TUGAS ASINKRON 2 MICROSOFT SECURITY COMPLIANCE, AND IDENTITY

Tipe layanan dan identity dari Azure AD.

Soal

1. Anda adalah seorang Microsoft Security Engineer di salah satu perusahaan jasa. Anda diminta untuk melakukan pengamanan identitas untuk internal dan eksternal. Di Internal, Anda memiliki aplikasi website untuk tempat perusahaan Anda menjualkan jasanya yang dikembangkan oleh divisi development. Sedangkan pada eksternal Anda memiliki layanan Microsoft 365 dan Azure. Jelaskan alur kerja pengamanan identitas dari masing-masing kasus tersebut dengan Azure AD, baik internal maupun ekternal. Sangat disarankan Anda menggunakan diagram alur untuk menjelaskan langkah-langkahnya
   Jawaban :
   Untuk memahami alur kerja pengamanan identitas untuk kasus internal dan eksternal, kita perlu memahami bagaimana Azure AD berfungsi. Azure AD adalah layanan manajemen identitas cloud yang menyediakan autentikasi dan otorisasi untuk aplikasi cloud dan sumber daya seperti Microsoft 365, Azure, dan aplikasi web internal.
   Berikut adalah alur kerja pengamanan identitas untuk masing-masing kasus:
   a. Alur kerja kasus Internal

- Langkah 1: Pengguna mengakses aplikasi web internal yang dijaga oleh Azure AD
- Langkah 2: Azure AD memeriksa kredensial pengguna (username dan password) terhadap direktori Azure AD
- Langkah 3: Jika kredensial pengguna valid, Azure AD akan memberikan token akses ke pengguna
- Langkah 4: Token akses akan digunakan oleh pengguna untuk mengakses aplikasi web internal
- Langkah 5: Aplikasi web internal akan memverifikasi token akses pengguna dengan Azure AD sebelum memberikan akses ke sumber daya yang diminta pengguna.

   b. Alur kerja kasus Eksternal

- Langkah 1: Pengguna mencoba mengakses sumber daya seperti Microsoft 365 atau Azure
- Langkah 2: Pengguna akan diarahkan ke halaman masuk Azure AD
- Langkah 3: Pengguna memasukkan kredensialnya ke halaman masuk Azure AD
- Langkah 4: Azure AD memverifikasi kredensial pengguna terhadap direktori Azure AD
- Langkah 5: Jika kredensial pengguna valid, Azure AD akan memberikan token akses ke pengguna
- Langkah 6: Token akses akan digunakan oleh pengguna untuk mengakses sumber daya yang diminta

- Langkah 7: Sumber daya akan memverifikasi token akses pengguna dengan Azure AD sebelum memberikan akses ke sumber daya yang diminta pengguna.

2. Anda diminta untuk memilih edisi/tipe Azure AD yang cocok dan merupakan solusi minimal dari edisi yang disediakan. Perusahaan menginginkan akses bersyarat berbasis risiko ke aplikasi yang mereka kembangkan serta untuk mengamankan data penting yang terdapat di perusahaan tersebut. Edisi plan apa yang harus Anda pilih? Jelaskan alasan Anda memilih edisi tersebut

   Jawaban :

   Dalam kasus ini, edisi Azure AD yang paling cocok dan merupakan solusi minimal adalah Azure AD Premium Plan 1. Karena Azure AD Premium P1 menawarkan fitur yang memungkinkan akses berbasis risiko ke aplikasi, seperti Conditional Access dan Identity Protection. Dengan Conditional Access, perusahaan dapat membatasi akses ke aplikasi berdasarkan risiko pengguna, seperti lokasi, perangkat, atau perilaku pengguna. Dengan Identity Protection, Azure AD dapat mendeteksi ancaman keamanan dan memberikan tindakan yang tepat untuk melindungi akun pengguna.

