ACCESS CONTROL

Tujuan dari kontrol akses adalah untuk memungkinkan pengguna yang berwenang mengakses data yang sesuai dan menolak akses ke pengguna yang tidak sah. Kontrol akses melindungi ancaman seperti akses yang tidak sah, modifikasi data, dan hilangnya kerahasiaan.

Kerahasiaan, integritas, dan ketersediaan

Kerahasiaan, integritas, dan Ketersediaan adalah konsep landasan "triad CIA" keamanan informasi. Triad, yang ditunjukkan pada Gambar 1.1, membentuk tiga bagian keamanan informasi bangku dibangun di atas. Urutan akronim dapat berubah (beberapa "AIC" mungkin untuk menghindari hubungan dengan badan intelijen tertentu), kecuali konsep-konsep yang penting.

Kerahasiaan

Kerahasiaan bertujuan untuk mencegah pengungkapan informasi yang tidak sah (hal itu membuat data tetap aman). Dengan kata lain, kerahasiaan berusaha untuk mencegah akses yang tidak sah untuk membaca data. Contoh dari serangan kerahasiaan akan pencurian Personally Iden- tifiable Information (PII), seperti informasi kartu kredit.

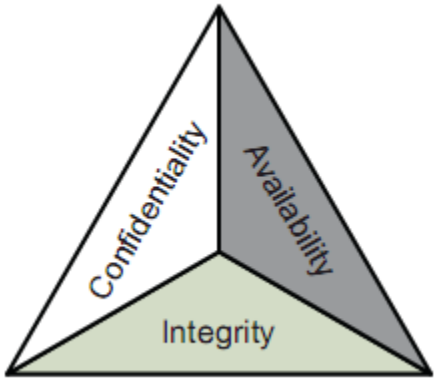

FIGURE 1.1

Integritas

Integritas bertujuan untuk mencegah modifikasi informasi yang tidak sah. Dengan kata lain, integritas berusaha untuk mencegah akses tulis tidak sah ke data.

Ketersediaan

Tersedianya ketersediaan memastikan bahwa informasi yang tersedia bila diperlukan. Sistem harus dapat digunakan (tersedia) untuk penggunaan bisnis normal. Contoh dari serangan terhadap ketersediaan akan menjadi serangan (DoS) Denial-of-Service, yang berusaha untuk menolak layanan (atau availability) dari sistem.

Pengungkapan, pengubahan, dan perusakan

CIA triad juga dapat dijelaskan oleh kebalikannya: Pengungkapan, Perubahan, dan Perusakan. Pengungkapan adalah pengungkapan informasi yang tidak sah; pengubahan adalah modifikasi yang tidak sah dari data, dan perusakan adalah membuat sistem tidak tersedia.

Identitas dan Autentikasi

Identitas adalah klaim: jika nama anda adalah "X," Anda mengidentifikasi diri dengan mengatakan "Saya X. "Identitas saja lemah karena tidak ada bukti. anda juga dapat mengidentifikasi diri dengan mengatakan "Saya Y." Membuktikan klaim identitas disebut authentication: anda mengotentikasi klaim identitas, biasanya dengan menyediakan sepotong informasi atau sebuah benda yang hanya anda miliki, seperti password atau paspor anda.

Autorisasi

Otorisasi menjelaskan tindakan yang dapat performon sebuah systemonce Anda memiliki identified dan dikonfirmasi. Tindakan mungkin termasuk membaca, menulis, atau file eksekusi atau program.

Akuntabilitas

Akuntabilitas memegang tanggung jawab atas tindakan mereka. Ini biasanya dilakukan dengan login dan menganalisis data audit. Menegakkan akuntabilitas membantu menjaga "Orang-orang jujur." Untuk beberapa pengguna, mengetahui bahwa data login tidak cukup untuk memberikan akuntabilitas: mereka harus tahu bahwa data yang dicatat dan diaudit dan sanksi mungkin akibat dari pelanggaran kebijakan.

Nonrepudiation

Nonrepudiation berarti pengguna tidak dapat menyangkal (menolak) setelah dilakukan sebuah transaksi. Ini menggabungkan otentikasi dan integritas: nonrepudiation mengotentikasi identitas dari pengguna yang melakukan transaksi dan memastikan integritas transaksi itu. Kalian harus memiliki kedua otentikasi dan integritas untuk memiliki nonrepudiation: membuktikan Anda menandatangani kontrak untuk membeli mobil.

Least privilege and need to know

Least privilege berarti pengguna harus diberikan jumlah minimum akses (otorisasi) diperlukan untuk melakukan pekerjaan mereka, tapi tidak lebih. Least privilege diterapkan untuk kelompok benda. Need to know lebih rinci dari Least privilege: pengguna harus tahu bagian tertentu dari informasi sebelum mengakses itu.

Subyek dan obyek

Sebuah subjek merupakan entitas yang aktif pada sistem data. Sebagian contoh pelajaran melibatkan orang mengakses file data. Namun, program komputer yang menjalankan adalah subyek demikian juga. Sebuah objek adalah data pasif dalam sistem. Benda dapat berkisar from database ke file teks. Hal penting untuk diingat tentang obyek adalah bahwa mereka pasif dalam sistem. Mereka tidak memanipulasi benda-benda lain. 3 Konsep Cornerstone Keamanan Informasi

Defense-in-depth

Defense-in-depth (juga disebut pertahanan berlapis) berlaku beberapa perlindungan (juga disebut kontrol: tindakan yang diambil untuk mengurangi resiko) untuk melindungi aset. Setiap keamanan tunggal control mungkin gagal; dengan mengerahkan beberapa kontrol, Anda meningkatkan kerahasiaan, integritas, dan ketersediaan data Anda.