Projektdokumentation

Fachinformatiker für Systemintegration
Abschlussprojekt Sommer 2016

Mobile Device Management (MDM)

Zentralisierte Verwaltung von Mobilgeräten

Projektausführender:

Urs Luhmann
21.05.1970
49393 Lohne
Ausbildungsberuf: Fachinformatiker Systemintegration

Projektbetrieb:

große Austing GmbH
Bergweg 26
49393 Lohne

Ausbildungsbetrieb:

große Austing GmbH
Bergweg 26
49393 Lohne

Inhaltsverzeichnis

Unternehmensportrait

Als mittelständisches IT-Systemhaus beschäftigt die große Austing GmbH derzeit 22 Mitarbeiter und hat einen facettenreichen Kundenkreis, der vom Privatkunden bis hin zum Geschäftskunden mit mehreren hundert Mitarbeitern reicht. Die Bereiche in unserem Unternehmen reichen von der Installation und Wartung der Kundenendgeräte und Netzwerke, bis hin zum Server. Zudem unterstützen wir unsere Kunden bei der IT-Beratung, der IT-Sicherheit, dem Managed Print Service und dem Dokumentenmanagement

1.Projektvorbereitung

1.1 Gespräch mit der Unternehmensleitung

Die Geschäftsführung äußerte den Wunsch, dass zum 1. Juli 2016 eine Mobile Device Management (im Folgenden als MDM abgekürzt) Lösung für das Unternehmen eingeführt werden soll. Die Geschäftsleitung möchte, dass die Mitarbeiter zukünftig auf betriebsinterne und kundenrelevante Dokumente sicheren Zugriff mit einem Mobilgerät bekommen. Ziel ist die Aufnahme des MDM in das Firmenportfolio. Ein weiterer wichtiger Punkt ist die Umsetzung einer ausgewogenen Schutzfunktion ohne dass die Benutzerfreundlichkeit zu stark leidet bei der Bedienung. Dafür wird eine Testumgebung realisiert, die sich nicht in unserem Produktivnetz befindet, um den Betriebsablauf nicht zu gefährden. Für die Realisierung des Projektes ist auch eine Kosten Analyse und der Vergleich verschiedener Anbieter gewünscht. Nach einer ausgiebigen Betrachtung aller Kriterien, soll mit der Geschäftsführung eine Entscheidung getroffen werden, welche der möglichen Lösungen zum Einsatz kommen soll.

1.2 Projektphasen und Zeitplanung in Stunden

- IST-Analyse 1
- Soll-Konzept 1
- Kosten Analyse 2
- Kosten Leistungsvergleich 2
- Planung der Testumgebung inkl. Virtueller Maschine 1
- Installation der Software 1
- Einrichtung und Konfiguration der Software 6
- Verteilung der Software auf die Mobilgeräte 2
- Kontrolle der Lösung auf den Mobilgeräten 3
- Test von Szenarien auf den Mobilgeräten 4
- Nachkalkulation 1
- Benutzerdokumentation 4
- Administrationsanleitung 6
- Abschließendes Gespräch mit der Geschäftsleitung 1

1.3 IST – Analyse

Derzeit werden 20 firmeneigene und private Mobilgeräte mit dem Betriebssystem Apple iOS verwendet. Vorhandene Dienste, die im laufenden Arbeitsalltag unumgänglich sind, werden größtmöglich abgesichert. Dazu gehören sichere Protokolle wie z.B. HTTPS, IPsec und TLS (die Weiterentwicklung von SSL). Dennoch ist jeder Mitarbeiter vorerst für die Sicherheit seiner Geräte selbst verantwortlich. Erschwerend kommt hinzu, dass Firmenhandys im privaten Bereich eingesetzt werden und umgekehrt. Eine strikte Trennung der privaten und betrieblichen Nutzung ist hierbei in der Praxis nicht umsetzbar. Aktuell gibt es keine Dokumentation der eingesetzten Mobilgeräte.

1.4 Soll – Konzept

Die Geschäftsführung möchte, dass die Mobileräte, Smartphones/Tablets, über eine zentral verwaltete Software geschützt und eingerichtet werden können. Wichtig ist, dass die Daten der Geräte bei Diebstahl oder Verlust gelöscht werden können. Im Rahmen dieses Projektes sollen die verschiedenen Anbieter von MDM Lösungen verglichen und einer Kosten-Leistungs-Analyse unterzogen werden. Die Geschäftsführung legt besonderen Wert auf die lokale Installation der Software, zurücksetzten und löschen der Geräte, verschlüsselte Verbindungen, Exchange ActiveSync, ein gut erreichbarer Support und der Zugriff auf die App-Stores soll verhindert werden. Nach der Einführung einer MDM Lösung soll eine detaillierte Dokumentation der Software, und eine Dokumentation der Geräte und der Benutzer erstellt werden.

1.5 Am Markt verfügbare Anbieter auswählen

Im Verlauf der Vorbereitung zur Verwaltung der Mobilgeräte und deren Sicherheit hat sich gezeigt, dass es eine Vielzahl von Lösungen gibt, die sich in grundsätzlichen Eigenschaften unterscheiden. Einige sind ausschließlich Cloud basiert, bei anderen liegen die Daten auf den Servern der Hersteller. Andere Unternehmen bieten eine kombinierte Datenverwaltung, wo die Daten auf den Servern des Herstellers und in der Cloud liegen. Nachteile dieser Lösungen könnten z.B. die Verfügbarkeit der Server, der Schutz der Daten, sowie Sicherheitslücken sein. Die gängigen Betriebssysteme können bei allen Anbietern verwaltet werden. Die Unterstützung von Blackberry und anderen wenig genutzten Systemen werden nicht von allen Herstellern angeboten.

1.6 Vergleich der Software

Durch die Recherche im Internet[1], die Kommunikation mit den Herstellern[2] und beim Erfahrungsaustausch mit Partnern bei der Systemhauskooperation iTeam[1], haben die 3 Lösungen „Kaspersky Security for Mobile“, „vmware AirWatch“ und „Sophos Mobile Control“ überzeugt und sollen miteinander verglichen werden. Im folgenden „Kaspersky“, „AirWatch“ und „Sophos“ genannt.

Anforderungen an die MDM Lösung

Systeme

Betriebssysteme die unterstützt werden. iOS, Android, Windows Phone, Blackberry.

Administration

Geräteinformation	Empfangsstatus, Systemversion
Inventarisierung	Aufnahme in das Management, Zertifikate
Konfiguration	Gruppenprofil, Einzelprofil
Überwachung	Reporting (ja/nein), live, zusammengefasst, zeitversetzt
Richtlinien	Wi-Fi, VPN, Bluetooth, Massendatenspeicher ja-nein
GUI	Webclient, Anwendung
E-Mail	Exchange ActiveSync Anbindung
Applikationen	Remote Installation und Deinstallation, Black/White List

Sicherheit

Verschlüsselung	Komplett, einzelne Datenverschlüsselung
Löschen	Komplett, teilweise, einzelne Daten
Sperrung	Automatisch, manuell durch den Administrator oder Benutzer
Passwörter	Steuerung der Passwortkomplexität, 2 Faktor Authentifizierung
Lokalisierung	Lokalisierung, Tracking
Datenschutz	Schutz der Kundendaten, Verhinderung von Kopieren der Daten

Support

Erreichbarkeit	Reaktionszeit des Supports innerhalb von 4 Stunden

Lizenzen

Vereinbarung	Preis pro User, Pro Gerät, Kombination, Basispreis

1.6.1 Funktionsvergleich der Lösungen

Vergleicht man die Betriebssysteme, die unterstützt werden, stellt man fest, dass AirWatch auf alle Systeme Rücksicht nimmt. Bei Kaspersky und Sophos werden nur die gängigsten Systeme unterstützt.
Die Eckwerte der Geräteinformationen unterscheiden sich bei einem Vergleich nur gering. Das Verfahren und die Komplexität der Inventarisierung verlaufen bei jedem Hersteller anders, dennoch wurde bei allen auf eine komfortable und übersichtliche Bedienung geachtet.
Bei den Merkmalen Konfiguration, Überwachung der Mobilgeräte und Richtlinien sticht AirWatch hervor, Sophos und besonders Kaspersky decken nur Basisanwendungen ab.
Die Übersichtlichkeit der GUI wird von Sophos professionell umgesetzt. Während Kaspersky hier eine solide Leistung zeigt, schwächelt Air Watch bei diesem Feature. Betrachtet man die Einbindung der E-Mail Applikation bei den Anbietern offenbart einzig Kaspersky Lücken, da unter anderem eine Anbindung per ActiveSync nicht geboten wird.
Im Bereich der Applikationsverwaltung zeigt sich Air Watch überdacht mit einer vielfältigen Anzahl an Optionen. Sophos bietet eine gute Verwaltung, leider ist die Sandbox Funktion noch in der Beta Phase, diese vermisst man ebenfalls bei Kaspersky. Zusätzlich wäre die Möglichkeit die Applikationen als Administrator zu installieren wünschenswert.

Jeder Anbieter stellt eine teilweise oder komplette Verschlüsselung der Daten und Dateien bereit, welche sich nur mit einem Kennwort öffnen lassen.
Das Löschen und Sperren der Geräte stellt sich bei Kaspersky und Sophos als solide heraus. Air Watch hat dagegen eine intuitivere Bedienung mit allen Funktionen.

Ein Alpha-Nummerisches Kennwort sowie dessen vordefinierte Länge bieten alle Lösungen an. Ergänzend kann bei allen Anbietern ein Intervall zum Ändern des Kennwortes festgelegt werden sowie die maximale Anzahl an Versuchen zum Entsperren des Gerätes.
Beim Thema der Lokalisierung/Tracking lassen alle 3 Anbieter eine gleichwertige Lösung erkennen. Es ist noch hervor zu heben, dass AirWatch zusätzliche Informationen anzeigt, wie die Zugriffsaktivität auf den Content Locker, und Verstöße gegen die Richtlinien.
Von allen verglichenen Anbietern stellt lediglich AirWatch ein ausgereiftes Sandbox Verfahren zum Datenschutz zur Verfügung. Mögliche Richtlinien, Verstöße oder Verletzungen der Datenschutz Richtlinien, werden bei AirWatch gesondert dargestellt. Der Aufruf der Daten aus der Cloud wird bei AirWatch und Sophos über eine 256bit Verschlüsselung gesichert, darüber hinaus sind die Webclients mit Zertifikaten validiert.
Die Logistik bei der Umsetzung der Reaktionszeit des Supportes, ist bei AirWatch eher durchschnittlich. Kaspersky und Sophos hingegen sichern hier kurze Reaktionszeiten zu.
Sophos eröffnet bei den Lizenzmodellen die ausgewogenste Wahlmöglichkeit. Kaspersky und AirWatch haben nicht diese Auswahlmöglichkeiten.