   Selain itu, Azure AD Premium P1 juga menawarkan fitur-fiture keamanan seperti Multi-Factor Authentication dan Privileged Identity Management, yang dapat membantu mengamankan data penting di perusahaan.Dengan demikian, Azure AD Premium P1 adalah pilihan yang tepat untuk perusahaan yang ingin mengamankan akses ke aplikasi dan data penting mereka.

3. Jelaskan ketiga konsep berikut dan berikan perbandingan kapan Anda harus menggunakan dan kelebihan dari masing-masing konsep dibawah ini

   o Sinkronisasi hash kata sandi Azure AD.

   o Autentikasi Pass-through Microsoft Azure AD

   o Autentikasi federasi

   Jawaban:

   a. **Sinkronisasi hash kata sandi Azure AD**

   Sinkronisasi hash kata sandi Azure AD adalah fitur yang memungkinkan pengguna untuk menggunakan satu set kredensial untuk masuk ke aplikasi di lingkungan lokal dan cloud. Dalam konfigurasi ini, hash kata sandi dikirim dari lingkungan lokal ke Azure AD dan disimpan di sana. Saat pengguna mencoba untuk masuk ke aplikasi cloud, hash kata sandi dikirim ke Azure AD untuk memverifikasi bahwa pengguna memiliki kredensial yang benar. Keuntungan dari sinkronisasi hash kata sandi adalah memungkinkan pengguna untuk memiliki satu set kredensial untuk semua lingkungan, yang mengurangi kompleksitas manajemen kredensial.

   b. **Autentikasi Pass-through Microsoft Azure AD**

   Autentikasi Pass-through Microsoft Azure AD adalah fitur yang memungkinkan pengguna untuk masuk ke aplikasi cloud dengan menggunakan kredensial yang sama yang mereka gunakan untuk masuk ke lingkungan lokal. Dalam konfigurasi ini, kredensial pengguna tidak disimpan di cloud, melainkan disimpan di lingkungan lokal. Saat pengguna mencoba untuk masuk ke aplikasi cloud, permintaan otentikasi dikirim ke lingkungan lokal, yang memverifikasi bahwa pengguna memiliki kredensial yang benar. Keuntungan dari autentikasi Pass-through adalah memungkinkan pengguna untuk menggunakan kredensial yang sama di lingkungan lokal dan cloud, yang mengurangi kompleksitas manajemen kredensial.

   c. **Autentikasi federasi**

   Autentikasi federasi adalah fitur yang memungkinkan pengguna untuk masuk ke aplikasi cloud dengan menggunakan kredensial yang dikelola oleh penyedia identitas eksternal. Dalam konfigurasi ini, pengguna masuk ke penyedia identitas eksternal, yang memverifikasi bahwa pengguna memiliki kredensial yang benar. Setelah pengguna terotentikasi, penyedia identitas eksternal mengirimkan token otentikasi ke aplikasi cloud, yang memverifikasi bahwa pengguna memiliki izin untuk mengakses aplikasi tersebut. Keuntungan dari autentikasi federasi adalah memungkinkan pengguna untuk menggunakan kredensial yang mereka gunakan di lingkungan lain, seperti kredensial perusahaan, yang dapat meningkatkan keamanan dan mengurangi kompleksitas manajemen kredensial.

   Perbandingan:

   - Sinkronisasi hash kata sandi Azure AD dan autentikasi Pass-through Microsoft Azure AD keduanya memungkinkan pengguna untuk menggunakan kredensial yang sama di lingkungan lokal dan cloud, sedangkan autentikasi federasi

memungkinkan pengguna untuk menggunakan kredensial dari penyedia identitas eksternal.

