

## Keamanan Dan Manajemen Perusahaan

Seringkali sulit untuk membujuk manajemen perusahaan atau pemilik sistem informasi untuk melakukan investasi di bidang keamanan. Di tahun 1997 majalah Information Week melakukan survey terhadap 1271 *system* atau *network manager* di Amerika Serikat. Hanya 22% yang menganggap keamanan sistem informasi sebagai komponen sangat penting (“*extremely important*”). Mereka lebih mementingkan “*reducing costi*” dan “*improving competitiveness*” meskipun perbaikan sistem informasi setelah dirusak justru dapat menelan biaya yang lebih banyak.

Keamanan itu tidak dapat muncul demikian saja. Dia harus direncanakan. Ambil contoh berikut. Jika kita membangun sebuah rumah, maka pintu rumah kita harus dilengkapi dengan kunci pintu. Jika kita terlupa memasukkan kunci pintu pada budget perencanaan rumah, maka kita akan dikagetkan bahwa ternyata harus keluar dana untuk menjaga keamanan.

Kalau rumah kita hanya memiliki satu atau dua pintu, mungkin dampak dari budget tidak seberapa. Bayangkan bila kita mendesain sebuah hotel dengan 200 kamar dan lupa membudgetkan kunci pintu. Dampaknya sangat besar. Demikian pula di sisi pengamanan sebuah sistem informasi. Jika tidak kita budgetkan di awal, kita akan dikagetkan dengan kebutuhan akan adanya perangkat pengamanan (firewall, Intrusion Detection System, anti virus, Dissaster Recovery Center, dan seterusnya).

Meskipun sering terlihat sebagai besaran yang tidak dapat langsung diukur dengan uang (*intangible*), keamanan sebuah sistem informasi sebetulnya dapat diukur dengan besaran yang dapat diukur dengan uang (*tangible*). Dengan adanya ukuran yang terlihat, mudah-mudahan pihak manajemen dapat mengerti pentingnya investasi di bidang keamanan. Berikut ini adalah berapa contoh kegiatan yang dapat kita lakukan :

- ▶ Hitung kerugian apabila sistem informasi kita tidak bekerja selama 1 jam, selama 1 hari, 1 minggu, dan 1 bulan. (Sebagai perbandingan, bayangkan jika server Amazon.com tidak dapat diakses selama beberapa hari. Setiap harinya dia dapat menderita kerugian beberapa juta dolar.)
- ▶ Hitung kerugian apabila ada kesalahan informasi (data) pada sistem informasi anda. Misalnya web site anda mengumumkan harga sebuah barang yang berbeda dengan harga yang ada di toko kita.
- ▶ Hitung kerugian apabila ada data yang hilang, misalnya berapa kerugian yang diderita apabila daftar pelanggan dan invoice hilang dari sistem kita. Berapa biaya yang dibutuhkan untuk rekonstruksi data.
- ▶ Apakah nama baik perusahaan kita merupakan sebuah hal yang harus dilindungi? Bayangkan bila sebuah bank terkenal dengan rentannya pengamanan data-datanya, bolak-balik terjadi *security incidents*. Tentunya banyak nasabah yang pindah ke bank lain karena takut akan keamanan uangnya.

Pengelolaan terhadap keamanan dapat dilihat dari sisi pengelolaan resiko (risk management). Lawrie Brown dalam menyarankan menggunakan “*Risk Management Model*” untuk menghadapi ancaman (*managing threats*). Ada tiga komponen yang memberikan kontribusi kepada Risk, yaitu *Asset*, *Vulnerabilities*, dan *Threats*.

Nama Komponen	Contoh & Keterangan Lebih Lanjut
Asset (Aset)	<ul style="list-style-type: none"> <li>▪ Hardware</li> <li>▪ Software</li> <li>▪ Dokumentasi</li> <li>▪ Data</li> <li>▪ Komunikasi</li> <li>▪ Lingkungan</li> <li>▪ Manusia</li> </ul>
Threats (Ancaman)	<ul style="list-style-type: none"> <li>▪ Pemakai (Users)</li> <li>▪ Teroris</li> <li>▪ Kecelakaan (Accidents)</li> <li>▪ Crackers</li> <li>▪ Penjahat Kriminal</li> <li>▪ Nasib (Acts Of God)</li> <li>▪ Intel Luar Negeri (Foreign Intelligence)</li> </ul>
Vulnerability (Kelemahan)	<ul style="list-style-type: none"> <li>▪ Software Bugs</li> <li>▪ Hardware Bugs</li> <li>▪ Radiasi (dari layar, transmisi)</li> <li>▪ Tapping, Crosstalk</li> <li>▪ Unauthorized Users</li> <li>▪ Cetakan, Hardcopy</li> <li>▪ Keteledoran (Oversight)</li> <li>▪ Cracker via telepon</li> <li>▪ Storage media</li> </ul>

Tabel Kontribusi Terhadap Risk

Untuk menanggulangi resiko (*Risk*) tersebut dilakukan apa yang disebut “*countermeasures*” yang dapat berupa :

- ▶ Usaha untuk mengurangi *Threat*
- ▶ Usaha untuk mengurangi *Vulnerability*
- ▶ Usaha untuk mengurangi dampak (*impact*)
- ▶ Mendeteksi kejadian yang tidak bersahabat (*hostile event*)
- ▶ Kembali (*recover*) dari kejadian

### **Meningkatnya Kejahatan Komputer**

Jumlah kejahatan komputer (*computer crime*), terutama yang berhubungan dengan sistem informasi, akan terus meningkat dikarenakan beberapa hal, antara lain :

- ▶ Aplikasi bisnis yang menggunakan (berbasis) teknologi informasi dan jaringan komputer semakin meningkat. Sebagai contoh saat ini mulai bermunculan aplikasi bisnis seperti *on-line banking*, *electronic commerce (e-commerce)*, *Electronic Data Interchange (EDI)*, dan masih banyak lainnya. Bahkan aplikasi *e-commerce* akan menjadi salah satu aplikasi pemacu di Indonesia (melalui “Telematika Indonesia” dan Nusantara 21). Demikian pula di berbagai penjuru dunia aplikasi ecommerce terlihat mulai meningkat.
- ▶ Desentralisasi (dan *distributed*) server menyebabkan lebih banyak sistem yang harus ditangani. Hal ini membutuhkan lebih banyak operator dan administrator yang handal yang juga kemungkinan harus disebar di seluruh lokasi. Padahal mencari operator dan administrator yang handal adalah sangat sulit, apalagi jika harus disebar di berbagai

tempat. Akibat dari hal ini adalah biasanya server-server di daerah (bukan pusat) tidak dikelola dengan baik sehingga lebih rentan terhadap serangan. Seorang cracker akan menyerang server di daerah lebih dahulu sebelum mencoba menyerang server pusat. Setelah itu dia akan menyusup melalui jalur belakang. (Biasanya dari daerah / cabang ke pusat ada routing dan tidak dibatasi dengan firewall.)