Die daraus resultierenden Erfahrungen werden hier bildhaft dargestellt.

Legende: - ↳ negativ, O ↳ erwartet, + ↳ positiv

	AirWatch	Kaspersky	Sophos
Betriebssysteme, die unterstützt werden	+	O	O
Geräteinformationen	O	O	O
Verfahren und Komplexität der Inventarisierung	+	+	+
Konfiguration	+	-	-
Überwachung	+	-	O
Richtlinien	+	-	O
GUI	-	O	+
E-Mail	+	O	+
Applikationen	+	-	O
Verschlüsselung der Daten	+	+	+
Löschen	+	O	O
Sperren	+	-	O
Passwörter	+	+	+
Lokalisierung	+	O	O
Datenschutz	+	-	O
Erreichbarkeit des Supports	-	+	+
Lizenzmodel	O	O	+

Tabelle1: Funktionsvergleich

1.6.3 Vorteile und Nachteile der Lösungen

Sophos bietet eine einfache Installation, die mindestens das Betriebssystem Windows auf einem Server 2012 voraussetzt. Entweder erfolgt die Installation auf einer physikalischen oder einer virtuellen Maschine. Der solide Umfang lässt nur ein paar Funktionen offen. Die Weboberfläche ist übersichtlich und selbst erklärend. Zum normalen Support via Telefon und E-Mail ist auch ein Live Chat verfügbar. Leider sind Funktionen wie ein Datencontainer nicht

vorgesehen. Das Sandbox Verfahren ist noch in der Beta Phase. Optionen, wie der Datenschutz sind noch nicht ausgereift.

Kaspersky deckt den Antivirenschutz komplett ab. Das Hinzufügen der Lizenz ist schnell erledigt und man hat Zugriff auf einen soliden Umfang. Der Support besticht durch kurze Reaktionszeiten. Leider setzt Kaspersky noch auf eine veraltete, nicht mehr von Apple unterstützte Software. Das Verwalten der Geräte gestaltet sich ohne Anleitung als schwierig. Die Funktionen der Lösung sind auf ein Minimum reduziert.

AirWatch ist auf einem physikalischen oder virtuellen Server mit dem Windows Betriebssystem Server 2012 zu installieren. Die umfangreiche Software bietet viele Features. Wenig genutzte Betriebssysteme wie Tizen, ChromeOS und Symbian werden ebenfalls unterstützt. Es ist eine lange Einarbeitungsphase in den verschachtelten Aufbau nötig, um sich mit allen Optionen vertraut zu machen. Ein Blick in das englische Handbuch ist unerlässlich. Der Support hat eine lange Reaktionszeit. Ein deutscher Telefonsupport ist nicht verfügbar.

1.6.4 Auswertung des Funktionsvergleiches

Dies ist ein Auszug aus der Abbildung des Funktionsvergleiches. Die komplette Auswertung des Funktionsvergleiches mit einer Erläuterung befindet sich im Anhang.

Hauptziel	AirWatch		Kaspersky		Sophos	
	Punkte	Wertigkeit	Punkte	Wertigkeit	Punkte	Wertigkeit
Systeme 5%	6	0,60	3	0,15	4	0,20
Administration 30%	42	1,26	29	1,09	39	1,47
Sicherheit 35%	35	1,75	30	1,50	33	1,65
Support 20%	5	1,00	6	1,20	6	1,20
Lizenzvereinbarung 10%	5	0,50	6	0,40	5	0,50
Wertigkeit	93	5,11	74	4,54	87	5,02

Tabelle 2: Auswertung

1.7 Kosten Analyse

Nach Rücksprache mit den Anbietern wurde mir eine Preisliste zugesandt. Die Kosten werden mit 25 Geräten in der Basisversion für das Anschaffungsjahr gerechnet. Bei AirWatch ist es so, dass die Lizenzen nach dem Kauf unbefristet sind, dafür aber eine Bereitstellung der Software stattfindet. Danach fallen jährliche Gebühren für die Wartung der Software an. Bei Kaspersky und bei Sophos müssen die Lizenzen jährlich neu gekauft werden, dafür ist die Software frei erhältlich. Für die Wartung der Software fallen bei den beiden Anbietern keine Gebühren an. Für die Einrichtung der Software, die Profilerstellung, das RollOut der Profile und die Arbeitszeit, wurde bei AirWatch ein Preis von 673,80€ Netto ermittelt. Da keine Vergleichswerte für Kaspersky und Sophos vorliegen, wurde der Einrichtungspreis von AirWatch als Basis genommen. Für die Virtuelle Maschine berechnet sich der Preis aus dem Stundenlohn eines internen Administrators für die Einrichtungszeit der Maschine und die Installation des Betriebssystemes.

	AirWatch	Kaspersky	Sophos
Bereitstellung / Software	1903,50 Euro	0,00 Euro	0,00 Euro
Lizenzen	851,50 Euro	876,00 Euro	1075,00 Euro
Jährliche Wartung	209,50 Euro	0,00 Euro	0,00 Euro
Virtuelle Maschine	99,90 Euro	99,90 Euro	99,90 Euro
Windows 2012 Lizenz	719,00 Euro	719,00 Euro	719,00 Euro
Einrichtung	673,80 Euro	673,80 Euro	673,80 Euro
Zusammen	4457,20 Euro	2185,90 Euro	2393,90 Euro

Tabelle 3: Kosten

Da eine solche Lösung länger eingesetzt wird, werden die Kosten auf 5 Jahre hochgerechnet, um einen Überblick über die laufenden Kosten zu erhalten. Die Kosten für die Virtuelle Maschine, Einrichtung und Windows Lizenz werden nicht mehr berücksichtigt, da es einmalige Kosten sind.

Dadurch ergibt sich ein anderer Blick auf die Kosten im Vergleich zum Anschaffungspreis.

	AirWatch	Kaspersky	Sophos
Anschaffungsjahr	4457,20 Euro	2185,90 Euro	2393,90 Euro
Lizenzen für 4 weitere Jahre	0,00 Euro	3504,00 Euro	4300,00 Euro
Software	0,00 Euro	0,00 Euro	0,00 Euro
Wartung	838,00 Euro	0,00 Euro	0,00 Euro
Kosten für 5 Jahre	5295,20 Euro	5689,90 Euro	6693,90 Euro

Tabelle 4: Hochrechnung

1.7.1 Kosten

Sophos liegt im Kostenvergleich für ein Jahr im Mittelfeld. Dass keine Kosten für die Software und die Wartung anfallen ist positiv. Dies wird quasi wieder durch den Kauf einzelner Module ausgeglichen. Für eine langfristige Entscheidung der Lösung ist sie im 5 Jahres Vergleich am kostspieligsten.

Die Lösung von **Kaspersky** ist auf ein Jahr gesehen am preiswertesten. Da wir im Betrieb Kaspersky schon als Virensoftware einsetzten, ist dort auch die MDM Lösung inbegriffen. So fallen zum jetzigen Zeitpunkt keine Kosten für den Erwerb der Software, die Lizenzen der VM und des Betriebssystems an. Auf längere Sicht gesehen wäre die Lösung im Mittelfeld angesiedelt.

In der Anschaffung ist die Lösung von **AirWatch** eindeutig am teuersten. Es ist fast der doppelte Preis im Vergleich zu den anderen Anbietern in der Neuanschaffung. Da jedoch fast alle Anforderungen erfüllt werden und danach nur noch die Kosten für die jährliche Wartung anfallen, ist dies auf lange Sicht eindeutig am preiswertesten.

Zur besseren Übersicht, werden die Kosten in einem Kostendiagramm grafisch dargestellt.

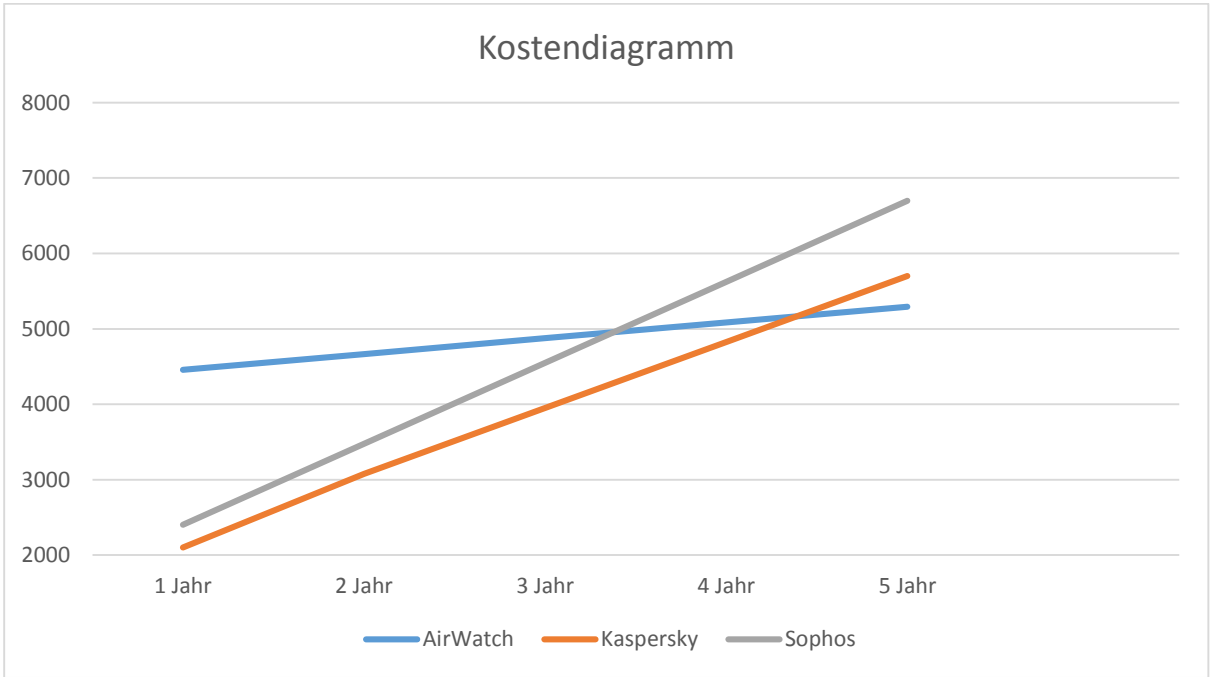


Bild 1: Kostendiagramm

1.7.2 Leistung

Mit **Sophos** kauft man eine solide Leistung ein. Schwachpunkte sind hier die fehlende Möglichkeit des Löschens der Geräte bei Diebstahl sowie die fehlende Verschlüsslung von Daten bzw. Dateien. Auch wenn nicht alle Betriebssysteme unterstützt werden, überzeugen doch die Gruppenrichtlinien, das einfache Hinzufügen von Geräten und die Übersichtlichkeit als wichtige Pluspunkte.