- Sinkronisasi hash kata sandi Azure AD dan autentikasi Pass-through Microsoft Azure AD keduanya mengurangi kompleksitas manajemen kredensial, sedangkan autentikasi federasi dapat meningkatkan keamanan dengan memungkinkan pengguna untuk menggunakan kredensial perusahaan atau penyedia identitas eksternal.
- Sinkronisasi hash kata sandi Azure AD lebih cocok untuk organisasi yang ingin menggunakan satu set kredensial di semua lingkungan, sedangkan autentikasi Pass-through Microsoft Azure AD lebih cocok untuk organisasi yang ingin menggunakan kredensial lokal di cloud. Autentikasi federasi lebih cocok untuk organisasi yang ingin menggunakan kredensial dari penyedia identitas eksternal.
- Sinkronisasi hash kata sandi Azure AD dan autentikasi Pass-through Microsoft Azure AD lebih mudah diimplementasikan daripada autentikasi federasi. Autentikasi federasi memerlukan integrasi dengan penyedia identitas eksternal, yang dapat memakan waktu dan sumber daya yang lebih banyak.

Dalam memilih antara ketiga konsep tersebut, perlu dipertimbangkan kebutuhan organisasi dan tingkat keamanan yang diinginkan. Jika organisasi ingin menggunakan satu set kredensial di semua lingkungan, sinkronisasi hash kata sandi Azure AD dapat menjadi pilihan yang tepat. Jika organisasi ingin menggunakan kredensial lokal di cloud, autentikasi Pass-through Microsoft Azure AD dapat menjadi pilihan yang tepat. Jika organisasi ingin meningkatkan keamanan dengan menggunakan kredensial perusahaan atau penyedia identitas eksternal, autentikasi federasi dapat menjadi pilihan yang tepat.

4. Jelaskan apa perbedaan otentikasi dan otorisasi. Ketika Anda dapat melihat OneDrive for Business di portal.office.com, layanan tersebut termasuk pada bagian apa?
   Jawaban :
   Perbedaan Otentikasi dan Otorisasi
   Otentikasi dan otorisasi adalah dua konsep penting dalam dunia keamanan informasi. Otentikasi mengacu pada proses verifikasi identitas seseorang atau perangkat, sedangkan otorisasi mengacu pada proses memberikan izin atau akses ke sistem atau sumber daya tertentu.
   Proses otentikasi dapat melibatkan penggunaan nama pengguna dan kata sandi, sertifikat digital, atau fitur biometrik seperti sidik jari atau pemindaian wajah. Setelah seseorang atau perangkat terotentikasi, mereka dapat diberikan izin atau akses ke sistem atau sumber daya tertentu melalui proses otorisasi.
   Proses otorisasi melibatkan penggunaan aturan dan kebijakan untuk menentukan siapa yang memiliki hak akses ke sistem atau sumber daya tertentu. Misalnya, administrator sistem dapat menentukan bahwa hanya pengguna tertentu yang memiliki hak akses ke folder tertentu, atau bahwa hanya pengguna dengan tingkat akses tertentu yang dapat mengedit file tertentu.
   Dalam ringkasan, otentikasi adalah proses verifikasi identitas, sedangkan otorisasi adalah proses memberikan izin atau akses.
   OneDrive for Business
   OneDrive for Business adalah layanan penyimpanan awan yang ditawarkan oleh Microsoft sebagai bagian dari paket Office 365. Layanan ini memungkinkan pengguna untuk menyimpan, mengakses, dan berbagi file dan dokumen dari mana saja dan kapan saja melalui internet.
   Dalam portal.office.com, OneDrive for Business termasuk dalam bagian "Aplikasi" bersama dengan aplikasi Office 365 lainnya seperti Outlook, Word, Excel, dan PowerPoint. Pengguna dapat mengakses OneDrive for Business dengan mengklik ikon aplikasi OneDrive di portal.office.com.

