WIRTSCHAFTSINFORMATIK

Studylab

TIMMY LUTZ

WIE UNTERNEHMEN MOBILE ENDGERÄTE ERFOLGREICH IN BESTEHENDE IT-INFRASTRUKTUREN INTEGRIEREN

MOBILE DEVICE MANAGEMENT IN ZEITEN VON MOBILEM ARBEITEN

Timmy Lutz

Mobile Device Management in Zeiten von mobilem Arbeiten

Wie Unternehmen mobile Endgeräte erfolgreich in bestehende IT-Infrastrukturen integrieren

Bibliografische Information der Deutschen Nationalbibliothek:

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Impressum:

Ein Imprint der GRIN Publishing GmbH, München

Druck und Bindung: Books on Demand GmbH, Norderstedt, Germany

Coverbild: GRIN Publishing GmbH | Freepik.com | Flaticon.com | ei8htz

Management Summary

Immer mehr Mitarbeiter möchten ihre privaten mobilen Endgeräte auch geschäftlich nutzen können. Zudem ist es für ein Unternehmen in der heutigen Wirtschaft notwendig, Innovationen als Erster umzusetzen, um sich Wettbewerbsvorteile zu verschaffen und auf dem Markt führend zu sein. Dem Wunsch der Mitarbeiter, eine simultane Umgebung gegenüber dem Desktoparbeitsplatz mit mobilen Endgeräten im Unternehmen zu ermöglichen, sollte nachgegangen werden. Alle Prozesse und Einrichtungen eines Unternehmens, die dem Zweck dienen, mobile Endgeräte in die Geschäftsprozesse einzubinden, fasst man unter dem Begriff mobile IT-Infrastruktur zusammen.

Um eine wirksame Strategie für ein Unternehmen zu entwickeln, ist es unabdingbar, sich auch Gedanken über Mobile Applikation Management (MAM), Mobile Informationen Management (MIM), Mobile Security Management (MSM) und Mobile Content Management (MCM) zumachen. Mobile Device Management (MDM) ist eine Art Sicherheitssoftware, die von einer IT-Abteilung verwendet wird, um die mobilen Endgeräte von Mitarbeitern zu überwachen, zu verwalten und zu sichern. Beim Mobile Device Management kann vieles aus dem klassischen Device Management adaptiert werden, doch bei einigen Punkten müssen die Konzepte überprüft werden.

Mobile Device Management-Systeme werden hauptsächlich dann eingesetzt, wenn ein Unternehmen seine Daten schützen möchte. In punkto Sicherheit, verliert ein Unternehmen schnell mal die Kontrolle über ihre Daten, da ein Mitarbeiter diese Daten, die sich möglicherweise in seiner privaten Cloud befinden, mit anderen teilen lassen, ohne dass irgendeine Compliance-Anforderung an das mobile Endgerät gestellt wird. Vor allem Grossunternehmen mit hochsensiblen Daten wie Patientendaten oder Daten aus dem Finanzbereich sollten hier strenge Richtlinien erlassen, um die Daten zu schützen. Dabei gilt es jedoch rechtliche Aspekte zu beachten, welche aufgrund der Tatsache, dass sich das mobile Endgerät möglicherweise in privatem Besitz befindet nicht zu verachten sind.

Es bestehen Verschiedenste Ansätze wie man einem Mitarbeiter die Arbeit ausserhalb des Unternehmensnetzwerkes vereinfachen kann. Man spricht hier von Bring your own Device (BYOD) oder Coporate owned personally enabled (COPE). Dabei sind die Ansätze dementsprechend unterschiedlich in deren Anschaffung und Verwaltung der mobilen Endgeräte.

Die dafür verwendeten Mobile Device Management Server stehen entweder im Unternehmen selbst oder werden über einen Cloud Service als SaaS angemietet.

Inhaltsverzeichnis

Abkürzungsverzeichnis

Abkürzung	Erklärung
BCM	Business Continuity Management
BIA	Business Impact Analysis
BES	BlackBerry Enterprise Server
BYOD	Bring Your Own Device
CI	Configuration Item
CMDB	Configuration Management Database
CMS	Configuration Management System
COPE	Corporate Owned – Personally Enabled
CRM	Customer Relationship Management
CSI	Continual Service Improvement
CSS	Cascading Style Sheets
EMM	Enterprise Mobility Management
GPS	Global Positioning System
GSM	Global System for Mobile Communications
IDE	Integrated Development Environment
IoT	Internet of Things
ITIL	IT Infrastructure Library
ITSM	IT Service Management
LTE	Long Term Evolution
MAM	Mobile Application Management
MCM	Mobile Content Management
MDM	Mobile Device Management
MIM	Mobile Information Management
MSM	Mobile Security Management
OS	Operation System
OTA	Over the Air

PIM	Personal Information Manager
RAM	Random Access Memory
RIM	Research in Motion
SaaS	Software as a Service
SACM	Service Asset Configuration Management
SDK	Software Development Kit
VPN	Virtual Private Network