- ▶ Transisi dari *single vendor* ke *multi-vendor* sehingga lebih banyak sistem atau perangkat yang harus dimengerti dan masalah *interoperability* antar vendor yang lebih sulit ditangani. Untuk memahami satu jenis perangkat dari satu vendor saja sudah susah, apalagi harus menangani berjenis-jenis perangkat. Bayangkan, untuk router saja sudah ada berbagai vendor; Cisco, Juniper Networks, Nortel, Linux-based router, BSD-based router, dan lain-lain. Belum lagi jenis sistem operasi (operating system) dari server, seperti Solaris (dengan berbagai versinya), Windows (NT, 2000, 2003), Linux (dengan berbagai distribusi), BSD (dengan berbagai variasinya mulai dari FreeBSD, OpenBSD, NetBSD). Jadi sebaiknya tidak menggunakan variasi yang terlalu banyak.
- ▶ Meningkatnya kemampuan pemakai di bidang komputer sehingga mulai banyak pemakai yang mencoba-coba bermain atau membongkar sistem yang digunakannya (atau sistem milik orang lain). Jika dahulu akses ke komputer sangat sukar, maka sekarang komputer sudah merupakan barang yang mudah diperoleh dan banyak dipasang di sekolah serta rumah-rumah.
- ▶ Mudahnya diperoleh software untuk menyerang komputer dan jaringan komputer. Banyak tempat di Internet yang menyediakan software yang langsung dapat diambil (*download*) dan langsung digunakan untuk menyerang dengan *Graphical User Interface* (GUI) yang mudah digunakan. Beberapa program, seperti SATAN, bahkan hanya membutuhkan sebuah web browser untuk menjalankannya. Sehingga, seseorang yang hanya dapat menggunakan web browser dapat menjalankan program penyerang (*attack*). Penyerang yang hanya bisa menjalankan program tanpa mengerti apa maksudnya disebut dengan istilah *script kiddie*.
- ▶ Kesulitan dari penegak hukum untuk mengejar kemajuan dunia komputer dan telekomunikasi yang sangat cepat. Hukum yang berbasis ruang dan waktu akan mengalami kesulitan untuk mengatasi masalah yang justru terjadi pada sebuah sistem yang tidak memiliki ruang dan waktu. Barang bukti digital juga masih sulit diakui oleh pengadilan Indonesia sehingga menyulitkan dalam pengadilan. Akibatnya pelaku kejahatan cyber hanya dihukum secara ringan sehingga ada kecenderungan mereka melakukan hal itu kembali.
- ▶ Semakin kompleksnya sistem yang digunakan, seperti semakin besarnya program (*source code*) yang digunakan sehingga semakin besar probabilitas terjadinya lubang keamanan (yang disebabkan kesalahan pemrograman, bugs).

### ***Klasifikasi Kejahatan Komputer***

Kejahatan komputer dapat digolongkan kepada yang sangat berbahaya sampai ke yang hanya mengesalkan (*annoying*). Menurut David Icove berdasarkan lubang keamanan, keamanan dapat diklasifikasikan menjadi empat, yaitu :

1. *Keamanan yang bersifat fisik (physical security)*

Termasuk akses orang ke gedung, peralatan, dan media yang digunakan. Beberapa bekas penjahat komputer (*crackers*) mengatakan bahwa mereka sering pergi ke tempat sampah untuk mencari berkas-berkas yang mungkin memiliki informasi tentang keamanan. Misalnya pernah ditemukan coretan password atau manual yang dibuang tanpa dihancurkan.

Wiretapping atau hal-hal yang berhubungan dengan akses ke kabel atau komputer yang digunakan juga dapat dimasukkan ke dalam kelas ini. Pencurian komputer dan notebook juga merupakan kejahatan yang bersifat fisik. Menurut statistik, 15% perusahaan di Amerika pernah kehilangan notebook. Padahal biasanya notebook ini tidak dibackup (sehingga data-datanya hilang), dan juga seringkali digunakan untuk menyimpan data-data yang seharusnya sifatnya confidential (misalnya pertukaran email antar direktur yang menggunakan notebook tersebut).

*Denial of service*, yaitu akibat yang ditimbulkan sehingga servis tidak dapat diterima oleh pemakai juga dapat dimasukkan ke dalam kelas ini. *Denial of service* dapat dilakukan misalnya dengan mematikan peralatan atau membanjiri saluran komunikasi dengan pesan-pesan (yang dapat berisi apa saja karena yang diutamakan adalah banyaknya jumlah pesan). Beberapa waktu yang lalu ada lubang keamanan dari implementasi protokol TCP/IP yang dikenal dengan istilah *Syn Flood Attack*, dimana sistem (*host*) yang dituju dibanjiri oleh permintaan sehingga dia menjadi terlalu sibuk dan bahkan dapat berakibat macetnya sistem (*hang*).

Mematikan jalur listrik sehingga sistem menjadi tidak berfungsi juga merupakan serangan fisik. Masalah keamanan fisik ini mulai menarik perhatian ketika gedung World Trade Center yang dianggap sangat aman dihantam oleh pesawat terbang yang dibajak oleh teroris. Akibatnya banyak sistem yang tidak bisa hidup kembali karena tidak diamankan. Belum lagi hilangnya nyawa.

## 2. *Keamanan yang berhubungan dengan orang (personel)*

Termasuk identifikasi, dan profil resiko dari orang yang mempunyai akses (pekerja). Seringkali kelemahan keamanan sistem informasi bergantung kepada manusia (pemakai dan pengelola). Ada sebuah teknik yang dikenal dengan istilah “*social engineering*” yang sering digunakan oleh kriminal untuk berpura-pura sebagai orang yang berhak mengakses informasi. Misalnya kriminal ini berpura-pura sebagai pemakai yang lupa passwordnya dan minta agar diganti menjadi kata lain.

## 3. *Keamanan dari data dan media serta teknik komunikasi (communications)*

Yang termasuk di dalam kelas ini adalah kelemahan dalam software yang digunakan untuk mengelola data. Seorang kriminal dapat memasang *virus* atau *trojan horse* sehingga dapat mengumpulkan informasi (seperti password) yang semestinya tidak berhak diakses. Bagian ini yang akan banyak kita bahas dalam buku ini.

## 4. *Keamanan dalam operasi*

Termasuk kebijakan (*policy*) dan prosedur yang digunakan untuk mengatur dan mengelola sistem keamanan, dan juga termasuk prosedur setelah serangan (*post attack recovery*). Seringkali perusahaan tidak memiliki dokumen kebijakan dan prosedur.

## **Aspek / Service Dari Keamanan (Security)**

Garfinkel mengemukakan bahwa keamanan komputer (*computer security*) melingkupi empat aspek, yaitu *privacy*, *integrity*, *authentication*, dan *availability*.

### 1. *Privacy / Confidentiality*

Inti utama aspek *privacy* atau *confidentiality* adalah usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. *Privacy* lebih kearah data-data yang sifatnya privat sedangkan *confidentiality* biasanya berhubungan dengan data yang diberikan ke pihak lain untuk keperluan tertentu (misalnya sebagai bagian dari pendaftaran sebuah servis) dan hanya diperbolehkan untuk keperluan tersebut. Contoh hal yang berhubungan dengan *privacy* adalah e-mail seorang pemakai (*user*) tidak boleh dibaca oleh administrator.