5. Apa metode otentikasi paling aman menurut Anda? Jelaskan alasan Anda?
   Jawaban :
   Menurut saya, metode otentikasi paling aman saat ini adalah otentikasi multifaktor (MFA) atau juga dikenal sebagai dua faktor otentikasi (2FA). Metode ini memerlukan lebih dari satu faktor untuk memverifikasi identitas pengguna, yang biasanya terdiri dari kombinasi antara password, token akses, atau biometrik seperti sidik jari atau pengenalan wajah.
   Berikut adalah alasan mengapa saya memilih otentikasi multifaktor sebagai metode otentikasi yang paling aman:

a) Membutuhkan lebih dari satu faktor Dalam otentikasi multifaktor, pengguna harus memasukkan lebih dari satu faktor untuk memverifikasi identitas mereka. Dengan demikian, meskipun password pengguna telah dicuri atau dibocorkan, penyerang tetap tidak dapat mengakses akun pengguna tanpa faktor otentikasi tambahan seperti token akses atau biometrik.
b) Meningkatkan kesulitan bagi penyerang Dengan menggunakan otentikasi multifaktor, penyerang harus mendapatkan akses tidak hanya ke password pengguna, tetapi juga faktor otentikasi tambahan seperti token akses atau perangkat biometrik pengguna. Hal ini membuatnya lebih sulit bagi penyerang untuk mencuri atau memalsukan informasi otentikasi.
c) Menyediakan lapisan keamanan tambahan Otentikasi multifaktor juga menyediakan lapisan keamanan tambahan yang dapat membantu melindungi akun pengguna dari serangan phishing atau serangan malware. Sebagai contoh, ketika pengguna menggunakan token akses untuk otentikasi, penyerang yang mencoba untuk mencuri kredensial pengguna melalui phishing tidak akan dapat memperoleh token akses tersebut.
d) Mendukung peraturan keamanan dan privasi Otentikasi multifaktor juga dapat membantu organisasi memenuhi persyaratan keamanan dan privasi yang diperlukan oleh undang-undang atau peraturan, seperti PCI-DSS atau HIPAA.

   Dalam kesimpulannya, otentikasi multifaktor adalah metode otentikasi yang paling aman karena memerlukan lebih dari satu faktor untuk memverifikasi identitas pengguna, meningkatkan kesulitan bagi penyerang, menyediakan lapisan keamanan tambahan, dan mendukung peraturan keamanan dan privasi. Oleh karena itu, saya sangat merekomendasikan penggunaan otentikasi multifaktor sebagai metode otentikasi yang paling aman.

6. Berikan penjelasan dan alur kerja dari Multi factor authentication di Azure AD
   Jawaban :
   Multi-Factor Authentication (MFA) di Azure AD adalah metode otentikasi yang memerlukan pengguna untuk memasukkan lebih dari satu faktor untuk memverifikasi identitas mereka. Azure AD MFA menyediakan lapisan keamanan tambahan dan melindungi akun pengguna dari serangan phishing atau serangan malware. Berikut adalah alur kerja dari MFA di Azure AD:
   a) Pengguna memasukkan nama pengguna dan kata sandi mereka pada halaman masuk Azure AD.
   b) Azure AD memeriksa apakah pengguna telah mengaktifkan MFA. Jika pengguna tidak mengaktifkan MFA, mereka akan diminta untuk mengaktifkannya terlebih dahulu.
   c) Jika pengguna telah mengaktifkan MFA, Azure AD akan meminta pengguna untuk memasukkan faktor otentikasi tambahan. Pengguna dapat memilih faktor otentikasi yang ingin mereka gunakan, seperti aplikasi otentikasi, pesan teks, panggilan telepon, atau perangkat biometrik seperti sidik jari atau pengenalan wajah.
   d) Setelah pengguna memasukkan faktor otentikasi tambahan, Azure AD memeriksa apakah faktor otentikasi tersebut cocok dengan yang telah dikonfigurasi untuk akun pengguna.
   e) Jika faktor otentikasi yang dimasukkan pengguna sesuai, Azure AD memberikan izin akses ke akun pengguna.
   f) Jika faktor otentikasi yang dimasukkan pengguna tidak sesuai, Azure AD akan menolak akses ke akun pengguna.
      Dalam kesimpulannya, MFA di Azure AD adalah metode otentikasi yang memerlukan pengguna untuk memasukkan lebih dari satu faktor untuk memverifikasi identitas mereka. MFA menyediakan lapisan keamanan tambahan dan melindungi akun pengguna dari serangan phishing atau serangan malware. Alur kerja MFA di Azure AD melibatkan memeriksa apakah pengguna telah mengaktifkan MFA, meminta pengguna untuk memasukkan faktor otentikasi tambahan, dan memeriksa apakah faktor otentikasi yang dimasukkan pengguna sesuai dengan yang telah dikonfigurasi untuk akun pengguna.

