Tugas Mata Kuliah Keamanan Komputer

Contoh Implementasi IT Policy dalam Lingkup Penjagaan Infrastruktur IT Perusahaan Server untuk Cloud Database

Fahima Lailul Ula (081711633017)

S1 Sistem Informasi

Fakultas Sains dan Teknologi

Universitas Airlangga

Implementasi IT Policy dalam Lingkup Penjagaan Infrastruktur IT Perusahaan Server untuk Cloud Database

1. Pendahuluan

IT Policy atau Kebijakan Teknologi Informasi digunakan oleh banyak perusahaan untuk meningkatkan kinerja dan menjaga asset-aset berharga perusahaan, terutama perusahaa yang bergerak di bidang IT, contohnya adalah pada perusahaan yang menyediakan layanan IT seperti layanan *Software as a Service* (SaaS), *Infrastructure as a Service* (IaaS), dan *Platform as a Service* (PaaS). Ketiga-tiga layanan tersebut merupakan layanan yang berkaitan erat dengan IT policy sendiri, karena dalam penggunaan SaaS, IaaS, dan PaaS perlu ada aturan dalam menjaga kinerja infrastruktur yang menghasilkan layanan yang handal untuk user agar layanan dapat bekerja optimal sesuai keinginan user dan baik aset milik perusahaan penyedia layanan IT dan user seperti *sharing system* yang telah dibangun oleh perusahaan penyedia layanan IT dan data-data di dalamnya tidak rusak. Implementasi IT policy tentunya juga akan berpengaruh pada proses bisnis, dan IT policy sendiri mempunyai banyak kategori, antara lain adalah IT policy untuk individu, IT policy untuk manajemen aset infrastruktur dan data, IT policy untuk keamanan, dan masih banyak lagi.

2. Pembahasan

2.1. Pengertian IT Policy atau Kebijakan Teknologi Informasi dan Kegunaannya

IT Policy adalah kebijakan yang mengatur perilaku user terhadap penggunaan fasilitas dan layanan informasi seperti penggunaan internet, website, email, wireless, software dan hardware. Kebijakan yang diterapkan di masing-masing institusi berbeda-beda tergantung dari fasilitas dan kondisi infrastruktur dari institusi tersebut. IT Policy di perlukan agar fasilitas serta layanan IT dapat digunakan sesuai dengan yang ketentukan dan tidak melanggar kebijakan yang ada.

Kebijakan Keamanan Teknologi Informasi (TI) atau IT policy merupakan aturan dan prosedur untuk semua individu yang mengakses dan menggunakan aset dan sumber daya TI organisasi. IT policy yang efektif adalah model budaya organisasi, di mana aturan dan prosedur didorong dari pendekatan karyawannya terhadap informasi dan pekerjaan mereka. Dengan demikian, IT policy yang efektif dapat dianggap sebagai dokumen khusus untuk setiap organisasi, yang dikembangkan dari sudut pandang orang-orangnya tentang toleransi risiko, dari bagaimana mereka melihat dan menilai informasi yang ada pada suatu institusi, dan bagaimana cara mereka dalam menjaga ketersediaan infrastruktur dan informasi. Karenanya, dalam pembuatan kebijakan, seringkali perusahaan juga menemukan kebijakan keamanan TI yang tidak tepat karena kurangnya pertimbangan tentang

bagaimana orang-orang organisasi benar-benar menggunakan dan berbagi informasi di antara mereka sendiri atau pada publik.

2.2. Manfaat IT Policy Terhadap Komponen-komponen Keamanan Cyber

Tujuan kebijakan IT adalah menjaga kerahasiaan, integritas, dan ketersediaan sistem dan informasi yang digunakan oleh anggota organisasi yang merupakan aspek komponen keamanan cyber. Berikut ini adalah manfaat IT policy bagi komponen-komponen keamanan cyber, yaitu:

1. IT policy terhadap aspek kerahasiaan (confidentiality) melibatkan perlindungan aset dari entitas yang tidak sah.

2. IT policy terhadap aspek integritas memastikan keamanan modifikasi aset ditangani dengan cara yang ditentukan dan disahkan.

3. Pada aspek ketersediaan, IT policy memastikan keadaan sistem di mana pengguna yang berwenang memiliki akses terus menerus ke aset tersebut.

Kebijakan IT adalah dokumen yang terus diperbarui agar dapat beradaptasi seiring dengan kebutuhan bisnis dan TI yang berkembang. Lembaga seperti Organisasi Internasional Standardisasi (ISO) dan Institut Nasional Standar dan Teknologi (NIST) Amerika Serikat telah menerbitkan standar dan praktik terbaik untuk pembentukan kebijakan keamanan. Sebagaimana ditetapkan oleh Dewan Riset Nasional (NRC), spesifikasi kebijakan IT perusahaan apa pun harus membahas:

1. Tujuan

2. Lingkup

3. Tujuan spesifik

4. Tanggung jawab dalam kepatuhan dan tindakan yang harus diambil jika terjadi ketidakpatuhan.

Contoh umum dari ini termasuk Standar Keamanan Data PCI dan Kesepakatan Basel di seluruh dunia, atau Pembaruan Wall Street Dodd-Frank, Undang-Undang Perlindungan Konsumen, Undang-undang Portabilitas dan Akuntabilitas Asuransi Kesehatan, dan Otoritas Pengatur Industri Keuangan di Amerika Serikat. Banyak dari lembaga pengatur ini membutuhkan kebijakan keamanan IT masing-masing.