Contoh *confidential information* adalah data-data yang sifatnya pribadi (seperti nama, tempat tanggal lahir, social security number, agama, status perkawinan, penyakit yang pernah diderita, nomor kartu kredit, dan sebagainya) merupakan data-data yang ingin diproteksi penggunaan dan penyebarannya. Contoh lain dari *confidentiality* adalah daftar pelanggan dari sebuah *Internet Service Provider* (ISP). Untuk mendapatkan kartu kredit, biasanya ditanyakan data-data pribadi. Jika saya mengetahui data-data pribadi anda, termasuk nama ibu anda, maka saya dapat melaporkan melalui telepon (dengan berpura-pura sebagai anda) bahwa kartu kredit anda hilang dan mohon penggunaannya diblokir. Institusi (bank) yang mengeluarkan kartu kredit anda akan percaya bahwa saya adalah anda dan akan menutup kartu kredit anda.

Masih banyak lagi kekacauan yang dapat ditimbulkan bila data-data pribadi ini digunakan oleh orang yang tidak berhak. Ada sebuah kasus dimana karyawan sebuah perusahaan dipecat dengan tidak hormat dari perusahaan yang bersangkutan karena kedapatan mengambil data-data gaji karyawan di perusahaan yang bersangkutan. Di perusahaan ini, daftar gaji termasuk informasi yang bersifat *confidential* /rahasia.

### 2. *Integrity*

Aspek ini menekankan bahwa informasi tidak boleh diubah tanpa seijin pemilik informasi. Adanya virus, *trojan horse*, atau pemakai lain yang mengubah informasi tanpa ijin merupakan contoh masalah yang harus dihadapi. Sebuah e-mail dapat saja “ditangkap” (*intercept*) di tengah jalan, diubah isinya (*altered, tampered, modified*), kemudian diteruskan ke alamat yang dituju. Dengan kata lain, integritas dari informasi sudah tidak terjaga. Penggunaan *enkripsi* dan *digital signature*, misalnya, dapat mengatasi masalah ini.

Salah satu contoh kasus *trojan horse* adalah distribusi paket program *TCP Wrapper* (yaitu program populer yang dapat digunakan untuk mengatur dan membatasi akses TCP/IP) yang dimodifikasi oleh orang yang tidak bertanggung jawab. Jika anda memasang program yang berisi *trojan horse* tersebut, maka ketika anda merakit (*compile*) program tersebut, dia akan mengirimkan eMail kepada orang tertentu yang kemudian memperbolehkan dia masuk ke sistem anda. Informasi ini berasal dari CERT Advisory, “CA-99-01 Trojan-TCP-Wrappers” yang didistribusikan 21 Januari 1999.

Contoh serangan lain adalah yang disebut “*man in the middle attack*” dimana seseorang menempatkan diri di tengah pembicaraan dan menyamar sebagai orang lain.

### 3. *Authentication*

Aspek ini berhubungan dengan metoda untuk menyatakan bahwa informasi betul-betul asli, orang yang mengakses atau memberikan informasi adalah betul-betul orang yang dimaksud, atau server yang kita hubungi adalah betul-betul server yang asli.

Masalah pertama, membuktikan keaslian dokumen, dapat dilakukan dengan teknologi *watermarking* dan digital signature. Watermarking juga dapat digunakan untuk menjaga "*intellectual property*", yaitu dengan menandai dokumen atau hasil karya dengan "tanda tangan" pembuat.

Masalah kedua biasanya berhubungan dengan access control, yaitu berkaitan dengan pembatasan orang yang dapat mengakses informasi. Dalam hal ini pengguna harus menunjukkan bukti bahwa memang dia adalah pengguna yang sah, misalnya dengan menggunakan password, biometric (ciri-ciri khas orang), dan sejenisnya. Ada tiga hal yang dapat ditanyakan kepada orang untuk menguji siapa dia :

- What you have (misalnya kartu ATM)
- What you know (misalnya PIN atau password)
- What you are (misalnya sidik jari, biometric)

Penggunaan teknologi *smart card*, saat ini kelihatannya dapat meningkatkan keamanan aspek ini. Secara umum, proteksi authentication dapat menggunakan *digital certificates*. Authentication biasanya diarahkan kepada orang (pengguna), namun tidak pernah ditujukan kepada server atau mesin. Pernahkan kita bertanya bahwa mesin ATM yang sedang kita gunakan memang benar-benar milik bank yang bersangkutan? Bagaimana jika ada orang nakal yang membuat mesin seperti ATM sebuah bank dan meletakkannya di tempat umum? Dia dapat menyadap data-data (informasi yang ada di magnetic strip) dan PIN dari orang yang tertipu. Memang membuat mesin ATM palsu tidak mudah. Tapi, bisa anda bayangkan betapa mudahnya membuat web site palsu yang menyamar sebagai web site sebuah bank yang memberikan layanan Internet Banking. (Ini yang terjadi dengan kasus klikBCA.com.)

### 4. *Availability*

Aspek availability atau ketersediaan berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang atau dijebol dapat menghambat atau meniadakan akses ke informasi. Contoh hambatan adalah serangan yang sering disebut dengan "*denial of service attack*" (DoS attack), dimana server dikirim permintaan (biasanya palsu) yang bertubi-tubi atau permintaan yang diluar perkiraan sehingga tidak dapat melayani permintaan lain atau bahkan sampai *down*, *hang*, *crash*. Contoh lain adalah adanya *mailbomb*, dimana seorang pemakai dikirim e-mail bertubi-tubi (katakan ribuan e-mail) dengan ukuran yang besar sehingga sang pemakai tidak dapat membuka e-mailnya atau kesulitan mengakses e-mailnya (apalagi jika akses dilakukan melalui saluran telepon).

## ***Pentingnya Akses Kontrol***

Bagi para profesional keamanan sistem/teknologi informasi, perhatian harus diberikan pada kebutuhan akses kontrol dan metode-metode implementasinya untuk menjamin bahwa sistem memenuhi *availability* (ketersediaan), *confidentiality* (kerahasiaan), dan *integrity* (integritas). Dalam komputer jaringan, juga diperlukan pemahaman terhadap penggunaan akses kontrol pada arsitektur terdistribusi dan terpusat.

Melakukan kontrol akses pada sistem informasi dan jaringan yang terkait juga merupakan hal penting untuk menjaga *confidentiality*, *integrity*, dan *availability*. *Confidentiality* atau kerahasiaan memastikan bahwa informasi tidak terbuka ke individu, program atau proses yang tidak berhak. Beberapa informasi mungkin lebih sensitif dibandingkan informasi lainnya dan memerlukan level kerahasiaan yang lebih tinggi. Mekanisme kontrol perlu ditempatkan untuk mendata siapa yang dapat mengakses data dan apa yang orang dapat lakukan terhadapnya saat pertama kali diakses. Aktivitas tersebut harus dikontrol, diaudit, dan dimonitor.

Beberapa tipe informasi yang dipertimbangkan sebagai informasi rahasia adalah misalnya catatan kesehatan, informasi laporan keuangan, catatan kriminal, kode sumber program, perdagangan rahasia, dan rencana taktis militer. Sedangkan beberapa mekanisme yang memebrikan kemampuan kerahasiaan sebagai contoh yaitu enkripsi, kontrol akses fisik dan logikal, protokol transmisi, tampilan database, dan alur trafik yang terkontrol.