Die Verwendung der veralteten Version des Apple-Konfigurations-Tools ist das größte Manko bei **Kaspersky**. Die Vielzahl an Optionen für die Richtlinien ist positiv zu bewerten. Leider ist auch hier keine Erstellung von Gruppen möglich. Das Verschlüsseln von Dateien ist zwar enthalten, aber nicht das Löschen der Geräte.

AirWatch bietet alles, was man von einer MDM Lösung erwarten würde. Die Aufnahme der Geräte ist einfach. Das Erstellen von Gruppenrichtlinien ist mit einem sehr großen Umfang vorgesehen. Enthalten ist hier auch das Löschen und Verschlüsseln der Geräte. Der sehr große Umfang der Software macht eine an das Handbuch angelehnte Einarbeitung notwendig.

1.7.3 Nutzen

Die zentrale Einrichtung und Konfiguration von zahlreichen und verschiedenen mobilen Geräten ist möglich - Einzelanmeldungen von Geräten sind nicht nötig. So wird sichergestellt, dass die Sicherheitsrichtlinien eingehalten und die vertraulichen Daten des Unternehmens jederzeit geschützt sind. Da der verantwortungsvolle Umgang mit den Mobilgeräten nicht immer eingehalten wird, könnten ohne eine solche Lösung Daten in die falschen Hände geraten. Auch bringt die zentrale Verwaltung der im Unternehmen befindlichen Geräte, im Gegensatz zu einer manuellen Verwaltung, eine Kostenersparnis.

1.8 Entscheidung über eine Lösung mit der Unternehmensleitung treffen

Die Entscheidung von der Firmenleitung, nach der Durchsicht des Funktionsvergleiches und der Kosten und Leistungsrechnung, fiel auf das Produkt von AirWatch.

2. Projektdurchführung

2.1 Vorbereitung der virtuellen Maschine

Zu Beginn wird auf unserem hoch verfügbaren ESXi Cluster eine virtuelle Maschine mit dem Betriebssystem Windows Server 2012 installiert. Um die Erreichbarkeit der Testumgebung zu gewährleisten, wird der Server in ein eigenes separates Netzwerk eingefügt, damit der Testserver nicht das Produktivnetz stört.

Um die Kommunikation zwischen den Endgeräten und dem Server einzurichten, müssen in der Firewall von Watchguard und in der Windows Firewall der virtuellen Maschine Regeln erstellt werden, die eingehende und ausgehende Verbindungen erlauben. Diese Verbindungen werden über sogenannte Ports in die jeweilige Richtung vermittelt. Dafür müssen folgende Ports freigeschaltet werden: 80 (http), 443 (https), 587 (smtp), 5223 (Apple-

Benachrichtigungsdienst), und 5228 (Android Dienste). Blackberry und Windows Phone nutzen keine zusätzlichen Ports.

2.2 Installation der Software

Auf dieser Basis, habe ich eine Testversion von AirWatch bestellt. Hierbei handelt es sich um eine Cloud basierte Version, die voraussetzt, dass eine Virtuelle Maschine für zusätzliche Dienste und Programme installiert wird. Unter anderem für den Content Locker oder das Mobile E-Mail Management. Die Version hat den vollen und uneingeschränkten Umfang, der für einen Monat gültig ist. Nach dieser Zeit ist die Umstellung auf eine Vollversion möglich. Die zuvor eingestellten Geräte und Richtlinien werden ohne Verlust übernommen. Der Vorteil einer virtuellen Maschine ist, wenn das Programm deinstalliert werden sollte, dass keine Rückstände auf dem Server und in der Registry verbleiben, sollte die Virtuelle Maschine gelöscht werden.

2.3 Konfiguration der Software

Da es sich hier um eine Cloud basierte Variante handelt, beschränkt sich die Grundkonfiguration auf die administrativen Kennwörter und die Auswahl der Sprache. Bei der Vollversion des Produktes auf einem Server wird auch dort alles über den Webclient gemacht, nur mit dem Unterschied, dass die Daten lokal auf den Servern in unserem Unternehmen liegen und nicht beim Hersteller.

2.4 Erstellung der Zertifikate

Der Sinn eines digitalen Zertifikates ist, das sie die Kommunikation in Netzwerken prüfen und verschlüsseln. Dies sorgt für eine sichere Kommunikation mit internen und externen Internetseiten durch eine 256-Bit Verschlüsselung. Damit wird überprüft, ob die Identität der Webseite zulässig und die Kommunikation geschützt ist.

Bei Apple werden die digitalen Zertifikate genutzt, um die Authentifizierung der Benutzer und der Geräte für die Verbindung zum MDM zu gewährleisten. Unterstützt werden auch die Zugriffe auf das Exchange ActiveSync, VPN und das WI-FI Netzwerk. Für die Geräte von Apple wird dieses Zertifikat benötigt, um in der MDM Software erstellte Profile hinzufügen zu können.

Aus der Software heraus kann eine sogenannte „csr“ Datei erzeugt werden. Diese muss dann über die Apple Internetseite „https://idmsa.apple.com“ hoch geladen werden. Dort wird die Datei zertifiziert und kann danach als pem Datei wieder heruntergeladen werden. Die pem Datei wird dann in der MDM Software hinzugefügt und als plist Datei hinterlegt. Erst damit ist das Verwalten der Apple Geräte möglich. Damit ist eine sichere Punkt-zu-Punkt Verschlüsselung gewährleistet. Bei Android, wird kein Zertifikat benutzt, und die Verbindung wird durch ein Management-Token gesichert. Eine Registrierung bei Google ist notwendig um den Token herunterladen zu können. Der Token wird danach in das MDM von AirWatch eingefügt.

2.5 Erstellung von Gruppen

Es können verschiedene Gruppen nach einer für den Betrieb geeigneten Namensverwaltung angelegt werden. Für unseren Betrieb wurden folgende Gruppen angelegt: Geschäftsführung,

Technische Leitung, Mitarbeiter und Auszubildende. Für die jeweiligen Gruppen lassen sich individuelle Profile mit eigenen Richtlinien erstellen. Beim Hinzufügen neuer Mitarbeiter und derer Mobilgeräte, können sie einer Gruppe zugewiesen werden, worauf das dafür vordefinierte Profil auf dem Gerät installiert wird

2.6 Erstellung der Profile

Profile lassen sich für Android, Apple IOS, Apple Mac OS X, Apple TV, Blackberry, Blackberry 10, Chrome OS, Symbian, Tizen, Windows und Windows Phone erstellen.

Bei der Profilerstellung wird man auf eine allgemeine Einstellungsseite geleitet, auf der man grundlegende Einstellungen des Profils hinterlegt. Dazu gehört zu Beginn der Name des Profils, welcher in einer Namenskonvention als Kombination aus Abteilung und Stelle fungiert. Weiter gibt man an zu welcher Gruppe das Profil hinzugefügt werden soll oder ob es sich um ein Einzelprofil handelt. Es wird ein direkter Veröffentlichungszeitpunkt des Profils hinterlegt, sodass die Einstellungen möglichst schnell den Benutzer erreichen. Das Löschen des Profils auf den Mobilgeräten durch den Benutzer wurde unterbunden.

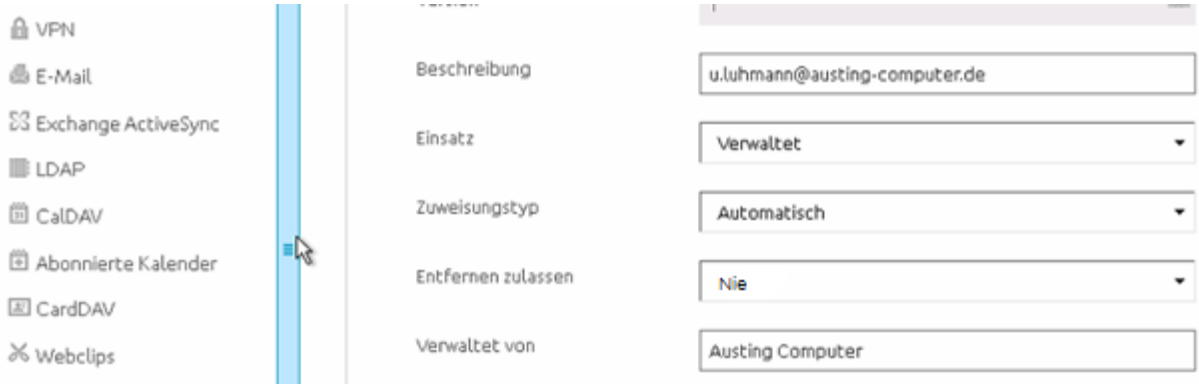


Bild 2: Profilmöglichkeiten

Der nächste Punkt betrifft die Richtlinien des Passwortschutzes. Hier wurde ein sechsstelliger nummerischer Pin gewählt, dass das Kennwort nie geändert werden muss und dass das Gerät nach vier Fehlversuchen bei der Kennworteingabe gelöscht wird. Aufgrund der letzten Einstellung sollte das Gerät regelmäßig gesichert werden.

Die restriktiven Einstellungen betreffen die Grundinformationen der Gerätefunktionen wie z.B. Apps, Datenschutz und Medieninhalte. Für uns wichtige Funktionen, wie die Benutzung der Kamera, Videoaufzeichnungen und die Verschlüsselung der Multimediadaten wurden zugelassen.

Die Option Daten in die iCloud hochzuladen und dort zu sichern ist nicht zugänglich, um das Kopieren von Daten zu unterbinden.

Die Benutzung des Sprachassistenten wurde vorerst erlaubt. Der Zugriff auf die App Stores wurde untersagt. Das Betrachten von Videos über Streaming Portale, wie z.B. Youtube, wurde unterbunden.

Bei den WLAN Konfiguration wurden die WLAN-Daten unseres Betriebes hinterlegt. Dazu gehören die SSID des WLAN‘s, der Sicherheitstyp WPA2 und der Schlüssel. Als Sicherheitstyp wäre auch WPA2 Enterprise über einen RADIUS Server möglich.

Bei dem Anschluss der Geräte an einen Computer bzw. Laptop wurde die Nutzung der Geräte als Massendatenspeicher untersagt. Dies soll gewährleisten, dass keine Unternehmensdaten oder Kundendaten auf die Computer kopiert werden können.

Nicht alle Geräte dürfen oder sollen eine VPN Verbindung aufbauen. Einige Mitarbeiter benötigen diese Funktion nicht, wiederum andere Mitarbeiter, z. B. die aus der Technik, sollen die VPN Verbindung auf den Mobilgeräten nutzen. So wurde das VPN Profil als separates MDM Profil erstellt und gesichert. Dies kann dann bei den betreffenden Geräten einzeln veröffentlicht werden. Als Verbindungstyp wird das IPSEC Protokoll verwendet.

