BAB II
LANDASAN TEORI

Dalam bab landasan teori, dijabarkan beberapa literatur dan studi pustaka yang digunakan sebagai acuan penyusunan laporan ini. Terdapat tiga pokok bahasan dari landasan teori, terdiri dari pembahasan penggunaan perangkat bergerak di lingkup perusahaan, dasar dari *Mobile Device Management* (MDM), dan komponen yang ada dalam MDM.

A. Perangkat Bergerak di Perusahaan

Dalam studi literatur yang dilakukan oleh Ortbach [14], penyebaran perangkat bergerak seperti *feature phone* dan Personal Digital Assistants (PDA) dimulai pada awal tahun 1990-an dan berakselerasi pada dekade berikutnya [15]. Aplikasi perangkat bergerak pertama kali diperkenalkan bersamaan dengan dirilisnya Apple iPhone pada tahun 2007 yang juga menciptakan peluang baru untuk penggunaan *smartphone*. Saat ini, terdapat berbagai bidang studi yang berbeda dalam ranah perangkat bergerak, seperti desain dan pengembangan aplikasi perangkat bergerak atau keamanan aplikasi dan perangkat bergerak [16]–[19]. Selain itu, beberapa studi telah menganalisis teknologi perangkat bergerak kasus dalam bidang aplikasi bisnis [16]–[19]. Secara umum dapat dikatakan bahwa perangkat seluler—khususnya *smartphone*—sudah memiliki dampak yang signifikan pada kehidupan bisnis dan pribadi [20]–[22] yang mengakibatkan sejumlah tantangan dan peluang bagi organisasi serta karyawan [23], [24]. Perusahaan harus menciptakan "strategi perangkat bergerak" untuk memenuhi kebutuhan staf serta mempertahankan atau meningkatkan nilai-nilai perusahaan mereka. Selain itu, mengelola transisi ke apa yang disebut "perangkat bergerak perusahaan (*mobile enterprise*)" mungkin penting. Frasa ini mengacu pada cita-cita perusahaan yang sepenuhnya menggabungkan perangkat seluler seperti *smartphone* atau tablet ke dalam prosedur operasional mereka [25], [26].

Tujuan utama dari sebuah organisasi adalah untuk memastikan kinerja organisasi yang mencakup produktivitas dan profitabilitas, inventaris, keunggulan kompetitif, serta biaya [27]. Menurut studi Stieglitz dan Brockmann [25], TI bergerak dapat meningkatkan kinerja organisasi apabila strategi yang dusun dengan baik dari keseluruhan perusahaan yang mencakup persoalan teknis dan organisasi diterapkan. Menurut penelitian lain, keragaman produsen perangkat dan sistem operasi yang tersedia menghasilkan tataran TI bergerak yang makin beragam [28]. Selain itu, tren konsumerisasi TI yang dapat diamati seperti penggunaan perangkat bergerak pribadi untuk tujuan bisnis serta budaya "bawa perangkat Anda sendiri (*bring your own device*)" (BYOD) menambah kompleksitas TI bergerak [29], [30]. BYOD dan tataran TI yang beragam, menimbulkan tantangan baru bagi departemen TI. Mengelola TI bergerak menjadi semakin kompleks, sehingga memerlukan perangkat lunak baru dan strategi manajemen TI [28]. Mobile Device Management (MDM) merupakan salah satu solusi perangkat lunak yang muncul yang membantu departemen TI dalam menyelesaikan masalah ini. Sistem ini menyediakan fitur untuk mengelola perangkat bergerak, aplikasi, serta mendorong regulasi kepatuhan.

B. *Mobile Device Management* (MDM)

MDM merupakan sebuah perangkat lunak yang berfungsi untuk mengamankan, memantau, mengelola, serta mendukung perangkat seluler yang digunakan di seluruh perusahaan. Pendistribusian aplikasi, data, dan pengaturan konfigurasi secara *over-the-air* untuk semua jenis perangkat bergerak, termasuk *feature phone*, *smartphone*, komputer tablet, komputer bergerak yang kokoh, printer bergerak, perangkat POS bergerak, dan sebagainya, merupakan tipikal fungsionalitas MDM tingkat perusahaan. MDM bertujuan untuk meningkatkan fungsionalitas dan keamanan jaringan komunikasi seluler sekaligus mengurangi biaya dan waktu henti. Hal ini berlaku di seluruh perusahaan baik untuk perangkat milik perusahaan maupun milik karyawan (BYOD) [31].

