NAMA : GITHA FADILLA O.P

NIM : 20200410700112

KELAS : Microsoft Platform Developer

TUGAS ASINKRON 1 MICROSOFT SECURITY COMPLIANCE, AND IDENTITY

Konsep Keamanan, Kepatuhan dan Identitas

Kasus:

Penerapan teknologi informasi membantu proses bisnis organisasi. Saat ini organisasi modern memerlukan model keamanan baru yang dapat beradaptasi lebih efektif dengan lingkungan modern yang kompleks. Model keamanan ini harus dapat mendukung tempat kerja hibrid, serta melindungi tenaga kerja, perangkat, aplikasi, dan data yang berada di berbagai tempat.

Saat ini Anda berada di posisi pimpinan perusahaan yang baru saja mengimplementasikan Microsoft 365 di perusahaan Anda. Dukungan teknologi ini akan dimanfaatkan untuk meningkatkan produktivitas dan mendukung kerja dalam tim staf perusahaan. Microsoft 365 tidak sebatas menyajikan aplikasi office untuk administrasi kantor harian, tetapi juga dukungan untuk kolaborasi antara pegawai-pegawai atau pegawai-pimpinan serta implementasi keamanan pada aplikasi.

1. Salah satu model pengamanan yang ada adalah Zero Trust.

a. Jelaskan konsep Zero Trust secara umum.

b. Tunjukkan implementasinya pada Microsoft 365. Berikan contoh konkrit berikut gambar yang mendukung.

Sertai referensi yang mendukung.

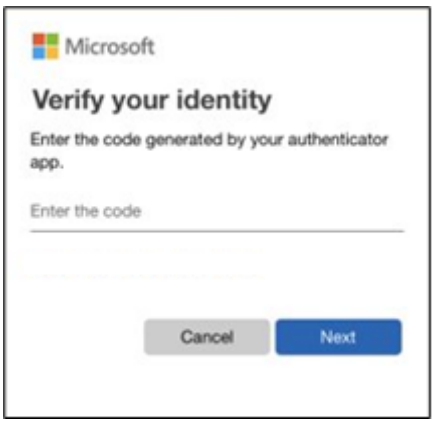
a. Konsep Zero Trust adalah suatu pendekatan keamanan yang didasarkan pada prinsip bahwa tidak ada entitas yang dapat dipercaya secara default, sehingga setiap permintaan atau akses ke suatu sumber daya harus diverifikasi secara independen sebelum diizinkan. Konsep ini melibatkan verifikasi dan validasi yang ketat pada setiap akses dan transaksi, menggunakan teknologi dan metode seperti autentikasi multifaktor, otorisasi dinamis, enkripsi, dan pemantauan yang ketat.

   Microsoft 365 adalah layanan cloud yang menyediakan berbagai aplikasi dan layanan produktivitas, termasuk email, kolaborasi, dan penyimpanan data. Microsoft telah mengadopsi konsep Zero Trust dalam platform Microsoft 365, dengan mengimplementasikan berbagai teknologi keamanan untuk

melindungi data pengguna dan memastikan akses yang aman ke layanan-layanan tersebut.

b. Salah satu contoh implementasi konsep Zero Trust pada Microsoft 365 adalah dengan menggunakan teknologi autentikasi multifaktor (MFA) dan otorisasi dinamis (Dynamic Authorization) pada layanan-layanan yang disediakan. Dengan menggunakan MFA, pengguna harus memasukkan lebih dari satu faktor autentikasi (seperti kata sandi dan kode verifikasi yang dikirim melalui SMS) sebelum diizinkan untuk mengakses akun mereka. Sedangkan dengan menggunakan Dynamic Authorization, Microsoft 365 dapat secara otomatis memberikan hak akses yang tepat berdasarkan kebutuhan pengguna, sehingga meminimalkan risiko akses yang tidak sah atau berlebihan.

Gambar berikut menunjukkan contoh proses autentikasi multifaktor pada layanan Microsoft 365:



Contoh autentikasi multifaktor pada layanan Microsoft 365

Referensi:

Microsoft. (2021). Microsoft 365 security. Retrieved from https://www.microsoft.com/en-us/microsoft-365/security

Microsoft. (2021). Zero Trust. Retrieved from https://www.microsoft.com/en-us/security/business/zero-trust

2. Salah satu mekanisme pengamanan Microsoft 365 adalah dengan menerapkan autentikasi. Berikan 2 contoh nyata beserta skenario pengamanan yang mungkin diterapkan pada layanan Microsoft 365. Sertakan referensi yang mendukung jika yang Anda jawab diperoleh dari suatu sumber.