Dies soll eine gesicherte Kommunikation ermöglichen, in dem verschiedene Mechanismen die Vertraulichkeit und Authentizität gewährleisten. Zur Authentifizierung werden der Benutzername und der Gruppenname verwendet. Das durch den Administrator vordefinierte 16-stellige alpha-nummerische Kennwort wird so hinterlegt, dass die Benutzer es nicht mehr eingeben müssen und so das Kennwort erst gar nicht bekannt gegeben werden muss. Ein Proxy Server wird nicht verwendet.

Bild 3: Passwörter

Damit die Geräte nicht auf unzulässige oder bekanntermaßen gefährdete Internetseiten zugreifen können, werden diese als eine vordefinierte Liste zur Verfügung gestellt, die den Geräten hinzugefügt werden kann. Der Benutzer hat dann keine Möglichkeit diese Seiten anzusteuern. Dem voreingestellten Filter können noch manuell Seiten hinzugefügt werden.

Es stehen noch weitere Konfigurationspunkte zur Verfügung. Da sie aber in unserem Arbeitsumfeld momentan keine Anwendung finden, werden sie hier auch nicht speziell aufgeführt. Zu diesen Punkten gehören z.B. CalDAV, CardDAV oder AirPlay Mirroring.

CalDAV und CardDAV sind Netzwerkprotokolle, die es ermöglichen auf Kalender und Adressbücher zu zugreifen und zu synchronisieren, sollte kein Exchange ActiveSync zur Verfügung stehen. AirPlay Mirroring erlaubt die Inhalte der Mobilgeräte über WLAN auf ein Apple TV zu senden, um sie so auf einem Fernseher zu betrachten.

Die aufgezählten Optionen lassen sich auch einzeln konfigurieren und sichern. Eine Konfiguration des Passwortschutzes ließe sich entweder als „Passwort Richtlinie Zentral“ oder „Passwort Richtlinie Leiter“ speichern und einzeln auf die Gruppen oder Geräte verteilen.

2.7 Benutzer und Mobilgeräte hinzufügen

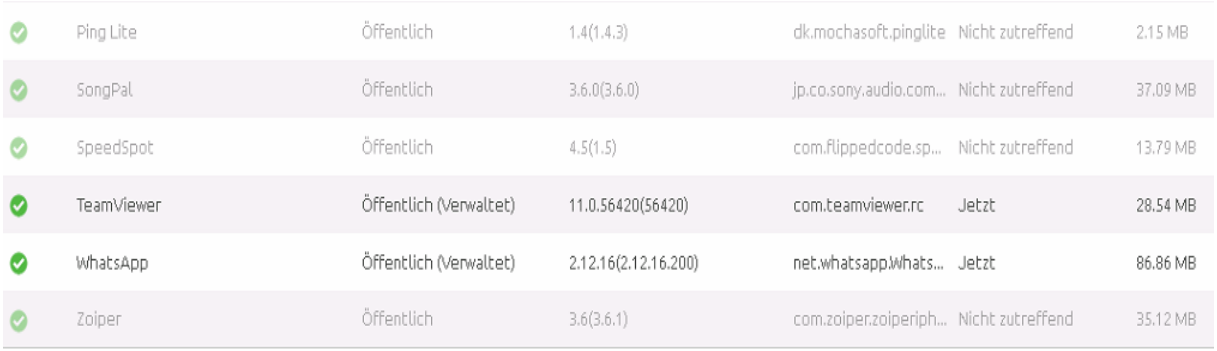
Das Einpflegen von Benutzern und Mobilgeräten in die Mobilverwaltung, erfolgt in einem Arbeitsschritt. Nachdem die Daten des Benutzers eingetragen wurden (Name, Vorname, Adresse, E-Mail-Adresse und die Mobilfunknummer) kann der Benutzer einer Gruppe hinzugefügt werden. Sollte er nicht zu einer Gruppe gehören, muss für den Benutzer ein separates Profil erstellt werden.

2.8 Veröffentlichung der Profile

Um das Mobilgerät überhaupt verwalten zu können, muss das Zertifikat oder der Token entweder per SMS oder per E-Mail an den Benutzer geschickt werden. Die Installation des Zertifikates erfolgt durch die Zustimmung des Benutzers. Ohne seine Zustimmung wäre die Installation nicht möglich.

2.9 Applikationsverwaltung

Für die Benutzer werden Container zur Verfügung gestellt, in denen sich die Applikationen befinden. Die Container basieren auf dem Sandbox Verfahren. Die Sandbox bezeichnet einen isolierten Bereich, dessen äußere Umgebung keinerlei Auswirkungen auf die Maßnahmen innerhalb haben. Da Applikationen, wie Teamviewer, in der Sandbox ausgeführt werden, können keine Eingaben, Daten und Kennwörter von Programmen oder Applikationen außerhalb des Containers ausgelesen werden, weil sie keinen Zugriff darauf haben.



Ping Lite	Öffentlich	1.4(1.4.3)	dk.mochasoft.pinglite	Nicht zutreffend	2.15 MB
SongPal	Öffentlich	3.6.0(3.6.0)	jp.co.sony.audio.com...	Nicht zutreffend	37.09 MB
SpeedSpot	Öffentlich	4.5(1.5)	com.flippedcode.sp...	Nicht zutreffend	13.79 MB
TeamViewer	Öffentlich (Verwaltet)	11.0.56420(56420)	com.teamviewer.rc	Jetzt	28.54 MB
WhatsApp	Öffentlich (Verwaltet)	2.12.16(2.12.16.200)	net.whatsapp.Whats...	Jetzt	86.86 MB
Zoiper	Öffentlich	3.6(3.6.1)	com.zoiper.zoiperiph...	Nicht zutreffend	35.12 MB

Bild 4: Applikationen

Da der Zugriff auf die App Stores geblockt wurde, wurden Applikationen ausgewählt, die im aktiven Betrieb gebraucht werden. Freigegeben wurden unter anderem der Teamviewer, die Telefonie App Media5-fone und der Netzwerk Scanner Fing. Installiert werden die Apps auf den Geräten direkt durch den Administrator. Da wir unterschiedliche Abteilungen haben und der Managed Print Service Bereich zum Beispiel andere Applikationen benötigt als die Applikationen ineo-PRINT oder NSI Moblie, werden sie durch den Administrator zwar bereitgestellt, aber benutzerspezifisch verteilt und veröffentlicht.

Bei den Geräten der technischen Leitung in unserem Hause, wurde der Zugriff auf die App Stores nicht völlig verhindert. Jedoch wurden ganze Kategorien aus den App Stores wie z.B Spiele und Filme nicht zugänglich gemacht. Erlaubt wurde nur der Zugriff auf die Kategorie der Dienstprogramme.

2.10 Backups

Backups können nicht durch den Administrator gemacht werden. Dies ist entweder durch den Anschluss an einen Computer (iTunes) oder durch die iCloud möglich. Da die Verwendung als Massendatenspeicher und der iCloud untersagt wurde, kann ein Backup erst einmal nur durch den Benutzer stattfinden. Nach Rücksprache mit dem Hersteller ist diese Funktion aber in der Planung. Fotos und Videos die der Benutzer aufnimmt, werden verschlüsselt in einem separaten Ordner im Content Lockers hinterlegt und können vom Benutzer auf den Server hoch geladen werden.

2.11 E-Mail Verwaltung

In unserem Unternehmen nutzen wir die E-Mail Lösung von Tobit. Diese Software enthält einen David12 Server in der aktuellen Sitecare Version in Verbindung mit der David Client-Software. Damit Mobilgeräte von außerhalb des Unternehmens mit dem David Server kommunizieren können, unterstützt David seit 2014 das etablierte ActiveSync-Protokoll von Microsoft. Um dies auf den mobilen Geräten nutzen können, wird für jeden Benutzer ein eigenes E-Mail Profil erstellt. In das Profil werden der Tobit-Benutzername und dessen Kennwort eingetragen. Für die Verbindung ist die externe IP Adresse bzw. der Hostname des Servers auf Port 443 für TLS unerlässlich. Die alternative Methode um E-Mails zu integrieren findet bei uns keinen Einsatz. So wäre es möglich die Daten des Accounts unter Verwendung von IMAP oder POP3, mit oder ohne TLS Verschlüsselung anzugeben. Eine Adresssynchronisierung wäre in diesem Schritt auch möglich.

2.12 Daten Container

Um den Datencontainer (Content Locker) nutzen zu können, müssen zwei separat erhältliche Applikation von AirWatch auf den Mobilgeräten installiert werden: Den Content Locker sowie den Content Viewer. Damit der sichere Austausch von Daten garantiert werden kann, werden diese in einer Sandbox Umgebung geöffnet. Die Installation wird direkt durch den Administrator auf den Geräten ausgeführt.

Der Content Locker ist dafür vorgesehen, Inhalte für das Mobilesystem bereitzustellen, damit diese sie herunterladen können. Entsprechend befinden sich im Content Locker Anwendungen wie zum Beispiel „Teamviewer“ oder „Fing“. Dokumente können beispielsweise in Form von Word oder Excel hinzugefügt werden.

2.13 Content Viewer

Der Content Viewer dient dazu, die im Content Locker bereitgestellten Daten zu öffnen und zu bearbeiten. Sofern Änderungen an den Dateien vorgenommen werden, werden die geänderten Dateien im Content Viewer in einem separaten Ordner abgespeichert. Des Weiteren ist es möglich Dokumente zu erstellen. Diese Dateien können bei Bedarf oder auf Anforderung auf den Server hochgeladen werden. Zur Auswahl stehen die Dateiformate von Word, Excel, Adobe PDF und TXT.

Der Zugang zu den Dokumenten erfolgt über eine Anmeldemaske beim Öffnen des Content Viewer. Dort wird der vom Administrator vordefinierte Schlüssel eingegeben.