Bagi suatu institusi (skala besar, menengah maupun kecil), adalah merupakan hal penting untuk mengidentifikasi data dan kebutuhan-kebutuhan yang terklasifikasi sehingga dapat dipastikan bahwa suatu peringkat prioritas akan melindungi data dan informasi serta terjaga kerahasiaannya. Jika informasi tidak terklasifikasi maka akan diperlukan banyak waktu dan biaya yang dikeluarkan saat mengimplementasikan besaran yang sama pada tingkat keamanan untuk informasi kritis maupun informasi tidak penting.

Integritas memiliki tujuan mencegah modifikasi pada informasi oleh *user* yang tidak berhak, mencegah modifikasi yang tidak sengaja atau tidak berhak pada informasi oleh orang yang tidak berkepentingan, dan menjaga konsistensi internal maupun eksternal.

Konsistensi internal memastikan bahwa data internal selalu konsisten. Misalnya, diasumsikan sebuah database internal memiliki jumlah unit suatu komponen tertentu pada tiap bagian suatu organisasi. Jumlah bilangan dari komponen di tiap bagian tersebut harus sama dengan jumlah bilangan komponen pada database yang terekam secara internal pada keseluruhan organisasi.

Konsistensi eksternal menjamin bahwa data yang tersimpan pada database konsisten dengan fisiknya. Sebagai contoh dari konsistensi internal di atas, konsistensi eksternal berarti bahwa besarnya komponen yang tercatat pada database untuk setiap bagian adalah sama dengan banyaknya komponen secara fisik di tiap bagian tersebut.

Informasi juga harus akurat, lengkap, dan terlindungi dari modifikasi yang tidak berhak. Ketika suatu mekanisme keamanan memberikan integritas, ia akan melindungi data dari perubahan yang tidak lazim, dan jika memang terjadi juga modifikasi ilegal pada data tersebut maka mekanisme keamanan harus memperingatkan user atau membatalkan modifikasi tersebut.

*Availability* (ketersediaan) memastikan bahwa untuk user yang berhak memakai sistem, memiliki waktu dan akses yang bebas gangguan pada informasi dalam sistem. Informasi,

sistem, dan sumberdaya harus tersedia untuk user pada waktu diperlukan sehingga produktifitas tidak terpengaruh. Kebanyakan informasi perlu untuk dapat diakses dan tersedia bagi user saat diminta sehingga mereka dapat menyelesaikan tugas-tugas dan memenuhi tanggung jawab pekerjaan mereka.

Melakukan akses pada informasi kelihatannya tidak begitu penting hingga pada suatu saat informasi tersebut tidak dapat diakses. Administrator sistem mengalaminya saat sebuah file server mati atau sebuah database yang pemakaiannya tinggi tiba-tiba rusak untuk suatu alasan dan hal lainnya. *Fault tolerance* dan mekanisme pemulihan digunakan untuk menjamin kontinuitas ketersediaan sumberdaya. Produktifitas user dapat terpengaruh jika data tidak siap tersedia.

Informasi memiliki atribut-atribut yang berbeda seperti akurasi, relevansi, sesuai waktu, *privacy*, dan keamanan. Mekanisme keamanan yang berbeda dapat memberikan tingkat kerahasiaan, integritas, dan ketersediaan yang berbeda pula. Lingkungan, klasifikasi data yang dilindungi, dan sasaran keamanan perlu dievaluasi untuk menjamin mekanisme keamanan yang sesuai dibeli dan digunakan sebagaimana mestinya.

Tujuan kontrol akses lainnya adalah *reliability* dan utilitas. Tujuan-tujuan tersebut mengalir dari kebijakan keamanan suatu organisasi. Kebijakan ini merupakan pernyataan tingkat tinggi dari pihak manajemen berkaitan dengan kontrol pada akses suatu informasi dan orang yang berhak menerima informasi tersebut.

Tiga hal lainnya yang patut dipertimbangkan untuk perencanaan dan implementasi mekanisme kontrol akses adalah ancaman pada sistem (*threats*), kerawanan sistem pada ancaman (*vulnerabilities*), dan resiko yang ditimbulkan oleh ancaman tersebut. Ancaman (*threats*) adalah suatu kejadian atau aktivitas yang memiliki potensi untuk menyebabkan kerusakan pada sistem informasi atau jaringan. Kerawanan (*vulnerabilities*) adalah kelemahan atau kurangnya penjagaan yang dapat dimanfaatkan oleh suatu ancaman, menyebabkan kerusakan pada sistem informasi atau jaringan. Sedangkan resiko adalah potensi kerusakan atau kehilangan pada sistem informasi atau jaringan; kemungkinan bahwa ancaman akan terjadi.

### **Penjelasan Akses Kontrol**

Akses kontrol merupakan fitur-fitur keamanan yang mengontrol bagaimana user dan sistem berkomunikasi dan berinteraksi dengan sistem dan sumberdaya lainnya. Akses kontrol melindungi sistem dan sumberdaya dari akses yang tidak berhak dan umumnya menentukan tingkat otorisasi setelah prosedur otentikasi berhasil dilengkap.

Akses adalah aliran informasi antara subjek dan objek. Sebuah subjek merupakan entitas aktif yang meminta akses ke suatu objek atau data dalam objek tersebut. Sebuah subjek dapat berupa user, program, atau proses yang mengakses informasi untuk menyelesaikan suatu tugas tertentu. Ketika sebuah program mengakses sebuah file, program menjadi subjek dan file menjadi objek. Objek adalah entitas pasif yang mengandung informasi. Objek bisa sebuah komputer, database, file, program komputer, direktori, atau field pada tabel yang berada di dalam database.

Kontrol akses adalah sebuah term luas yang mencakup beberapa tipe mekanisme berbeda yang menjalankan fitur kontrol akses pada sistem komputer, jaringan, dan informasi. Kontrol akses sangatlah penting karena menjadi satu dari garis pertahanan pertama yang

digunakan untuk menghadang akses yang tidak berhak ke dalam sistem dan sumberdaya jaringan.

Saat user diminta memasukan *username* dan *password* hal ini disebut dengan kontrol akses. Setelah user *log in* dan kemudian mencoba mengakses sebuah file, file ini dapat memiliki daftar user dan grup yang memiliki hak akses ke file tersebut. Jika user tidak termasuk dalam daftar maka akses akan ditolak. Hal itu sebagai bentuk lain dari kontrol akses. Hak dan ijin user adalah berdasarkan identitas, kejelasan, dan atau keanggotaan suatu grup. Kontrol akses memberikan organisasi kemampuan melakukan kontrol, pembatasan, monitor, dan melindungi ketersediaan, integritas, dan kerahasiaan sumberdaya.

Kontrol diimplementasikan untuk menanggulangi resiko dan mengurangi potensi kehilangan. Kontrol dapat bersifat preventif, detektif, atau korektif. Kontrol preventif dipakai untuk mencegah kejadian-kejadian yang merusak. Kontrol detektif diterapkan untuk menemukan kejadian-kejadian yang merusak. Kontrol korektif digunakan untuk memulihkan sistem yang menjadi korban dari serangan berbahaya.

