.4 Android). Im MDM-System von Cortado lassen sich deshalb für jeden Account konkrete Richtlinienvorlagen vorkonfigurieren. Etwa eine strikte DSGVO-Policy mit Empfehlungen, die sich als Basisvorlage nutzen lässt. Es besteht ferner die Wahl zwischen verschiedenen Abstufungen des Schutzniveaus (einfach, mittel, hoch). Cortado entwickelt seine deutschsprachigen Lösungen in Berlin datenschutzkonform nach DSGVO.



Kostenlos testen!

Starten Sie jetzt und entdecken Sie Mobile Device Management mit Cortado MDM. Ihre MDM-Konsole ist nach Ihrer Anmeldung umgehend startbereit.

- › Einfach anmelden und 14 Tage testen – kostenlos und unverbindlich
- › Keine Kreditkarte oder andere Zahlungsdaten erforderlich
- › Ihr Probeabo endet automatisch mit Ablauf der Testzeit

Kostenlos testen

..... Headquarters

Cortado Mobile Solutions GmbH

Alt-Moabit 91 a
10559 Berlin, Germany
Tel.: +49 (0)30 408 198 500
Fax: +49 (0)30 408 198 501
E-Mail: info@cortado.de
www.cortado.de

Cortado Pty Ltd.

..... Australia

ThinPrint Australia
Level 10, 20 Martin Place
Sydney NSW 2000
Australia
Tel.: +61 2 8079 2989

..... USA (Colorado)

Cortado, Inc.

3827 Lafayette St #130
Denver, CO 80205
USA
Tel.: +1 303 487 1302
E-mail: info@cortado.com
www.cortado.com

Cortado Japan

..... Japan

6F Shinmakicho Building
1-8-17 Yaesu
Chuo-ku Tokyo
Post Code 103-0028
Japan
Tel.: +81 3 5542 1551



Alle Namen und Warenzeichen sind Namen und Warenzeichen der jeweiligen Hersteller.

Folgen Sie Cortado auf:



facebook



twitter



youtube



linkedin