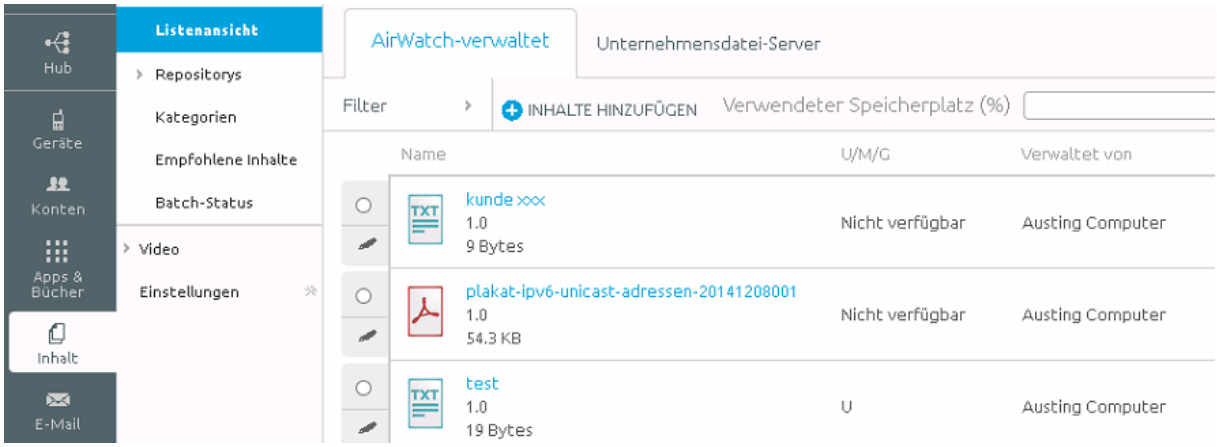


Bild 5: Content Viewer

Daten innerhalb des Content Locker können auch von anderen Benutzern eingesehen werden, die Zugriff auf den Content Locker haben. Vorgesehen ist auch hier, das Dritt-Anbieter-Applikationen nicht auf den Content Viewer zugreifen können.

3. Testphase der MDM Lösung

Es handelt sich um eine Testphase, um die Richtigkeit und Funktionalität der Software zu verifizieren. Hierbei wurde ein Teil der Geräte mit Richtlinien und Applikationen eingerichtet und dann möglichen Szenarien unterzogen.

Nicht autorisierter Datenzugriff: Bei dem Versuch an die Daten eines Gerätes zu kommen, wurde der PIN mehrmals falsch eingegeben, bis zum Hinweis das nur noch ein Versuch zur Verfügung steht. Dieser wurde ignoriert und ein weiteres Mal ein falscher PIN eingegeben. Nach dem der Pin daraufhin richtig eingegeben wurde, waren auf dem Gerät der Inhalt des Containers, dem Content Locker und die E-Mails gelöscht.

Gestohlenes / Verlorenes Gerät: Ein Gerät wurde „gestohlen“ und durch den Administrator gesperrt, was sich dahingehend auswirkte, das sich beim Gerät nach dem Einschalten kein PIN eingeben ließ. Über das Dashboard kann die Position des Geräts zu geortet werden.

Applikationen: Die freigegebenen Applikationen wurden teils den Gruppen oder einzelnen Geräten zugewiesen. Die Installation der Applikationen erfolgt durch den Administrator und der Benutzer erhielt darüber eine Nachricht. Um Applikationen von den Geräten zu löschen, wurden sie aus den Gruppenrichtlinien oder einzeln von den Geräten entfernt.

Content Locker: Das Kopieren von Daten aus dem Content Locker, um sie innerhalb des Content Locker einzufügen, war möglich. Jedoch konnten die Daten nicht in andere Programme eingefügt werden. Dem Content Locker wurden Daten in Form von Text- und PDF Dateien hinzugefügt. Nach dem Veröffentlichen waren die Dateien bei den Benutzern auf den Geräten vorhanden. Das Bearbeiten der Text Dateien war möglich. Die Synchronisation der Änderungen mit der Cloud verläuft automatisch. Das Aktualisieren der Applikationen war durch das Bereitstellen der neusten Version durch den Administrator möglich. Das Schreiben, Empfangen, Beantworten und Weiterleiten der E-Mails funktionierte im vollen Umfang.

Internetseiten: Das Aufrufen von gesperrten Internet Seiten war nicht möglich und wurde mit einer Mitteilung auf dem Bildschirm quittiert.

Wiederherstellung: Da noch keine Backups Verfügbar sind, wurde eine Neueinrichtung mit allen Richtlinien, Applikationen und Exchange ActiveSync durchgeführt. Die zuvor aufgenommenen und auf den Server hoch geladenen Fotos des Benutzers, konnten wieder auf das Gerät übertragen werden.

Richtlinien: Standard Symbole, die die Geräte von Haus aus haben, wurden testweise über die Software entfernt. Das Kamerasymbol war nach dem Veröffentlichen des speziellen Profils nicht mehr auf dem Bildschirm vorhanden. Eine Umgehung der Richtlinie durch Aufrufen der Sprachassistenten mit den Befehlen „Öffne die Kamera“ oder „Mach ein Foto“ wurde mit der Fehlermeldung des Sprachassistenten, dass die Applikation nicht zur Verfügung stände, beantwortet.

Dashboard: Im Dashboard werden die allgemeinen Informationen der Geräte sowie die Verstöße gegen die Richtlinien angezeigt. Zum Beispiel ob, wie in unserem Test, versucht wurde auf gesperrte Internetseiten zu kommen, Applikationen zu löschen oder Daten aus dem Content Locker zu kopieren.

Jailbreak: Auf einem Gerät ohne Richtlinien, wurde ein Jailbreak ausgeführt. Dies wurde nicht verhindert, aber es erfolgte eine Mitteilung an den Administrator, sowie eine Warnmeldung im Dashboard.

4. Projektabschluss

4.1 Inbetriebnahme des Mobile Device Management

Nach einer ausgiebigen Testphase und Vorführung der Software bei der Geschäftsleitung, wurde beschlossen, dass die Inbetriebnahme der Lösung zum 01.07.2016 in unserem Unternehmen durchgeführt werden kann. Auch werden alle firmeneigenen Mobilgeräte für eine Dokumentation katalogisiert.

4.2 Fazit

Nach der Einarbeitung in die Thematik und in die MDM Software, sehe ich es als unabdingbar an eine solche Lösung einzusetzen.

Die Variante von AirWatch ist ein mächtiges Werkzeug mit sehr vielen Optionen und Möglichkeiten. Auch die Vielzahl der zu verwaltenden Betriebssysteme ist beeindruckend. Die hohen Anschaffungskosten könnten viele Kunden abschrecken, die jedoch durch den komplexen Umfang des Systems und den außergewöhnlich umfangreichen Möglichkeiten gerechtfertigt sind. Die geringen Folgekosten sind ebenfalls ein gutes Argument sich diese Lösung näher anzusehen.

Sophos ist in diesem Vergleich fast gleichauf mit AirWatch. Wenn die Optionen des Datencontainer und das Sandbox Verfahren noch implementiert werden, ist dies eine gute Alternative zu AirWatch. Durch den hohen Preis und der Folgekosten, haben wir uns für AirWatch entschieden.

In unserem Unternehmen und bei unseren Kunden wird Kaspersky in der Business Version als Internet Security Software eingesetzt. In diesem Bereich ist die Software hervorragend, jedoch ist die MDM Lösung in vielen Teilen nicht ausgreift. Verglichen wurde sie, da durch die jährliche Lizenzverlängerung der Software das MDM integriert ist.

5. Glossar

ActiveSync	ist eine von Microsoft veröffentlichte Software zur Synchronisation von mobilen Endgeräten mit einem Server, für E-Mail, Kontakte, Kalender und Notizen.
Android	ist ein mobiles Betriebssystem für Smartphones und Tablets, welches von der Open Handset Alliance (Hauptmitglied Google) entwickelt wird.
Blackberry	ist ein vom gleichnamigen Unternehmen Blackberry entwickeltes und vertriebenes Mobiltelefon.
Blacklist	(schwarze Liste) ist eine Liste mit z.B. Anwendungen, die für die Nutzung durch die Anwender nicht erlaubt sind.
Bluetooth	ist eine Funktechnik für Kurzstrecken.
ChromeOS	ist ein Betriebssystem des Unternehmens Google.
Cloud	In einer Cloud werden IT-Services, wie z.B. Datenspeicher oder Anwendungen, über das Internet bereitgestellt.
csr-Datei	Ist ein digitaler Antrag, um aus einer digitalen Signatur einen öffentlichen Schlüssel für ein digitales Zertifikat zu machen.

GUI	Graphical User Interface (grafische Benutzeroberfläche): bietet dem Benutzer die Möglichkeit über grafische Objekte, welche über die Maus bedient werden können, mit einem PC zu interagieren.
http	Hypertext Transfer Protocol: Es wird hauptsächlich eingesetzt, um Webseiten aus dem World Wide Web in einen Webbrowser zu laden.
https	Hypertext Transfer Protocol Secure: Wie http, mit zusätzliche Verschlüsselung der Daten.
iOS	ist das mobile Betriebssystem von Apple für Smartphones und Tablets und Smart Watches.
Jailbreak	Ein Jailbreak oder ROOT-Zugriff bezeichnet die Entfernung von Nutzungsbeschränkungen eines mobilen Endgerätes. Dies geschieht durch die Manipulation der Firmware des Gerätes.
Port	ist eine Schnittstelle, mit der sich eine Applikation verbinden kann, um Informationen auszutauschen.
pem-Datei	ist ein Teil des X.509 Standards um eine Public-Key-Struktur für digitale Zertifikate zu erstellen.
plist-Datei	dient zur Speicherung von Konfigurationsdateien.
RADIUS	Remote Authentication Dial-In Service: Ein Client-Server Protokoll, das dazu dient Benutzer bei der Verbindung zu einem Netzwerk zu authentifizieren.
Remote	Engl. entfernt, fern.
SSL	Secure Sockets Layer. Verschlüsselungsprotokoll für die sichere Datenübertragung im Internet.
SMTP	Simple Mail Transfer Protocol. Ein Protokoll das zum Austausch und Weiterleiten von E-Mails dient.
Symbian	Symbian ist ein mobiles Betriebssystem für Smartphones. Es wird hauptsächlich durch den Hersteller Nokia genutzt.
TCP	Transmission Control Protocol. Bestimmt die Art und Weise wie Daten ausgetauscht werden.
Tizen	Ein freies Betriebssystem welches auf Linux basiert.
TLS	Transport Layer Security. Ein Verschlüsselungsprotokoll zur sichern Datenübertragung.
UDP	Transport Layer Security. Ein Verschlüsselungsprotokoll zur sichern Datenübertragung.
VM	Virtuelle Maschine: Bezeichnet die Nachbildung eines Rechners auf einem realen Computer.
VPN	Virtual Private Network: Bildet die Schnittstelle zu einem in sich geschlossenen privaten Rechnernetzwerk.
WLAN	Wireless Local Area Network: Ein lokales Funknetz
Webclient	bezeichnet einen Webbrowser..
Windows Phone	ist ein mobiles Betriebssystem für Smartphones, welches von Microsoft entwickelt wird.
Whitelist	(weiße Liste) ist eine Liste mit z.B. Anwendungen, die für die Nutzung durch die Anwender erlaubt sind.
WI-FI	Wireless Fidelity: Zertifizierung für die problemlose Kommunikation zwischen Geräten.
WPA2	Wi-Fi Protected Access 2: Sicherheitsstandard für Funknetze.