Untuk menerapkan ukuran-ukuran tersebut, kontrol diimplementasikan secara administratif, logikal atau teknikal, dan fisik. Kontrol administratif termasuk kebijakan dan prosedur, pelatihan perhatian terhadap keamanan, pemeriksaan latar belakang, pemeriksaan kebiasaan kerja, tinjauan riwayat hari libur, dan supervisi yang ditingkatkan.

Kontrol logikal atau teknikal mencakup pembatasan akses ke sistem dan perlindungan informasi. Contoh kontrol pada tipe ini adalah enkripsi, *smart cards*, daftar kontrol akses, dan protokol transmisi. Sedangkan kontrol fisik termasuk penjagaan dan keamanan bangunan secara umum seperti penguncian pintu, pengamanan ruang server atau laptop, proteksi kabel, pemisahan tugas kerja, dan backup data.

Kontrol fisik merupakan penempatan penjaga dan bangunan secara umum, seperti penguncian pintu, pengamanan ruang server atau laptop, perlindungan pada kabel, pembagian tanggung jawab, dan backup file.

### **Model Kontrol Akses**

Penerapan akses kontrol pada subjek sistem (sebuah entitas aktif seperti individu atau proses) terhadap objek sistem (sebuah entitas pasif seperti sebuah file) berdasarkan aturan (*rules*). Model kontrol akses merupakan sebuah framework yang menjelaskan bagaimana subjek mengakses objek. Model ini menggunakan teknologi kontrol akses dan mekanisme sekuriti untuk menerapkan aturan dan tujuan suatu model.

Ada tiga tipe utama model kontrol akses yaitu mandatory, discretionary, dan nondiscretionary (sering disebut juga role-based). Tiap tipe model memakai metode berbeda untuk mengontrol bagaimana subjek mengakses objek dan mempunyai kelebihan serta keterbatasan masing-masing.

Tujuan bisnis dan keamanan dari suatu organisasi akan membantu menjelaskan model kontrol akses mana yang sebaiknya digunakan, bersamaan dengan budaya perusahaan dan kebiasaan menjalankan bisnisnya. Beberapa model dipakai secara eksklusif dan kadang-kadang model tersebut dikombinasikan sehingga mampu mencapai tingkat keperluan keamanan lingkungan yang dibutuhkan. Aturan pada akses kontrol diklasifikasikan menjadi :

▶ *Mandatory access control*

Otorisasi suatu akses subjek terhadap objek bergantung pada label, dimana label ini menunjukkan ijin otorisasi suatu subjek dan klasifikasi atau sensitivitas dari objek. Misalnya, pihak militer mengklasifikasikan dokumen sebagai unclassified, confidential, secret, dan top secret.

Untuk hal yang sama, individu dapat menerima ijin otorisasi tentang confidential, secret, atau top secret dan dapat memiliki akses ke dokumen bertipe classified atau tingkatan di bawah status ijin otorisasinya. Sehingga individu dengan ijin otorisasi secret dapat mengakses tingkatan secret dan confidential dokumen dengan suatu batasan.

Batasan ini adalah bahwa individu memiliki keperluan untuk mengetahui secara relatif classified dokumen yang dimaksud. Meskipun demikian dokumen yang dimaksud harus benar-benar diperlukan oleh individu tersebut untuk menyelesaikan tugas yang diembannya. Bahkan jika individu memiliki ijin otorisasi untuk tingkat klasifikasi suatu informasi, tetapi tidak memiliki keperluan untuk mengetahui maka individu tersebut tetap tidak boleh mengakses informasi yang diinginkannya.

Pada model mandatory access control, user dan pemilik data tidak memiliki banyak kebebasan untuk menentukan siapa yang dapat mengakses file-file mereka. Pemilik data dapat mengizinkan pihak lain untuk mengakses file mereka namun operating system (OS) yang tetap membuat keputusan final dan dapat membatalkan kebijakan dari pemilik data.

Model ini lebih terstruktur dan ketat serta berdasarkan label keamanan sistem. User diberikan ijin otorisasi dan data diklasifikasikan. Klasifikasi disimpan di label sekuriti pada sumber daya. Klasifikasi label menentukan tingkat kepercayaan user yang harus dimiliki untuk dapat mengakses suatu file.

Ketika sistem membuat keputusan mengenai pemenuhan permintaan akses ke suatu objek, keputusan akan didasarkan pada ijin otorisasi subjek dan klasifikasi objek. Aturan-aturan bagaimana subjek mengakses data dibuat oleh manajemen, dikonfigurasi oleh administrator, dijalankan oleh operating system, dan didukung oleh teknologi sekuriti.

▶ *Discretionary access control*

Subjek memiliki otoritas, dengan batasan tertentu, untuk menentukan objek-objek apa yang dapat diakses. Contohnya adalah penggunaan daftar kontrol akses (access control list). Daftar kontrol akses merupakan sebuah daftar yang menunjuk user-user mana yang memiliki hak ke sumber daya tertentu. Misalnya daftar tabular akan menunjukkan subjek atau user mana yang memiliki akses ke objek (file x) dan hak apa yang mereka punya berkaitan dengan file x tersebut.

Kontrol akses triple terdiri dari user, program, dan file dengan hubungan hak akses terkait dengan tiap user. Tipe kontrol akses ini digunakan secara lokal, dan mempunyai situasi dinamis dimana subjek-subjek harus memiliki pemisahan untuk menentukan sumber daya tertentu yang user diijinkan untuk mengakses.

Ketika user dengan batasan tertentu memiliki hak untuk merubah kontrol akses ke objek-objek tertentu, hal ini disebut sebagai user-directed discretionary access control. Sedangkan kontrol akses berbasis identitas (identity-based access control) adalah tipe kontrol akses terpisah berdasarkan identitas suatu individu.

Dalam beberapa kasus, pendekatan hybrid juga digunakan, yaitu yang mengkombinasikan fitur-fitur user-based dan identity-based discretionary access control. Jika user membuat suatu file, maka ia merupakan pemilik file tersebut. Kepemilikan juga bisa diberikan kepada individu spesifik. Misalnya, seorang manager pada departemen tertentu dapat membuat kepemilikan suatu file dan sumber daya dalam domain-nya. Pengenal untuk user ini ditempatkan pada file header. Sistem yang menerapkan model discretionary access control memungkinkan pemilik sumber daya untuk menentukan subjek-subjek apa yang dapat mengakses sumber daya spesifik.

Model ini dinamakan discretionary karena kontrol akses didasarkan pada pemisahan pemilik. Pada model ini, akses dibatasi berdasarkan otorisasi yang diberikan pada user. Ini berarti bahwa subjek-subjek diijinkan untuk menentukan tipe akses apa yang dapat terjadi pada objek yang mereka miliki. Jika organisasi menggunakan model discretionary access control, administrator jaringan dapat mengizinkan pemilik sumber daya mengontrol siapa yang dapat mengakses file/sumber daya tersebut.

Implementasi umum dari discretionary access control adalah melalui access control list yang dibuat oleh pemilik, diatur oleh administrator jaringan, dan dijalankan oleh operating system. Dengan demikian kontrol ini tidak termasuk dalam lingkungan terkontrol terpusat dan dapat membuat kemampuan user mengakses informasi secara dinamis, kebalikan dari aturan yang lebih statis pada mandatory access control.

