Nama : Muhammad Iqbal Gofur
NIM : 1310651039
Kelas : TI-A

- **KONSEP CORNERSTONE KEAMANAN INFORMASI**

Sebelum kita bisa menjelaskan kontrol akses , kita harus mendefinisikan keamanan informasi landasan konsep . Konsep-konsep ini memberikan dasar yang di atasnya 10 domain

Tubuh umum Pengetahuan dibangun yaitu :

1. **Kerahasiaan** berusaha untuk mencegah pengungkapan yang tidak sah, Dengan kata lain, kerahasiaan berusaha untuk mencegah akses yang tidak sah. Contoh dari serangan kerahasiaan akan pencurian pribadi, seperti menyalahgunakan akun social media.
2. **Integritas** Integritas berusaha untuk mencegah modifikasi yang tidak sah dari informasi . Dengan kata lain, integritas berusaha untuk mencegah akses tulis tidak sah ke data. Ada dua jenis integritas : integritas data dan integritas sistem.
3. **Ketersediaan**, ketersediaan memastikan bahwa informasi yang tersedia bila diperlukan. Sistem harus dapat digunakan (tersedia) untuk penggunaan bisnis normal. Contoh dari serangan terhadap ketersediaan akan menjadi (DoS) serangan Denial -of -Service , yang berusaha untuk menolak layanan (atau ketersediaan) dari sistem.
4. **Pengungkapan , perubahan , dan perusakan** CIA triad juga dapat dijelaskan oleh kebalikannya : Pengungkapan , Perubahan , dan Destruction (DAD) . Pengungkapan adalah pengungkapan yang tidak sah informasi perubahan adalah modifikasi yang tidak sah dari data, dan kehancuran adalah membuat sistem tidak tersedia . Sementara singkatan CIA kadang-kadang berubah.
5. **Identitas dan otentikasi, otorisasi, dan akuntabilitas,** Istilah "AAA" sering digunakan, menggambarkan landasan konsep Authentication, Otorisasi, dan Akuntabilitas.

6. **Identitas dan otentikasi.** Identitas adalah klaim: jika nama Anda adalah "Orang X" Anda mengidentifikasi diri dengan mengatakan "Saya Orang X", identitas saja lemah karena tidak ada bukti. Anda juga dapat mengidentifikasi diri dengan mengatakan "Saya Orang Y." Membuktikan klaim identitas disebut otentikasi.
7. **Otorisasi,** menjelaskan tindakan yang dapat Anda lakukan pada sistem setelah Anda telah mengidentifikasi dan dikonfirmasi. Tindakan mungkin termasuk membaca, menulis, atau file eksekusi atau program.
8. **Akuntabilitas** memegang penanggungjawab atas tindakan mereka. Hal ini biasanya dicapai dengan login dan menganalisis data audit. Menegakkan akuntabilitas membantu menjaga "Orang-orang jujur jujur."
9. **Nonrepudiation,** berarti pengguna tidak dapat menyangkal (menolak) setelah dilakukan transaksi. Ini menggabungkan otentikasi dan integritas: nonrepudiation mengotentikasi identitas dari pengguna yang melakukan transaksi dan memastikan integritas transaksi itu. Anda harus memiliki kedua otentikasi dan integritas untuk memiliki nonrepudiation.
10. **Kontrol akses nondiscretionary** Peran Berbasis Access Control (RBAC) mendefinisikan bagaimana informasi diakses pada sistem berdasarkan peran subjek. RBAC adalah jenis kontrol akses nondiscretionary karena pengguna tidak memiliki kebijaksanaan mengenai kelompok benda mereka diizinkan untuk mengakses dan tidak mampu untuk mentransfer objek untuk mata pelajaran lainnya. Kontrol akses tugas berbasis model kontrol akses nondiscretionary lain, berkaitan dengan RBAC . Kontrol akses tugas berbasis didasarkan pada tugas masing-masing harus tunduk.

- **Akses kontrol berbasis aturan**

  Sebuah sistem kontrol akses berbasis aturan menggunakan serangkaian aturan yang ditetapkan, pembatasan, dan filter untuk mengakses objek dalam suatu sistem. Aturan-aturan dalam bentuk "Jika / kemudian" pernyataan.