a) Contoh pertama adalah autentikasi multifaktor (MFA), di mana pengguna harus memasukkan dua faktor autentikasi sebelum mereka dapat mengakses akun Microsoft 365 mereka. Faktor autentikasi tambahan dapat berupa kode yang diterima melalui SMS atau aplikasi autentikasi, sidik jari, atau pengenalan wajah. Skenario pengamanan yang mungkin diterapkan adalah ketika seorang pengguna mencoba untuk masuk dari lokasi atau perangkat yang tidak biasa, MFA akan dipicu untuk memastikan bahwa orang tersebut memang benar-benar pemilik akun. Hal ini dapat membantu mengurangi risiko serangan oleh pihak yang tidak sah yang mencoba untuk mengakses akun pengguna.

b) Contoh kedua adalah kebijakan kata sandi yang kuat, di mana Microsoft 365 memerlukan pengguna untuk membuat kata sandi yang kompleks dan memperbarui kata sandi mereka secara berkala. Skenario pengamanan yang mungkin diterapkan adalah ketika pengguna mencoba untuk memasukkan kata sandi yang lemah atau telah terlalu sering digunakan sebelumnya, mereka akan diminta untuk membuat kata sandi baru yang lebih kuat. Hal ini dapat membantu mengurangi risiko serangan brute-force atau serangan kata sandi yang lain.

Referensi:

"Multifactor authentication for Microsoft 365" Microsoft, https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/multi-factor-authentication-for-microsoft-365?view=o365-worldwide

"Password policy recommendations for Azure Active Directory" Microsoft, https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-policy-recommendations

3. Sebagai pimpinan Anda perlu mengadopsi pendekatan keamanan dari organisasi lain. Buka laman https://azure.microsoft.com/en-gb/services/active-directory/#customer-stories Pilih 2 kasus pada Customer Stories dan uraikan bagaimana implementasi pada 2 kasus tadi bisa Anda adopsi pada perusahaan Anda. Tuliskan 2 kasus yang Anda pilih dan berikan alasan jelas.

Setelah saya mencari informasi di laman https://azure.microsoft.com/en-gb/services/active-directory/#customer-stories, saya memilih dua kasus yang dapat diadopsi oleh perusahaan. Berikut adalah penjelasan mengenai kedua kasus tersebut beserta alasan mengapa bisa diadopsi oleh perusahaan:

a) Kasus Pertama: AmWINS Group, Inc.

AmWINS Group, Inc. adalah perusahaan asuransi terbesar di Amerika Serikat. Mereka menghadapi masalah dalam mengelola identitas dan akses pengguna dengan lebih dari 3.800 pengguna aktif dan 115 kantor di seluruh dunia. Mereka mengadopsi Azure Active Directory untuk meningkatkan keamanan dan efisiensi manajemen identitas. Dengan Azure Active Directory, AmWINS dapat mengelola akses pengguna dan hak istimewa di seluruh organisasi mereka dan mengurangi risiko terhadap serangan siber.

Implementasi yang bisa diadopsi oleh perusahaan adalah dengan mengadopsi Azure Active Directory sebagai platform manajemen identitas dan akses pengguna. Hal ini dapat membantu perusahaan untuk meningkatkan keamanan dan efisiensi manajemen identitas. Azure Active Directory memungkinkan perusahaan untuk mengelola akses pengguna dan hak istimewa di seluruh organisasi dan memperkenalkan tingkat keamanan yang lebih tinggi dengan autentikasi multifaktor.

b) Kasus Kedua: GE Aviation

GE Aviation adalah sebuah perusahaan yang bergerak di bidang produksi mesin pesawat dan layanan pendukungnya. Mereka menghadapi masalah dalam mempertahankan keamanan jaringan di seluruh lokasi dan sistem global mereka. GE Aviation memilih untuk mengadopsi Azure Active Directory untuk meningkatkan keamanan dan kontrol akses pengguna mereka. Dengan Azure Active Directory, mereka dapat mengelola akses pengguna dan hak istimewa secara terpusat dan memberikan tingkat keamanan yang lebih tinggi dengan autentikasi multifaktor dan pengawasan akses yang lebih ketat.

Implementasi yang bisa diadopsi oleh perusahaan adalah dengan mengadopsi Azure Active Directory untuk meningkatkan keamanan dan kontrol akses pengguna di seluruh lokasi dan sistem global mereka. Dengan Azure Active Directory,

perusahaan dapat mengelola akses pengguna dan hak istimewa secara terpusat dan memberikan tingkat keamanan yang lebih tinggi dengan autentikasi multifaktor dan pengawasan akses yang lebih ketat.

Alasan mengapa kedua kasus di atas dapat diadopsi oleh perusahaan adalah karena Azure Active Directory adalah platform manajemen identitas dan akses pengguna yang dapat membantu meningkatkan keamanan dan efisiensi manajemen identitas. Azure Active Directory memberikan tingkat keamanan yang lebih tinggi dengan autentikasi multifaktor dan pengawasan akses yang lebih ketat.