6. Anhang

Quellenverzeichnis
Tabellenverzeichnis
Bilderverzeichnis
Betriebsdokumentation
Anwenderdokumentation
Angebote

6.1 Quellenverzeichnis

[1] Bis zum 23.04.2016 waren alle hier angegebenen Internetseiten verfügbar.

Rüdiger Ariane (2014): Mobile Device Management: Funktionen im Überblick
►http://www.zdnet.de/88193558/mobile-device-management-funktionen-im-ueberblick/

Wilkowski Simon, **Biell** Patrick, **Lehnert** Christian, **Göbel** Maximilian (2014), Bewertung aktueller Lösungen für das Mobile Device Management.
►http://winfwiki.wi-fom.de/index.php/Bewertung_aktueller_L%C3%B6sungen_f%C3%BCr_das_Mobile_Device_Management

Schmidt Jürgen, **Kollaten Venne** Patrick, **Eikenberg** Ronald (2012), Selbstbedienung Smartphone
►http://www.heise.de/ct/artikel/Selbstbedienungsladen-Smartphone-1464717.html

O.V. (ohne Verfasser): Marktüberblick: Lösungen für Mobile Device Management
►http://t3n.de/magazin/marktueberblick-loesungen-fuer-mobile-device-management-235812/

Thannheiser Achim, Höller Heinz-Peter (2015), Basics und Tipps zur Regelung der mobilen Kommunikation
►http://www.thannheiser.de/downloads/mobile-device-management_CuA_2015-11.pdf

O.V.: Zehn M;DM-Lösungen im Vergleich
►http://www.cio.de/g/zehn-mdm-loesungen-im-vergleich,11138,2

O.V.: Austausch im Forum
►http://www.iteam.de/startseite/

Sommergut Wolfgang (2013) Vergleich von Mobile Device Management
►https://www.windowspro.de/wolfgang-sommergut/vergleich-von-mobile-device-management-citrix-microsoft-symantec

Künstler Diana MDM: Wer hat die beste Software-Kösung
►http://www.funkschau.de/mobile-solutions/artikel/97419/

Pohl Jacqueline (2013) Sicherheit durch Kontrolle
►http://www.chip.de/artikel/Smartphones-und-Tablets-im-Unternehmen-verwalten_54342516.html

Manhart Klaus (2013): MDM, MAM oder EMM - Wer braucht was
►http://ibmexperts.computerwoche.de/a/mdm-mam-oder-emm-wer-braucht-was,3206863

[2]

Kaspersky ► https://www.kaspersky.de
Sophos ► https://www.sophos.de
AirWatch ► https://www.airwatch.de
Apptech ► https://www.apptec360.com/
Mobiliron ► https://www.mobileiron.com/de
Maas360 ► http://www-03.ibm.com/security/mobile/maas360.html

6.2 Tabellenverzeichnis

Tabelle 1: Funktionsvergleich der verschiedenen Lösungen

Legende: - ↳ negativ, O ↳ erwartet, + ↳ positiv

	AirWatch	Kaspersky	Sophos
Betriebssysteme, die unterstützt werden	+	O	O
Geräteinformationen	O	O	O
Verfahren und Komplexität der Inventarisierung	+	+	+
Konfiguration	+	-	-
Überwachung	+	-	O
Richtlinien	+	-	O
GUI	-	O	+
E-Mail	+	O	+
Applikationen	+	-	O
Verschlüsselung der Daten	+	+	+
Löschen	+	O	O
Sperren	+	-	O
Passwörter	+	+	+
Lokalisierung	+	O	O
Datenschutz	+	-	O
Erreichbarkeit des Supports	-	+	+
Lizenzmodel	O	O	+

Tabelle 2: Auszug aus der Auswertungstabelle

Hauptziel	AirWatch		Kaspersky		Sophos	
	Punkte	Wertigkeit	Punkte	Wertigkeit	Punkte	Wertigkeit
Systeme 10%	6	0,6	3	0,3	4	0,4
Administration 30%	48	1,26	29	0,78	33	1,11
Sicherheit 30%	45	1,08	30	0,81	44	0,9
Support 20%	5	0,8	6	1,2	6	1,2
Lizenzvereinbarung 10%	5	0,6	6	0,4	5	0,4
Wertigkeit	93	5,13	74	4,52	87	4,94

Tabelle 3: Vollständige Auswertung des Funktionsvergleiches

1 Sehr gut, 2 Gut, 3 Befriedigend, 4 Ausreichend, 5 Ungenügend, 6 Mangelhaft

Die Wertigkeit errechnet sich aus der Gesamtpunktzahl multipliziert mit den Prozent der Kriterien dividiert durch 100 multipliziert mit den Prozent des Hauptzieles dividiert durch 100.

Zum Beispiel bei dem Punkt „Konfiguration“ aus der „Administration“ ist die Rechnung wie folgt

$$\frac{5 * 15}{100} * 30/100 = 0{,}225$$

Wie in diesem Beispiel (0,225), werden die Ergebnisse aufgerundet (0,23).

AirWatch

Kategorie		**Merkmal**		**Punkte**	**Wertigkeit**
Unterstützte Systeme	5 %	Betriebssysteme	100 %	6	0,30
Administration	30 %	Inventarisierung	10 %	5	0,15
		Geräteinformationen	10 %	6	0,18
		Überwachung	10 %	5	0,15
		Konfiguration	15 %	5	0,23
		Richtlinien	15 %	6	0,27
		Applikationen	15 %	6	0,27
		E-Mail Verwaltung	15 %	5	0,23
		GUI / Oberfläche	10 %	4	0,12
Datenschutz / Sicherheit	35 %	Lokalisierung	14,28 %	5	0,25
		Passwörter	14,28 %	6	0,30
		Verschlüsselung	14,28 %	5	0,25
		Datenschutz	14,28 %	6	0,30
		Löschen	14,28 %	5	0,25
		Sperren	14,28 %	5	0,25
		Backup	14,28 %	3	0,15
Support	20 %	Erreichbarkeit	100 %	5	1,00
Lizenzen	10 %	Lizenzmodel	100 %	5	0,50
Gesamt Wertigkeit					**5,11**

Kaspersky

Kategorie		**Merkmal**		**Punkte**	**Wertigkeit**
Unterstützte Systeme	5 %	Betriebssysteme	100 %	3	0,15
Administration	30 %	Inventarisierung	10 %	3	0,09
		Geräteinformationen	10 %	4	0,12
		Überwachung	10 %	4	0,12
		Konfiguration	15 %	3	0,14
		Richtlinien	15 %	3	0,14
		Applikationen	15 %	4	0,18
		E-Mail Verwaltung	15 %	4	0,18
		GUI / Oberfläche	10 %	4	0,12
Datenschutz / Sicherheit	35 %	Lokalisierung	14,28 %	5	0,25
		Passwörter	14,28 %	5	0,25
		Verschlüsselung	14,28 %	5	0,25
		Datenschutz	14,28 %	4	0,20
		Löschen	14,28 %	4	0,20
		Sperren	14,28 %	4	0,20
		Backup	14,28 %	3	0,15
Support	20 %	Erreichbarkeit	100 %	6	1,20
Lizenzen	10 %	Lizenzmodel	100 %	6	0,60
Gesamt Wertigkeit					**4,54**

Sophos

Kategorie		Merkmal		Punkte	Wertigkeit
Unterstützte Systeme	5 %	Betriebssysteme	100 %	4	0,20
Administration	30 %	Inventarisierung	10 %	5	0,15
		Geräteinformationen	10 %	5	0,15
		Überwachung	10 %	4	0,12
		Konfiguration	15 %	5	0,23
		Richtlinien	15 %	5	0,23
		Applikationen	15 %	5	0,23
		E-Mail Verwaltung	15 %	4	0,18
		GUI / Oberfläche	10 %	6	0,18
Datenschutz / Sicherheit	35 %	Lokalisierung	14,28 %	5	0,25
		Passwörter	14,28 %	5	0,25
		Verschlüsselung	14,28 %	5	0,25
		Datenschutz	14,28 %	5	0,25
		Löschen	14,28 %	5	0,25
		Sperren	14,28 %	5	0,25
		Backup	14,28 %	3	0,15
Support	20 %	Erreichbarkeit	100 %	6	1,20
Lizenzen	10 %	Lizenzmodel	100 %	5	0,50
Gesamt Wertigkeit					**4,94**

Tabelle 3: Kostenaufstellung für das Anschaffungsjahr

	AirWatch	Kaspersky	Sophos
Bereitstellung / Software	1903,50 Euro	0,00 Euro	0,00 Euro
Lizenzen	851,50 Euro	876,00 Euro	1075,00 Euro
Jährliche Wartung	209,50 Euro	0,00 Euro	0,00 Euro
Virtuelle Maschine	99,90 Euro	99,90 Euro	99,90 Euro
Windows 2012 Lizenz	719,00 Euro	719,00 Euro	719,00 Euro
Einrichtung	673,80 Euro	673,80 Euro	673,80 Euro
Zusammen	4457,20 Euro	2185,90 Euro	2393,90 Euro

Tabelle 4: Hochrechnung der Kosten auf 5 Jahre

	AirWatch	Kaspersky	Sophos
Anschaffungsjahr	4457,20 Euro	2185,90 Euro	2393,90 Euro
Lizenzen für 4 weitere Jahre	0,00 Euro	3504,00 Euro	4300,00 Euro
Software	0,00 Euro	0,00 Euro	0,00 Euro
Wartung	838,00 Euro	0,00 Euro	0,00 Euro
Kosten für 5 Jahre	5295,20 Euro	5689,90 Euro	6693,90 Euro