- **Kontrol akses terpusat**

  Kontrol akses terpusat berkonsentrasi kontrol akses di satu titik logis untuk sistem atau organisasi. Kontrol akses terpusat dapat digunakan untuk menyediakan Single Sign-On (SSO), di mana subjek dapat mengotentikasi sekali, dan kemudian mengakses beberapa

sistem. Kontrol akses terpusat dapat terpusat menyediakan tiga "A" dari kontrol akses: Otentikasi, Otorisasi, dan akuntabilitas.

- **Daftar kontrol akses**

  Daftar kontrol akses (ACL) digunakan di seluruh banyak kebijakan keamanan IT, prosedur, dan teknologi. Daftar kontrol akses adalah daftar objek; setiap entri menggambarkan mata pelajaran yang dapat mengakses objek tersebut. Akses upaya subjek untuk obyek yang tidak memiliki entri yang cocok pada ACL akan ditolak.

- **Akses pengadaan siklus hidup**

  Akses penyediaan siklus hidup harus dijaga dan diamankan. Sementara banyak organisasi ikuti praktik terbaik untuk mengeluarkan akses, banyak kekurangan proses formal untuk memastikan seumur hidup akses disimpan aman. IBM menjelaskan aturan siklus hidup identitas berikut:

  • "Password pemeriksaan kepatuhan kebijakan

  • Memberitahu pengguna untuk mengubah password mereka sebelum mereka berakhir

  • Mengidentifikasi hidup perubahan siklus seperti rekening yang tidak aktif selama lebih dari 30 hari berturut-turut

  • Mengidentifikasi akun baru yang belum digunakan selama lebih dari 10 hari setelah penciptaan mereka

- **Hak pengguna, akses review, dan audit**

  Akses agregasi terjadi sebagai pengguna individu memperoleh lebih banyak akses ke banyak sistem. Ini dapat terjadi secara sengaja, sebagai fungsi Single Sign-On (SSO). Hal ini juga dapat terjadi tidak sengaja: pengguna sering mendapatkan hak baru (juga disebut hak akses) karena mereka mengambil peran atau tugas baru. Hal ini dapat mengakibatkan otorisasi merayap: pengguna mendapatkan lebih banyak hak tanpa penumpahan yang lama. Kekuatan hak-hak ini dapat senyawa dari waktu ke waktu, mengalahkan kontrol seperti hak istimewa setidaknya dan pemisahan tugas. Hak pengguna harus secara rutin ditinjau dan diaudit.

- **Protokol kontrol akses dan kerangka kerja**

Kedua model sentralisasi dan desentralisasi dapat mendukung pengguna jauh otentikasi untuk sistem lokal. Sejumlah protokol dan kerangka kerja dapat digunakan untuk mendukung ini butuhkan, termasuk RADIUS, Diameter, TACACS / TACACSþ, PAP, dan CHAP. RADIUS Remote Authentication Dial-In Service Pengguna (RADIUS) protokol adalah pihak ketiga sistem otentikasi. RADIUS menggunakan User Datagram Protocol (UDP) port 1812 (Otentikasi) dan 1813 (akuntansi). RADIUS dianggap sebagai "AAA" sistem, yang terdiri dari tiga komponen: otentikasi, otorisasi, dan akuntansi. Ini mengotentikasi kredensial subjek terhadap database otentikasi. Ini kewenangan pengguna dengan memungkinkan pengguna tertentu ' akses ke objek data tertentu.

- **Diameter**

  Diameter adalah RADIUS 'penerus, dirancang untuk memberikan Authentication ditingkatkan, Otorisasi, dan Akuntansi (AAA) kerangka. RADIUS menyediakan terbatas akuntabilitas dan memiliki masalah dengan fleksibilitas, skalabilitas, kehandalan, dan keamanan. Diameter lebih fleksibel, yang memungkinkan dukungan bagi pengguna jarak jauh ponsel, misalnya. TACACS dan TACACS1

- **Terminal Access Controller Access Control System (TACACS)** adalah terpusat

  Sistem kontrol akses yang mengharuskan pengguna untuk mengirim ID dan statis (reusable) password untuk otentikasi. TACACS menggunakan port UDP 49 (dan mungkin juga menggunakan TCP). Reusable password memiliki kerentanan keamanan: ditingkatkan TACACSþ memberikan yang lebih baik proteksi password dengan memungkinkan otentikasi dua faktor yang kuat. TACACSþ tidak kompatibel dengan TACACS. TACACS menggunakan TCP Port 49 untuk otentikasi dengan TACACS server.