Kebanyakan orang mengasosiasikan Microsoft Endpoint Manager (MEM) dengan Mobile Device Management (MDM). Hingga sekitar tahun 2019, MDM

merupakan istilah industri yang digunakan ketika membahas kontrol aplikasi dan konfigurasi perangkat seluler yang semula hanya ponsel, namun lambat laun digunakan untuk laptop juga. Para profesional dalam bidang ini baru-baru ini menggunakan istilah "Unified Endpoint Management' (UEM). Pergeseran ini mencerminkan pergeseran industri di mana produk manajemen seperti MEM berevolusi menjadi rangkaian produk terpadu yang digunakan untuk mengelola rangkaian *endpoint* yang jauh lebih luas daripada hanya perangkat seluler. Misalnya, MEM (melalui integrasi dengan Configuration Manager) digunakan untuk mengelola sejumlah besar PC desktop, tetapi juga memiliki beberapa kemampuan manajemen server [32].

C. Komponen alat MDM

Menurut IBM [33], setidaknya terdapat lima komponen dalam alat MDM yang terdiri dari *device tracking, mobile management, application security, identity and access management* (IAM), dan *endpoint security*.

1. *Device Tracking*

Setiap perangkat yang terdaftar atau disediakan oleh perusahaan dapat dikonfigurasi untuk menyisipkan pelacakan *global positioning system* (GPS) dan program-program lainnya. Program-program ini memungkinkan profesional TI perusahaan untuk memantau, memperbaharui serta memecahkan masalah perangkat secara aktual. Program ini juga dapat mendeteksi dan melaporkan perangkat yang berisiko tinggi atau tidak patuh dan bahkan mengunci atau menghapus perangkat dari jarak jauh jika hilang atau dicuri.

2. *Mobile Management*

Departemen TI melakukan pengadaan, penyebaran, pengelolaan, dan dukungan perangkat bergerak untuk karyawan perusahaan, seperti pemecahan masalah fungsionalitas perangkat. Departemen ini memastikan setiap perangkat dilengkapi dengan sistem operasi dan aplikasi yang diperlukan untuk penggunanya;

termasuk aplikasi produktivitas, keamanan dan perlindungan data, pencadangan dan pemulihan.

3. *Application security*

Keamanan aplikasi dapat melibatkan pembungkusan aplikasi, di mana administrator TI menerapkan fitur keamanan atau manajemen ke dalam aplikasi. Aplikasi tersebut kemudian disebarkan kembali sebagai program yang terkontainerisasi. Fitur keamanan ini dapat menentukan apakah otentikasi pengguna diperlukan untuk membuka aplikasi; apakah data dari aplikasi dapat disalin, ditempelkan, atau disimpan pada perangkat; serta menentukan apakah pengguna dapat berbagi berkas.

4. *Identity and Access Management*

Manajemen perangkat bergerak yang aman memerlukan IAM yang kuat. IAM memungkinkan perusahaan untuk mengelola identitas pengguna yang terikat dengan perangkat. Akses setiap pengguna dalam perusahaan dapat diatur sepenuhnya, menggunakan fitur-fitur seperti *single sign-on* (SSO), autentikasi multifaktor, dan akses berbasis peran.

5. *Endpoint Security*

Endpoint security mencakup semua perangkat yang mengakses jaringan perusahaan, termasuk perangkat yang dapat dikenakan, sensor *Internet of Things* (IoT) dan perangkat bergerak non-tradisional. *Endpoint security* mencakup alat keamanan jaringan standar seperti antivirus, kontrol akses jaringan serta respons insiden, penyaringan URL dan keamanan *cloud*.

Dari tiga landasan teori di atas, *mobile device management* atau *unified endpoint management* mempermudah divisi TI dalam mengelola perangkat bergerak dalam tataran TI yang beragam [14]. Selain itu, MDM juga membantu pengelola TI untuk pendistribusian aplikasi secara *over-the-air* [31] serta mengelola regulasi kepatuhan (*compliance policy*) terhadap perangkat [14]. Dengan

menggunakan Microsoft Endpoint Manager, divisi TI dapat mengelola perangkat berkerak dengan berbagai rangkaian produk terpadu yang ditawarkan [32].