6.3 Bilderverzeichnis

Bild 1: Grafischer Vergleich der Kosten für 5 Jahre

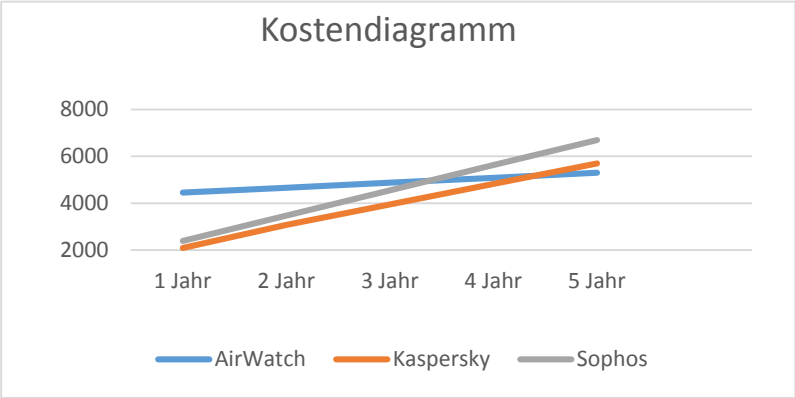


Bild 2: Profilerstellung

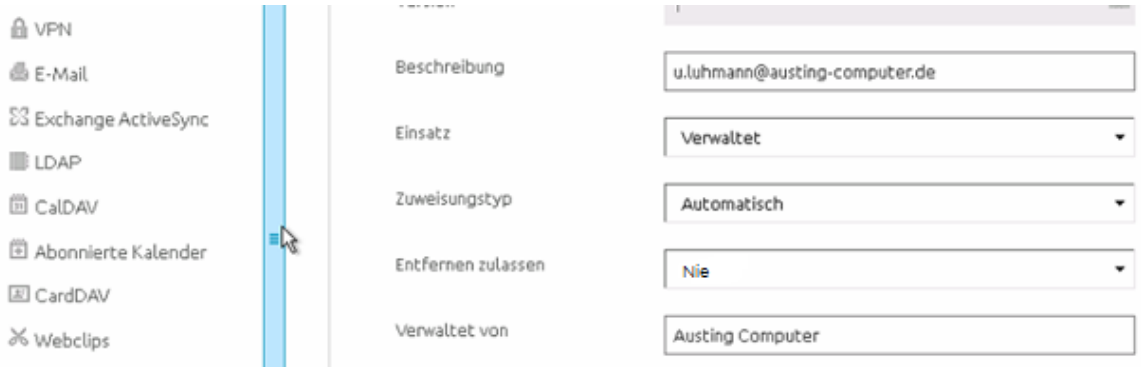
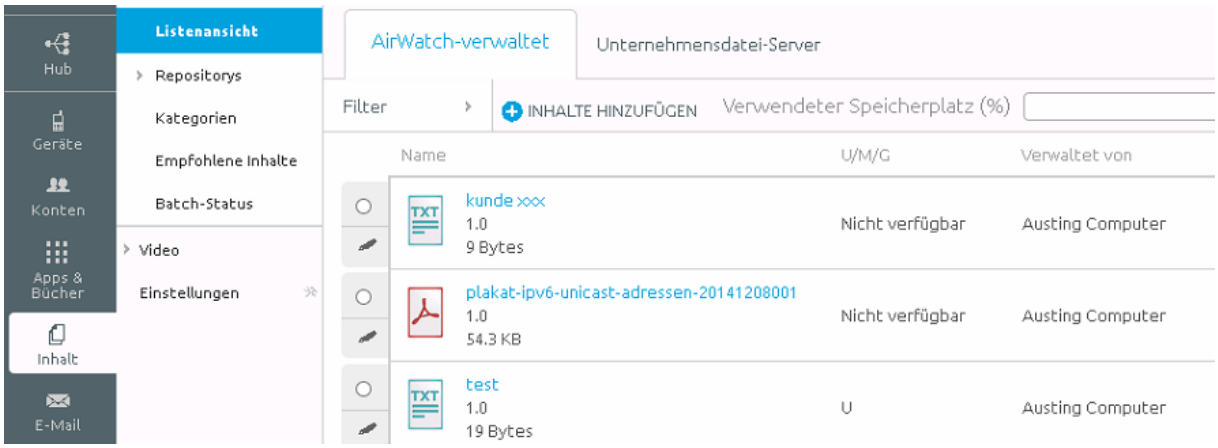


Bild 3: Passwörter

Bild 4: Applikationen

	Ping Lite	Öffentlich	1.4(1.4.3)	dk.mochasoft.pinglite	Nicht zutreffend	2.15 MB
	SongPal	Öffentlich	3.6.0(3.6.0)	jp.co.sony.audio.com...	Nicht zutreffend	37.09 MB
	SpeedSpot	Öffentlich	4.5(1.5)	com.flippedcode.sp...	Nicht zutreffend	13.79 MB
	TeamViewer	Öffentlich (Verwaltet)	11.0.56420(56420)	com.teamviewer.rc	Jetzt	28.54 MB
	WhatsApp	Öffentlich (Verwaltet)	2.12.16(2.12.16.200)	net.whatsapp.Whats...	Jetzt	86.86 MB
	Zoiper	Öffentlich	3.6(3.6.1)	com.zoiper.zoiperiph...	Nicht zutreffend	35.12 MB

Bild 5: Content View

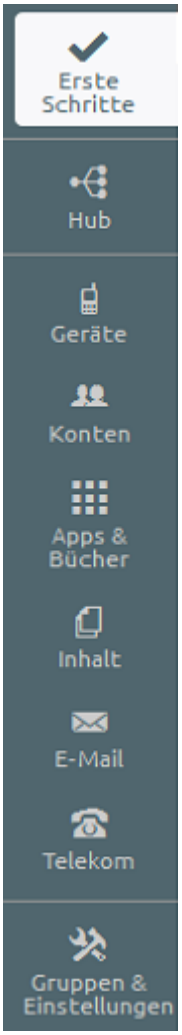


6.4 Betriebsdokumentation

Auf den folgenden Seiten folgt ein Auszug aus der Betriebsdokumentation

Auszug 1:

Menuleiste



Nachdem man nun auf der Weboberfläche ist, befindet sich links die Leiste mit den Hauptpunkten. Es folgt eine kleine Übersicht zur Orientierung über die dahinter stehenden Funktionen.

„Erste Schritte“ beinhaltet ein Tutorial, das in drei Oberbegriffe aufgeteilt ist. MDM, Inhaltsverwaltung und App-Verwaltung.

Dort kann man sich zu jedem Punkt der Software ein englischsprachiges Video ansehen, was einem bei der Konfiguration hilft.

„Hub“ ermöglicht es einem, einen Überblick über die Berichte und Analysen der Benutzer und die Mobilgeräte zu erlangen. Ebenso enthalten sind die Anzahl der verwalteten Geräte, eine Aufteilung der genutzten Betriebssysteme auf den Geräten, Verstöße gegen Richtlinien und weitere Informationen.

„**Geräte“** bietet unter anderem die Funktionen Mobilgeräte hinzuzufügen, Richtlinien und Profile zu erstellen, Zertifikate und Token zu generieren oder Drucker einzurichten.

„Konten“ enthalten die Erstellung und Übersicht der Benutzer. Welche Rechte die Benutzer haben, die Rechte des Administrators, Gruppenzuweisungen und Verwaltung.

„**Apps & Bücher“** ermöglicht die Erstellung des Content Locker und das Hinzufügen eigener, öffentlicher oder gekaufter Applikationen. Deren Verwaltung und Verteilung auf die Geräte.

„Inhalte“ dient zur Veröffentlichung von Kundendokumentationen, PDF’s oder Exceltabellen im Content Locker. Eine Kategorie Aufteilung, Einstellungen und eine Übersicht wie oft und welcher Benutzer Zugriff auf ein Dokument hatte existiert zusätzlich.

„E-Mail“ erlaubt die Möglichkeiten des E-Mail Empfanges und Versandes. Die Einrichtung eine LDAP und einer ActiveSync Anbindung.

„Telekom“ ist ein Abschnitt, in dem Einstellungen vorgenommen werden können, wie z.B. Roaming. Einstellungen der maximalen Telefoniekosten der jeweiligen Benutzer und Benachrichtigungen, wenn Geräte sich der Konfigurationsgrenze der Einstellungen nähern.

„Gruppen & Einstellungen“ ermöglicht die Erstellung von Gruppen, Untergruppen, App-Gruppen und Admin-Gruppen. Allgemeine Gruppeneinstellungen sind hier auch vorhanden.

Auszug 2:

Cloud Connector

Der Cloud Connector (nachfolgend CC) wird benötigt, damit der Mobile Access Gateway für die Geräte einen sicheren Kommunikationsweg bereitstellen kann, um auf die Unternehmensdaten zugreifen zu können. Sollten die Unternehmensdaten nicht mit der Cloud verknüpft werden, ist die Installation des EIS (Enterprise Integration Service) nötig. Siehe *Enterprise Integration Service.*

Über *Konten* ► *Benutzereinstellungen* ► *Einstellung für alle Benutzer*, gelangt man zu den *Einstellungen*. Unter dem Punkt *Systeme* werden rechts mehrere Einstellungsmöglichkeiten aufgelistet. Bei einem Klick auf *Cloud Connector*, öffnet sich ein neues Fenster in dem eine Aufforderung erscheint, den *Cloud-Connector-Installer* runterzuladen.

Nach der Installation des CC gelangen Sie wieder auf die vorherige Seite zurück. Wählen Sie *Erweiterte Einstellungen* und den Punkt *Zertifikat Erstellung*. Dieses Zertifikat wird für den Cloud-Connector und den AirWatch Server (Virtuelle Maschine) erstellt.

Nun müssen die Dienste ausgewählt werden, die in den CC integriert werden sollen. Dazu gehören:

- SMTP
- LDAP/AD
- Exchange PowerShell
- BlackBerry Sync
- Systemlog

Nach einem Klick auf *Weiter* gelangen Sie auf die nächste Seite mit auswählbaren Einstellungen. Diese Einstellungen betreffen den AirWatch Service in Verbindung mit dem CC, da diese in den CC integriert werden.

- Geräte Verwaltung
- Verwaltungskonsole
- App-Kataloge
- Content Locker
- Content Viewer

Klicken Sie nach den Einstellungen auf *Speichern,* um die Einstellungen zu übernehmen.

6.5 Anwenderdokumentation

Die Anwenderdokumentation wird für Mitarbeiter und neu in das Unternehmen kommende Mitarbeiter aufgegliedert. Allgenmein gültige Passagen werden zusammen gefasst nach der Gliederung aufgezeigt.

Bestehende Mitarbeiter: In unseren Unternehmen verwenden wir zum 01.07.2016 eine zentralisierte Geräteverwaltung. Dazu wird Ihnen per E-Mail ein Zertifikat zugeschickt, um Ihr Gerät in das MDM aufzunehmen. Dazu können Sie entweder mit Ihrem Gerät den QR-Code scannen, der in der E-Mail enthalten ist oder Sie öffnen die E-Mail auf Ihrem Gerät und folgen dem Link, der darin enthalten ist. Damit geben Sie Ihr Einverständnis, dass das Gerät nun von einem Administrator verwaltet werden kann und darf. Nachdem die Bestätigung auf dem MDM Server eingegangen ist, werden sich im Laufe des Tages zwei Applikationen installieren: Der Content Locker und der Content Viewer. Die beiden Symbole befinden sich dann auf dem Homescreen.

Neue Mitarbeiter:

Ihr mobiles Gerät wurde für Sie schon mit den MDM-Richtlinien unseres Unternehmens vorkonfiguriert. Bei Erhalt und Nutzung des Gerätes stimmen Sie der Verwaltung und der Administration zu. Auf dem Homescreen befinden sich zwei Applikationen zur Verwaltung von Apps und Kundendokumentationen: Der Content Locker und der Content Viewer.