7. Kapan seharusnya perusahaan menggunakan self-service password reset?
   Jawaban :
   Self-service password reset (SSPR) adalah fitur yang memungkinkan pengguna untuk mereset kata sandi mereka sendiri tanpa perlu menghubungi helpdesk atau administrator sistem. Fitur ini dapat membantu mengurangi beban kerja untuk tim IT dan memberikan pengguna kemampuan untuk mengontrol kata sandi mereka sendiri dengan lebih mudah.
   Perusahaan seharusnya menggunakan self-service password reset jika mereka ingin:

- Mengurangi beban kerja untuk tim IT: Dengan SSPR, pengguna dapat mereset kata sandi mereka sendiri tanpa perlu menghubungi helpdesk atau administrator sistem. Ini dapat membantu mengurangi beban kerja untuk tim IT, yang dapat fokus pada tugas-tugas yang lebih kompleks.

- Meningkatkan produktivitas pengguna: Dengan SSPR, pengguna dapat mereset kata sandi mereka sendiri dengan cepat dan mudah, tanpa perlu menunggu bantuan dari tim IT. Ini dapat membantu meningkatkan produktivitas pengguna dan mengurangi waktu henti yang tidak perlu.
- Meningkatkan keamanan: Dengan SSPR, pengguna dapat mereset kata sandi mereka sendiri dengan cepat dan mudah, sehingga mereka dapat segera mengambil tindakan jika terjadi pelanggaran keamanan. Ini dapat membantu meningkatkan keamanan perusahaan dengan memastikan bahwa kata sandi pengguna selalu terkendali dan aman.
  Namun, perusahaan seharusnya juga mempertimbangkan beberapa faktor sebelum mengimplementasikan SSPR, seperti:
- Tingkat keamanan yang diperlukan: SSPR memungkinkan pengguna untuk mereset kata sandi mereka sendiri, yang dapat berpotensi menjadi celah keamanan. Oleh karena itu, perusahaan harus memastikan bahwa SSPR diimplementasikan dengan benar dan bahwa ada kontrol keamanan yang memadai untuk mencegah penyalahgunaan.
- Kebutuhan untuk kepatuhan: Beberapa regulasi dan standar industri mungkin memerlukan perusahaan untuk memperketat kontrol akses ke sistem dan sumber daya. Dalam hal ini, SSPR mungkin tidak cocok untuk kebutuhan kepatuhan yang diperlukan.
- Biaya dan kompleksitas: Implementasi SSPR dapat memerlukan biaya dan usaha yang signifikan, terutama jika perusahaan harus mengintegrasikan SSPR dengan infrastruktur IT yang ada. Perusahaan harus mempertimbangkan biaya dan kompleksitas sebelum mengimplementasikan SSPR.

  Dalam kesimpulannya, perusahaan seharusnya menggunakan self-service password reset jika mereka ingin mengurangi beban kerja untuk tim IT, meningkatkan produktivitas pengguna, dan meningkatkan keamanan. Namun, perusahaan juga harus mempertimbangkan faktor-faktor seperti tingkat keamanan yang diperlukan, kebutuhan untuk kepatuhan, dan biaya dan kompleksitas sebelum mengimplementasikan SSPR.