► *Non-Discretionary access control*

Otoritas sentral menentukan subjek-subjek apa yang mempunyai akses ke objek-objek tertentu berdasarkan kebijakan keamanan organisasi. Kontrol akses bisa berdasarkan peran individu dalam suatu organisasi (role-based) atau tanggung jawab subjek dan tugasnya (task-based).

Dalam organisasi dimana sering terdapat adanya perubahan/pergantian personel, nondiscretionary access control merupakan model yang tepat karena kontrol akses didasarkan pada peran individu atau jabatan dalam suatu organisasi. Kontrol akses ini tidak perlu dirubah saat individu baru masuk menggantikan individu lama. Tipe lain dari non-discretionary access control adalah kontrol akses lattice-based. Dalam model lattice (lapis tingkatan), terdapat pasangan-pasangan elemen yang memiliki batas tertinggi terkecil dari nilai dan batas terendah terbesar dari nilai. Untuk menerapkan konsep kontrol akses ini, pasangan elemen adalah subjek dan objek, dan subjek memiliki batas terendah terbesar serta batas tertinggi terkecil untuk hak akses pada suatu objek.

Selain itu terdapat model role-based access control yang juga sebagai nondiscretionary access control. Model ini menerapkan seperangkat aturan terpusat pada kontrol untuk menentukan bagaimana subjek dan objek berinteraksi. Tipe model ini mengizinkan akses ke sumber daya berdasarkan peran yang user tangani dalam suatu organisasi. Administrator menempatkan user dalam peran dan kemudian memberikan hak akses pada peran tersebut.

Peran dan kelompok merupakan hal berbeda meskipun mereka mempunyai tujuan yang sama. Mereka bekerja sebagai penampung untuk para user. Perusahaan mungkin memiliki kelompok auditor yang terdiri dari beberapa user yang berbeda. Para user ini dapat menjadi bagian suatu kelompok lain dan biasanya memiliki hak

individunya masing-masing serta ijin yang diberikan kepada mereka. Jika perusahaan menerapkan peran, tiap user yang ditugaskan pada peran tertentu yang hanya memiliki hak pada peran tersebut. Hal ini menjadikan kontrol yang lebih ketat.

### ***Beberapa kombinasi sifat akses kontrol dengan implementasi***

▶ *Preventive/Administrative*

Kombinasi ini menekankan pada mekanisme lunak yang mendukung tujuan-tujuan kontrol akses. Mekanisme ini mencakup kebijakan-kebijakan dan prosedur-prosedur organisasi, pemeriksaan latar belakang calon karyawan, praktek penerimaan secara terbatas, perjanjian kerja, prosedur pemberhentian karyawan, jadwal liburan, pemberian label pada material sensitif, meningkatkan pengawasan, pelatihan kepedulian mengenai keamanan, kepedulian terhadap perilaku, dan prosedur-prosedur yang disepakati untuk memperoleh akses pada sistem informasi beserta jaringan.

▶ *Preventive/Technical*

Kombinasi ini menggunakan teknologi untuk menerapkan kebijakan kontrol akses. Kontrol teknikal juga dikenal sebagai kontrol logikal dan dapat dibangun ke dalam operating system, bisa berupa aplikasi perangkat lunak, atau dapat berupa suplemen unit perangkat lunak/keras. Beberapa tipe kombinasi preventif/teknikal yaitu protokol, enkripsi, kartu pintar, biometrik (untuk otentikasi), paket perangkat lunak kontrol akses lokal maupun jarak jauh (remote), sistem panggil kembali (call-back), password, interface user terbatas, menu, shell, tampilan database, keypads terbatas, dan perangkat lunak anti virus.

▶ *Preventive/Physical*

Ukuran kombinasi ini bersifat intuitif. Ukuran-ukuran pada model ini dimaksudkan untuk membatasi akses fisik ke area dengan sistem yang memiliki informasi sensitif. Batas pengamanan sirkular (circular security perimeter) di bawah kontrol akses mendefinisikan area atau zona yang harus dilindungi.

Kontrol preventif/fisikal mencakup pagar pengamanan, lencana, pintu berlapis, sistem masuk dengan kartu magnetik, biometrik, penjaga, anjing penjaga, sistem kontrol lingkungan (suhu, kelembaban), dan layout area akses dan bangunan. Model ini diterapkan pada area yang berfungsi sebagai tempat penyimpanan data backup.

▶ *Detective/Administrative*

Beberapa kontrol detektif/administratif tumpang tindih dengan kontrol preventif/administratif karena dapat diterapkan untuk pencegahan pelanggaran kebijakan keamanan di masa mendatang atau untuk mendeteksi pelanggaran yang terjadi saat ini. Contoh dari kontrol ini yaitu kebijakan dan prosedur organisasi, pemeriksaan latar belakang, jadwal liburan, pemberian label pada material sensitif, peningkatan supervisi, pelatihan kepedulian keamanan, dan kepedulian perilaku. Tambahan kontrol detektif/administratif yaitu rotasi pekerjaan, pembagian tanggung jawab, dan tinjauan ulang catatan-catatan hasil audit.

▶ *Detective/Technical*

Ukuran kontrol detektif/teknikal dimaksudkan untuk menangani pelanggaran pada kebijakan keamanan melalui metode teknikal. Cara ini termasuk penggunaan sistem deteksi penyusup (intrusion detection system) dan secara otomatis menghasilkan laporan pelanggaran dari informasi jejak audit. Laporan-laporan tersebut dapat menunjukkan variasi dari normal operasi atau mendeteksi tanda-tanda yang diketahui dari episode akses yang tidak berhak.

▶ *Detective/Physical*

Kontrol detektif/fisikal biasanya memerlukan orang untuk melakukan evaluasi terhadap masukan atau input dari sensor atau kamera pengawas untuk menentukan apakah suatu ancaman benar-benar terjadi. Beberapa tipe dari kontrol ini yaitu deteksi gerak, detektor panas, dan kamera video.

### ***Identifikasi Dan Otentikasi***

Bagi user, untuk dapat mengakses suatu sumber daya, harus ditentukan apakah individu tersebut adalah siapa yang dia klaim, apakah punya bukti yang diperlukan, dan apakah dia diberikan hak atau privilege yang diperlukan untuk melaksanakan tugas-tugas yang diminta. Jika langkah-langkah tersebut berhasil dilengkapi, user dapat mengakses dan menggunakan sumber daya jaringan atau sistem, dan bagaimanapun juga perlu juga untuk menelusuri aktivitas user dan menerapkan akuntabilitas pada tindakannya.

Identifikasi menggambarkan metode yang menjamin bahwa subjek (user, program, atau proses) adalah benar-benar entitas yang dia klaim. Identifikasi dapat diverifikasi melalui penggunaan bukti seperti username, personal identification number (PIN), smart card, tanda tangan digital, nomor account, atau atribut anatomi.

Untuk menjamin otentikasi secara tepat, subjek biasanya diminta untuk menyediakan bagian kedua dari seperangkat bukti, misalnya password, passphrase, kunci kriptografi, atau token. Dua bukti ini akan dibandingkan pada informasi tentang subjek yang sebelumnya disimpan terlebih dahulu. Jika bukti tersebut cocok dengan informasi yang disimpan maka subjek terotentikasi.