- **KATEGORI AKSES KONTROL**

  Untuk memahami dan tepat menerapkan kontrol akses , pemahaman apa manfaat setiap kontrol dapat menambah keamanan sangat penting. Pada bagian ini, setiap jenis kontrol akses akan ditentukan atas dasar bagaimana menambah keamanan sistem .

  Ada enam jenis kontrol akses :

  - Pencegahan
  - Detektif
  - Corrective

• Pemulihan
• Pencegah
• Kompensasi

- **Pencegah**

  Kontrol preventif mencegah tindakan yang terjadi. Ini berlaku pembatasan untuk apa potensi pengguna, baik resmi atau tidak sah, dapat dilakukan. Contoh dari Access Control Defensive Kategori dan Jenis 7 Kontrol pencegahan administrasi adalah skrining obat pra kerja. Dirancang untuk mencegah organisasi dari mempekerjakan seorang karyawan yang menggunakan obat-obatan terlarang.

- **Detektif**

  Kontrol detektif adalah kontrol yang siaga selama atau setelah serangan yang berhasil. Intrusi sistem deteksi sinyal setelah serangan sukses, kamera televisi sirkuit tertutup (CCTV) yang penjaga waspada terhadap penyusup, dan sistem bangunan alarm yang dipicu oleh penyusup merupakan contoh dari kontrol detektif.

- **Pemulihan**

  Setelah insiden keamanan telah terjadi, kontrol pemulihan mungkin perlu diambil dalam memesan untuk mengembalikan fungsi dari sistem dan organisasi. Pemulihan berarti bahwa sistem harus pulih: diinstal ulang dari OS Media atau gambar, data dikembalikan dari backup, dll

- **Pencegah**

  Kontrol jera mencegah pengguna dari melakukan tindakan pada sistem. Contohnya termasuk "Waspadalah terhadap anjing" tanda: pencuri menghadapi dua bangunan, satu dengan anjing penjaga dan satu tanpa, lebih mungkin untuk menyerang bangunan tanpa anjing penjaga.

- **Kompensasi**

  Sebuah kontrol kompensasi adalah kontrol keamanan tambahan dimasukkan ke dalam tempat untuk mengkompensasi kelemahan dalam kontrol lainnya.

- **METODE AUTHENTIKASI**

Sebuah konsep kunci untuk melaksanakan jenis kontrol akses mengendalikan tepat otentikasi subyek dalam sistem IT . Subjek A pertama mengidentifikasi dirinya atau dirinya ; Identifikasi ini tidak bisa dipercaya . Subjek kemudian mengotentikasi dengan menyediakan jaminan bahwa identitas diklaim berlaku . Satu set credential adalah istilah yang digunakan untuk kombinasi keduanya identifikasi dan otentikasi pengguna.

- **Password**

Password telah menjadi landasan untuk kontrol akses ke sistem TI. Mereka relatif mudah dan murah untuk melaksanakan. Banyak perbankan, layanan portofolio saham online, Web mail pribadi, dan kesehatan sistem masih menggunakan nama pengguna dan password sebagai Metode kontrol akses. Ada empat jenis password untuk dipertimbangkan ketika menerapkan kontrol akses: password statis, passphrase, satu kali password, dan password dinamis.

- **TECHNOLOGIES ACCESS CONTROL**

Ada beberapa teknologi yang digunakan untuk pelaksanaan kontrol akses. Karena setiap teknologi disajikan , penting untuk mengidentifikasi apa yang unik tentang masing-masing solusi teknis.

- **Single sign-on**

Sign-On tunggal (SSO) memungkinkan beberapa sistem untuk menggunakan server otentikasi pusat (AS) . Hal ini memungkinkan pengguna untuk mengotentikasi sekali dan kemudian mengakses beberapa , sistem yang berbeda. Hal ini juga memungkinkan administrator keamanan untuk menambah, mengubah , atau mencabut hak penggunapada satu sistem pusat . Kerugian utama untuk SSO itu memungkinkan penyerang untuk mendapatkan akses ke beberapa sumber setelah mengorbankan salah satu metode otentikasi , seperti password. SSO harus selalu digunakan dengan otentikasi multifaktor untuk alasan ini .