Allgemeine Passagen: Im Content Locker befinden sich die verwalteten Apps, wie zum Beispiel Whatsapp oder Teamviewer und die Kundendokumentationen. Die Symbole der Apps (z.B. Teamviewer) sind, wie gewohnt, auf dem Homescreen. Fotos und Videos werden nicht mehr unter „Bilder “ gespeichert, sondern in einem Ordner im Content Locker. Um auf die Kundendokumentationen zuzugreifen, müssen diese aus dem Content Viewer geöffnet werden. Der Zugang zum Content Viewer ist mit einem Kennwort gesichert, den Sie bei dem Administrator erhalten. Nach dem Anmelden beim Content Viewer können Sie die bereitgestellten Dokumentationen mit einem Tippen öffnen. Sollten Daten geändert werden, werden sie in einem separaten Ordner im Content Viewer gespeichert. Um die geänderten Daten auf den Server hochzuladen, öffnen Sie den Ordner und tippen lange auf die Datei, bis sich ein Menu öffnet in dem man wählen kann was mit der Datei geschehen soll. Unter anderem kann sie von dort auf den Server geladen und vom Administrator übernommen werden.

Durch die interne Sicherheitsrichtline existieren weitere Einschränkungen bei dem Gebrauch des mobilen Endgerätes, welche hier nun Stichpunktartig aufgeführt werden:

- Es nicht möglich Videos zu streamen (z.B.Youtube).
- Ein Inhaltsfilter verwehrt den Zugang zu unseriösen Internetseiten.
- Der Zugang zum App-Store ist unterbunden.
- Ein Zugriff als Massendatenspeicher ist nicht erlaubt
- Der Upload in die iCloud ist nicht erlaubt
- Der Zugang zum WLAN wurde konfiguriert.
- Das Kennwort zum entsperren des Gerätes kann nicht geändert werden.
- Bei vier Fehlversuchen der Kennnworteingabe wird das Gerät gelöscht.

6.6 Angebote

ectacom

ectacom GmbH - Friedrich-Bergius-Str. 12 - 85662 Hohenbrunn / München

große Austing GmbH
Bergweg 26
49393 Lohne

Ansprechpartner: Herr

ANGEBOT

Kunden-Nr.: Belegdatum: 06.05.2016
Belegnummer:
Kontaktperson:
Telefon:
E-Mail:
externe Belegnummer:
Zahlungskonditionen:
Lieferart: Versand per Mail

Liefer- Endkunde:

Seite: 1

Pos.	Artikelnummer	Bezeichnung	Menge	ME	Einzelpreis	Rabatt %	Gesamt
		VARIANTE 1: Neukauf von SELECT-Lizenzen					
1	KL4863XAPFS	**Kaspersky Endpoint Security for Business - Select European Edition. 25-49 Node** **1 year Base License** Laufzeit 12 Monate	26	Lic.			€
		Alternativartikel (ist nicht im Gesamtbetrag enthalten):					
2	KL4863XAPDS	**Kaspersky Endpoint Security for Business - Select European Edition. 25-49 Node** **2 year Base License** Laufzeit 24 Monate	26	Lic.			€
		Alternativartikel (ist nicht im Gesamtbetrag enthalten):					
3	KL4863XAPTS	**Kaspersky Endpoint Security for Business - Select European Edition. 25-49 Node** **3 year Base License** Laufzeit 36 Monate	26	Lic.			€
		VARIANTE 2: Wettbewerbsablöse					
		Alternativartikel (ist nicht im Gesamtbetrag enthalten):					
4	KL4863XAPFW	**Kaspersky Endpoint Security for Business - Select European Edition. 25-49 Node** **1 year Cross-grade License** Laufzeit 12 Monate	26	Lic.			€
		Alternativartikel (ist nicht im Gesamtbetrag enthalten):					
5	KL4863XAPDW	**Kaspersky Endpoint Security for Business - Select European Edition. 25-49 Node** **2 year Cross-grade License** Laufzeit 24 Monate	26	Lic.			€

ectacom GmbH - Telefon: 08102/ 8952-0 - E-Mail: info@ectacom.com Übertrag: €

eMail

Betreff: [illegible]
Von: b.krupp@[illegible]
Priorität: Normal
Anhänge: 0

Hallo,

[illegible] das letzte Angebot für Sophos und WIN 2012. Bekommen wir sie leider nicht im PDF Format.

Sonst ein Screenshot von dem Angebot machen und das dann in die Projektmappe packen.

Grüß Bernd

Original Message [illegible]

Sophos Mobile Control Standard

Description

Tag

Part	SMC									
Users	5-9	10-24	25-49	50-99	100-249	250-499	500-999	1.000-2.499	2.500-4.999	5.000+
12 months	46,75	43,00	39,25	35,50	31,00	28,50	26,25	23,75	21,50	SMCP1CEAA
24 months	70,13	64,50	58,88	53,25	46,50	42,75	39,38	35,63	32,25	SMCP2CEAA
36 months	93,50	86,00	78,50	71,00	62,00	57,00	52,50	47,50	43,00	SMCP3CEAA
1 month	4,28	4,00	4,00	4,22	3,87	3,80	3,50	3,80	3,67	SMCP0CEAA

1965269	SBR-005 Sophos Mobile Control - 25-49 LIC SMCF1CEAA					
	1 ST	38,25	1 ST	0,00		38,25
1965314	SBR-005 Sophos Mobile Control - 25-49 LIC SMCF3CEAA					
	1 ST	50,25	1 ST	0,00		50,25
1965326	SBR-005 Sophos Mobile Control - 25-49 LIC SMCF3CEAA					
	1 ST	66,72	1 ST	0,00		66,72
2035964	MS LwMTSer Std 2012R2 X64 ZOPL/ZVM (DE) P73-06167					
	1 ST	5.720,00	1 ST	0,00		5.720,00

Schöne Grüße
Karin Hofmann

Karin Hofmann
Account Manager

ALSO Deutschland GmbH
Lange Wende 43
D 59494 Soest

Telefon +49 2921 99-5167
Fax +49 2921 99 5529

Karin.Hofmann@also.com
www.also.de

Von: Bernd Krupp [mailto:b.krupp@[illegible]]
Gesendet: Montag, 9. Mai 2016 10:14
An: Karin Hofmann
Betreff: Anfrage

Guten Morgen Frau Hofmann,

ich benötige einmal bitte ein Angebot über:

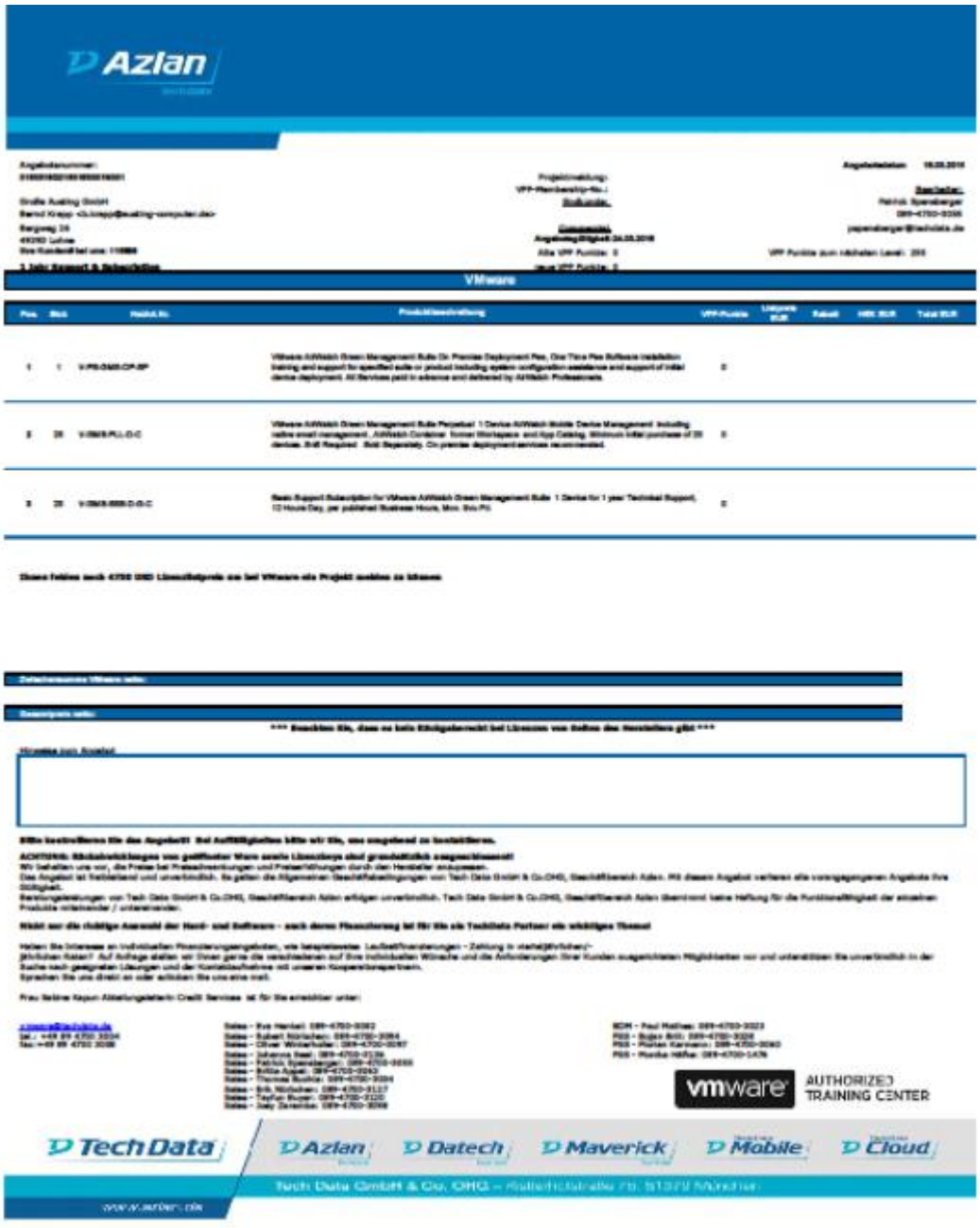
Also Sophos Mobile Control
1x Windows Server 2012 Standard

Dieses Mal benötige ich das Angebot bitte im PDF Format.

Vielen Dank

Sollten Sie Fragen haben stehe ich Ihnen sehr gerne zur Verfügung.

Mit freundlichen Grüßen aus Soest


Azlan
VMware
vmware
AUTHORIZED
TRAINING CENTER
Tech Data
Azlan
Datech
Maverick
Mobile
Cloud