Setelah subjek memberikan bukti dan secara tepat teridentifikasi, sistem yang diakses perlu untuk memastikan apakah subjek telah diberikan hak dan privilege yang sesuai untuk menjalankan tugas-tugas yang diperlukan. Sistem akan melihat beberapa tipe matrix kontrol akses atau membandingkan label keamanan untuk memverifikasikan bahwa subjek ini benar-benar dapat mengakses sumber daya yang diminta dan melakukan pekerjaan yang dia emban. Jika subjek dapat mengakses sumber daya maka subjek baru saja telah diotorisasi.

Meskipun identifikasi, otentikasi, dan otorisasi memiliki definisi yang mirip dan komplementer, masing-masing tetap mempunyai fungsi yang berbeda untuk memenuhi kebutuhan spesifik dalam proses kontrol akses. Seorang user mungkin secara benar telah diidentifikasi dan terotentikasi ke jaringan, tetapi ia mungkin tidak memiliki otorisasi untuk mengakses file pada file server. Pada sisi lain, user mungkin diberi otorisasi untuk mengakses file pada file server, namun hingga ia secara tepat teridentifikasi dan terotentikasi, sumber daya yang dimaksud tetap belum bisa diakses.

Subjek perlu dijaga akuntabilitasnya untuk setiap aktivitas atau tindakan yang dilakukan dalam sistem atau domain-nya. Cara untuk menjamin akuntabilitasnya adalah jika subjek secara unik teridentifikasi dan aktivitas-aktivitas subjek tercatat/terekam. Kontrol akses logikal adalah alat yang digunakan untuk identifikasi, otentikasi, otorisasi, dan akuntabilitas. Kontrol akses logikal merupakan komponen-komponen perangkat lunak yang menjamin aturan-aturan kontrol akses untuk sistem, program, proses, dan informasi. Kontrol akses logikal dapat dimasukkan dalam operating system, aplikasi, paket sekuriti tambahan, atau dalam database dan sistem manajemen telekomunikasi.

Identitas individu harus diverifikasi selama proses otentikasi. Otentikasi biasanya terdiri dari dua langkah proses yaitu memasukan informasi umum (username, nomor karyawan, nomor account, ID departemen, atau fitur biometrik) dan kemudian memasukan informasi pribadi (password statis, smart token, pasword kognitif, one-time password, PIN, tanda tangan digital, smart card, atau memory card).

Memasukan informasi publik adalah langkah identifikasi dan memasukan informasi pribadi adalah langkah otentikasi dari dua langkah proses. Tiap teknik yang digunakan untuk identifikasi dan otentikasi memiliki aspek pro dan kontra masing-masing. Sehingga tiap langkah harus secara tepat dievaluasi untuk menentukan mekanisme yang benar untuk lingkungan yang benar pula.

► *Biometrik*

Biometrik memverifikasi identitas individu melalui atribut personal yang unik, dimana satu dari metode-metode paling efektif dan akurat dalam verifikasi identifikasi. Biometrik adalah teknologi yang sangat canggih sehingga paling mahal dibandingkan tipe lain dari proses-proses verifikasi identifikasi.

Sistem melakukan scan pada atribut seseorang dan membandingkan dengan catatan yang telah lebih dahulu dibuat pada proses pendaftaran. Karena sistem ini menginspeksi alur sidik jari seseorang, pola retina mata, atau gelombang suara orang, sistem ini sangatlah sensitif. Sistem harus melakukan ukuran yang sangat akurat dan berulang pada karakteristik anatomi atau fisiologi. Tipe sensitifitas dapat dengan mudah menyebabkan kesalahan positif atau kesalahan negatif. Sistem harus dikalibrasi sehingga kesalahan positif dan kesalahan negatif memiliki kejadian yang rendah, dan hasilnya menjadi seakurat mungkin.

Ketika sistem biometrik menolak individu yang terotorisasi, hal ini disebut type I error. Ketika sistem menerima orang yang seharusnya ditolak, kondisi ini disebut type II error. Tujuannya adalah mencapai jumlah rendah dari tiap kesalahan tersebut.

Saat membandingkan sistem biometrik yang berbeda, banyak variabel berbeda yang dipakai namun variabel yang paling penting adalah crossover error rate (CER). Rating ini ditunjukkan pada persentase dan mewakili pada titik dimana tingkat penolakan yang salah sebanding dengan tingkat penerimaan yang salah. Rating ini adalah ukuran yang paling penting ketika menentukan akurasi suatu sistem. Sistem biometrik yang menghasilkan CER 3 akan lebih akurat dibandingkan sistem yang memberikan CER 4.

Biometrik adalah metode yang paling mahal dalam verifikasi identitas orang dan mengalami hambatan untuk diterima secara luas. Halangan tersebut meliputi penerimaan user, kerangka watu penerimaan dan hasil. Banyak tipe sistem biometrik yang memeriksa karakteristik berbeda dari seseorang. Dalam tiap sistem tersebut,

individu harus melalui proses pendaftaran yang menangkap data biometrik dan menyimpannya pada file referensi. File referensi ini kemudian akan digunakan saat orang berusaha untuk diotentikasi.

Beberapa tipe dari sistem biometrik yang lain yaitu sidik jari, scan telapak tangan, geometri tangan, scan retina, scan iris, dinamik tanda tangan, dinamik keyboard, cetak suara, scan wajah, dan topologi tangan.

► *Otentikasi*

Setelah orang diidentifikasi, ia harus diotentikasi yang berarti bahwa ia harus membuktikan bahwa ia adalah seperti apa yang ia katakan. Tiga tipe umum otentikasi adalah sesuatu yang harus ia ketahui (*what you know*), sesuatu yang harus dimiliki (*what you have*), dan sesuatu yang menyatakan dia sebenarnya (*what you are*).

Melakukan otentikasi pada seseorang melalui sesuatu yang dia tahu biasanya paling mudah untuk diimplementasikan. Sisi buruk dari metode ini adalah orang lain mungkin dapat mengetahui hal tersebut dan memperoleh akses tidak resmi ke suatu sistem. Sesuatu yang orang miliki dapat berupa kunci, kartu gesek, kartu akses, atau lencana. Metode ini banyak digunakan untuk mengakses suatu fasilitas. Kelemahannya adalah bila barang-barang tersebut hilang atau dicuri sehingga dapat menyebabkan terjadinya akses ilegal bagi yang menemukannya. Sedangkan sesuatu yang menyatakan diri orang tersebut menjadi hal yang lebih menarik yaitu biometrik. Biometrik digunakan untuk identifikasi dalam kontrol fisik dan untuk tujuan otentikasi dalam kontrol teknikal.

Diluar dari sesuatu yang orang ketahui, miliki, atau dirinya, otentikasi kuat memiliki dua dari tiga metode tersebut. Menggunakan sistem biometrik tidak memberikan otentikasi kuat karena hanya menyediakan satu dari tiga metode tersebut. Biometrik memberikan solusi mengenai siapa orang tersebut dan bukan apa yang orang ketahui atau miliki.

