TUGAS ASINKRON 3

MICROSOFT SECURITY, COMPLIANCE, AND IDENTITY

Kasus:

Sebagai admin Anda bertugas menjaga keamanan sistem perusahaan dari akses pengguna yang tidak berhasil. Kebijakan dan prosedur yang diambil harus sesuai dengan kebutuhan perusahaan.

1. Suatu hari Anda diminta untuk menjaga akses ke sistem perusahaan hanya bisa dilakukan melalui jaringan yang terpercaya. Staf perusahaan yang mengakses melalui wifi umum tidak akan bisa mengakses. Buat desain conditionally access untuk kasus tersebut. Gunakan penerapan logika if-then untuk kasus ini.
   Jawaban :
   Desain Conditional Access untuk membatasi akses ke sistem perusahaan melalui jaringan terpercaya saja menggunakan logika if-then sebagai berikut:

   If user is accessing from trusted network
   Then allow access
   Else deny access

   Implementasi ini dapat dilakukan dengan membuat kebijakan Conditional Access di Azure Active Directory, memilih aplikasi atau sumber daya yang ingin dibatasi aksesnya, dan menentukan kondisi seperti lokasi jaringan yang terpercaya untuk memungkinkan akses.

2. Jelaskan yang dimaksud dengan siklus hidup identitas. Bagaimana mengatur siklus hidup identitas untuk staf yang ada di kantor Anda? Berikan contoh implementasinya.
   Jawaban :

   Siklus hidup identitas adalah proses pengelolaan akun pengguna dari awal hingga akhir, termasuk pembuatan, pengaturan hak akses, penghapusan, dan pembaruan data pengguna. Untuk mengatur siklus hidup identitas staf di kantor, perusahaan dapat mengimplementasikan tiga tahap berikut:

   - Provisioning: Pembuatan akun pengguna baru dengan hak akses yang sesuai.
   - Maintenance: Pembaruan informasi pengguna dan hak akses sesuai perubahan status kerja atau tugas.
   - Deprovisioning: Penghapusan akun pengguna saat pengguna tidak lagi membutuhkan akses ke sistem perusahaan.

   Contoh implementasi :

   dengan menggunakan Azure Active Directory untuk mengelola identitas dan akses pengguna. Perusahaan dapat memanfaatkan fitur fitur Azure AD seperti provisioning otomatis, penghapusan otomatis, dan integrasi dengan sumber daya yang berbeda untuk mengelola siklus hidup identitas staf.

3. Azure Active Directory (AD) access reviews memungkinkan organisasi mengelola keanggotaan grup, akses ke aplikasi perusahaan, dan penetapan peran secara efisien. Tinjauan akses rutin memastikan bahwa hanya staf yang tepat yang memiliki akses ke sumber daya. Resiko apa yang mungkin timbul saat seorang staf berpindah ke tim lain dengan hak akses yang berbeda? Bagaimana Azure AD access review bisa mengatasi hal ini? Berikan penjelasan dan alasannya.
   Jawaban :
   Risiko yang mungkin terjadi saat seorang staf berpindah ke tim lain dengan hak akses yang berbeda adalah kehilangan kontrol atas akses ke sumber daya yang tidak lagi relevan, atau pemberian akses yang tidak sesuai untuk tugas baru. Azure AD access review dapat mengatasi hal ini dengan melakukan peninjauan rutin pada keanggotaan grup, akses ke aplikasi perusahaan, dan penetapan peran. Fitur ini memungkinkan admin untuk melakukan peninjauan berkala dan memastikan bahwa hanya staf yang tepat yang memiliki akses ke sumber daya. Jika ada perubahan dalam tim atau tugas, admin dapat dengan cepat memperbarui hak akses staf dan mencegah potensi risiko.

4. Setiap perusahaan dapat menjadi target serangan jaringan. Salah satu serangan yang mungkin terjadi adalah DDoS.
   a. Jelaskan apa yang dimaksud dengan DDos
   b. Ada 3 tipe DDos yang sering terjadi. Sebutkan dan berikan penjelasan masing-masing.
   c. Bagaimana cara Azure melakukan proteksi terhadap serangan ini? Uraikan langkah-langkah yang mungkin Anda lakukan untuk mengatasi hal tersebut.

   Jawaban :

   a. DDoS (Distributed Denial of Service) adalah serangan yang dilakukan dengan cara mengirimkan sejumlah besar permintaan ke server atau jaringan dengan tujuan membuat layanan menjadi tidak tersedia atau melambat.
   b. Ada 3 tipe DDoS yang sering terjadi:

      - Volumetric: Serangan ini dilakukan dengan mengirimkan lalu lintas jaringan yang sangat besar ke server atau jaringan, sehingga membanjiri bandwidth dan membuat layanan menjadi tidak tersedia.

      - Protocol: Serangan ini dilakukan dengan mengeksploitasi celah di protokol jaringan atau aplikasi, sehingga membebani server atau jaringan dan membuat layanan menjadi tidak tersedia.

      - Application: Serangan ini dilakukan dengan mengeksploitasi celah pada aplikasi atau layanan tertentu, sehingga membuat layanan menjadi tidak tersedia atau lambat.

   c. Azure menyediakan layanan proteksi DDoS secara otomatis untuk semua layanan di Azure, yang terdiri dari dua lapisan prote