Kebijakan keamanan organisasi mempunyai peran besar dalam keputusan penggunaan teknologi informasi, tetapi kebijakan yang ada tetap tidak boleh mengubah strategi atau misi perusahaan tersebut. Oleh karena itu, penting bagi sebuah perusahaan atau organisasi untuk menulis kebijakan yang diambil dari kerangka budaya dan struktural organisasi yang

ada demi mendukung kelangsungan produktivitas dan inovasi kebijakan IT yang baik, dan bukan sebagai kebijakan umum yang menghambat organisasi dan orang-orangnya untuk memenuhi misi dan sasarannya.

2.3. Contoh Penggunaan IT Policy pada Perusahaan Penyedia Layanan Server dan Infrastruktur IT

IT policy sendiri mempunyai berbagai macam kategori, namun yang IT policy yang paling utama dalam perusahaan penyedia layanan server dan infrastruktur IT adalah IT policy pada kategori yang mengatur pemberdayaan aset infrastruktur dan data, yang antara lain adalah sebagai berikut;

1. Kebijakan penyimpanan perangkat keras (hardware) IT: Kebijakan ini mengatur organisasi untuk melacak, memproses, dan menonaktifkan peralatan IT yang alasannya berkaitan dengan pemeliharaan infrastruktur agar infrastruktur yang ada dapat digunakan secara optimal dalam jangka waktu panjang.

2. Kebijakan pengendalian aset (asset control policy): Bentuk kebijakan umum yang dapat disesuaikan tergantung dengan keadaan organisasi ataupun institusi yang ada. Kebijakan ini mengatur prosedur dan protokol untuk mendukung manajemen aset organisasi yang efektif yang secara khusus berfokus pada perangkat elektronik. Contohnya adalah pemeliharaan data bukti transaksi digital yang dimasukkan dalam basis data perusahaan. Jika dalam perusahaan yang menyediakan layanan hosting cloud, koneksi sharing antar server juga diatur oleh kebijakan ini.

3. Kebijakan pengadaan perangkat keras IT: Kebijakan pengadaan perangkat keras yang jelas dapat mendukung implementasi pemeliharaan sumber daya perangkat keras agar selalu tersedia kapanpun dibutuhkan. Ada pula kebijakan dan prosedur pemulihan sumber daya setelah bencana juga terdapat disini.

4. Kebijakan BYOD (Bring Your Own Device): Kebijakan BYOD (Bring Your Own Device) menjelaskan langkah-langkah yang harus diambil karyawan saat menghubungkan perangkat pribadi ke sistem dan jaringan organisasi.

5. Kebijakan pemakaian perangkat milik pribadi untuk sistem yang terhubung dengan sistem perusahaan: Kebijakan ini mengatur karyawan yang bekerja dari rumah yang menggunakan sistem dan perangkat yang dipasok perusahaan. Kebijakan ini membantu memastikan bahwa mereka memiliki perangkat yang konsisten dan canggih untuk melakukan pekerjaan mereka. Maka dari itu, pada kebijakan ini organisasi harus memberikan pedoman penggunaan dan tata tertib serta tanggung jawab staf dan karyawan pengguna infrastruktur IT yang terlibat dengan sistem.

3. Kesimpulan

Keberadaan dokumen “Kebijakaan Keamanan” atau “IT Security Policies” merupakan sebuah aturan keamanan yang harus dimiliki oleh sebuah organisasi atau perusahaan yang ingin melindungi aset informasi terpentingnya. Dokumen ini secara prinsip berisi berbagai cara yang perlu dilakukan untuk mengontrol manajemen, mekanisme, prosedur, dan tata kelola dalam mengamankan informasi, baik secara langsung maupun tidak langsung.

Karena berada pada tingkat kebijakan, maka dokumen ini biasanya berisi hal-hal yang bersifat prinsip dan strategis. Dengan adanya kebijakan ini, selain akan membantu organisasi dalam mengamankan aset pentingya, juga menghindari adanya insiden atau tuntutan hukum akibat organisasi yang tidak menaati kebijakan dalam melakukan pengelolaan internal terhadap aset informasi atau hal-hal terkait dengan tata kelola informasi yang berada dalam lingkungannya.

Daftar Pustaka

__.2018."Difference between SaaS, PaaS, and IaaS and How to Choose". Diakses pada 28 November 2019 pukul 20.11. Dari web : https://www.bmc.com/blogs/saas-vs-paas-vs-iaas-whats-the-difference-and-how-to-choose/

__.2019."100 IT Policies at Your Fingertips".Diakses pada 28 November 2019 pukul 20.47. Dari web : https://www.techrepublic.com/article/100-it-policies-at-your-fingertips-ready-for-download/

___.2019."Teknologi Cloud Computing". Diakses pada 28 November 2019 pukul 17.45. Dari web: http://formulabisnisindonesia.com/cloud-computing/

__.2019."What is an IT Security Policy?". Diakses pada 28 November 2019 pukul 20.40. Dari web : https://www.paloaltonetworks.com/cyberpedia/what-is-an-it-security-policy.