► *Password*

Identifikasi user dengan password adalah bentuk yang paling umum dari mekanisme identifikasi dan otorisasi. Password adalah string karakter terlindungi yang digunakan untuk mengotentikasi individu. Seperti yang dinyatakan sebelumnya, faktor-faktor otentikasi didasarkan pada apa yang orang ketahui, miliki atau dirinya. Sebuah password adalah berdasarkan pada sesuatu yang user ketahui.

Meskipun password adalah mekanisme yang paling umum digunakan untuk otentikasi, ia juga dipertimbangkan sebagai mekanisme keamanan yang paling lemah yang ada. Karena user biasanya memilih password yang biasanya mudah ditebak, memberitahukan ke orang lain, dan banyak juga yang menulis password di selembar kertas lalu menaruh di dekat keyboard.

Bagi banyak user, keamanan biasanya bukan hal yang paling penting atau bagian menarik dalam pemanfaatan komputer mereka, kecuali ketika seseorang melakukan hacking pada komputer mereka dan mencuri informasi rahasia. Kemudian baru sekuriti menjadi hal yang populer.

▶ *Token*

Perangkat token atau pembangkit password biasanya merupakan alat genggam yang memiliki tampilan LCD dan keypad. Alat ini terpisah dari komputer yang user coba untuk akses. Alat token dan layanan otentikasi harus disinkronisasikan, atau menggunakan metode challenge-response, untuk dapat melakukan otentikasi pada user. Token menampilkan pada user dengan daftar karakter yang harus dimasukkan sebagai password saat logging ke komputer. Hanya token dan layanan otentikasi yang mengetahui maksud dari karakter tersebut. Karena tersinkronisasi, token akan memberikan password eksak yang diharapkan oleh layanan otentikasi tersebut.

▶ *Kunci Kriptografi*

Cara lain untuk membuktikan identitas seseorang adalah menampilkan kunci pribadi (private key) atau tanda tangan digital (digital signature). Kunci pribadi atau tanda tangan digital akan digunakan untuk menggantikan password. Password adalah bentuk terlemah dari otentikasi dan dapat dengan mudah disadap saat melintas di jaringan. Kunci pribadi dan tanda tangan digital merupakan bentuk otentikasi yang digunakan pada lingkungan yang memerlukan perlindungan lebih tinggi daripada yang bisa ditangani oleh password.

Kunci pribadi adalah nilai rahasia yang harus dimiliki oleh seseorang, dan hanya oleh satu orang. Tanda tangan digital menggunakan kunci pribadi untuk mengenkripsi suatu nilai acak. Tindakan mengenkripsi nilai acak ini dengan menggunakan kunci pribadi disebut penandaan digital (digital signing) suatu pesan. Sedangkan kunci umum dapat tersedia kepada siapa saja, ini yang menyebabkan disebut sebagai kunci publik (public key).

▶ *Otorisasi*

Perbedaan antara otentikasi dan otorisasi awalnya dapat membingungkan. Meskipun kedua konsep ini sangat berbeda, mereka perlu relasi sinergis untuk menyelesaikan tugas dalam mengizinkan user mengakses sumber daya. Otentikasi adalah proses membuktikan bahwa individu memegang identitas yang dia klaim. Sistem bisa tahu siapa anda, namun apakah sistem mengizinkan anda melakukan aksi yang anda minta? Hal ini dijawab dengan otorisasi.

Otorisasi adalah komponen inti dari semua operating system, tetapi aplikasi, paket tambahan sekuriti, dan sumber daya bisa menyediakan fungsionalitas ini. Pemberian hak akses pada subjek harus didasarkan pada tingkat kepercayaan yang organisasi miliki pada suatu subjek dan kebutuhan subjek untuk mengetahui. Kriteria akses yang berbeda dapat dibagi kedalam peran, kelompok, lokasi, waktu, dan tipe transaksi.

Peran bisa menjadi cara yang efisien untuk menempatkan hak pada tipe user yang melakukan tugas tertentu. Peran ini berdasarkan penugasan kerja atau fungsi kerja. Jika ada posisi dalam perusahaan untuk seseorang mengaudit transaksi atau catatan audit, peran tersebut hanya perlu fungsi baca pada tipe file tersebut. Peran ini tidak perlu hak kontrol penuh, merubah, atau menghapus.

▶ *Single Sign-On*

Seringkali karyawan perlu untuk mengakses banyak komputer berbeda dan sumber daya untuk menyelesaikan tugas-tugasnya. Hal ini menyebabkan karyawan harus

mengingat banyak user ID dan password untuk komputer yang berbeda. Secara utopia, user hanya perlu untuk memasukan satu user ID dan password untuk dapat mengakses semua sumber daya dalam semua jaringan diman user bekerja. Dalam dunia nyata, hal tersebut sulit diimplementasikan dan sulit untuk dikontrol.

Dikarenakan proliferasi dari teknologi client/server, jaringan bermigrasi dari jaringan terkontrol terpusat menjadi lingkungan terdistribusi yang heterogen. Propagasi dari sistem terbuka dan peningkatan keberagaman aplikasi, platform, dan operating system menyebabkan user untuk mengingat beberapa user ID dan password hanya untuk dapat mengakses dan menggunakan sumber daya berbeda dalam jaringannya.

Peningkatan biaya dalam pengelolaan lingkungan yang berbeda, perhatian pada sekuriti, dan kebiasaan user membawa ide tentang kemampuan single sign-on. Kemampuan ini akan mengijinkan user memasukan bukti-bukti satu kali dan dapat mengakses semua sumber daya dalam domain jaringan primer dan sekunder.

▶ *Kerberos*

Kerberos adalah protokol otentikasi dan didesain pada pertengahan 1980 sebagai bagian dari proyek Athena di MIT. Kerberos merupakan contoh dari sistem single sign-on untuk

lingkungan terdistribusi, dan standar de facto untuk jaringan heterogen. Kerberos menerapkan teknologi keamanan secara luas, dimana memberikan perusahaan lebih banyak fleksibilitas dan skalabilitas saat perlu untuk menyediakan arsitektur keamanan. Meskipun demikian, arsitektur terbuka ini juga mengundang masalah-masalah interoperabilitas.

Kerberos menggunakan kriptografi kunci simetris dan menyediakan keamanan end-to-end. Yang berarti bahwa informasi yang dilewati antara user dan layanan akan dilindungi tanpa perlu komponen perantara. Meskipun mengijinkan pemakaian password untuk otentikasi, Kerberos didesain secara khusus untuk menghilangkan kebutuhan pemindahan password melalui jaringan. Implementasi Kerberos kebanyakan bekerja dengan kunci kriptografi dan membagi kunci rahasia dibandingkan password.

▶ *Sesame*

Proyek secure european system for applications in a multivendor environment (SESAME) adalah tipe lain dari teknologi single sign-on yang dikembangkan untuk menjawab kelemahan di sistem Kerberos. SESAME memakai kriptografi kunci publik untuk mendistribusikan kunci-kunci rahasia, dimana mengurangi overhead manajemen kunci.

Seperti halnya kerberos, SESAME menggunakan tiket untuk otorisasi yang disebut dengan privilege attribute certificate. SESAME menambah beberapa fitur kontrol akses, memiliki skalabilitas sistem kunci publik dan lebih mudah dikelola. Namun SESAME juga rentan terhadap pendugaan/tebakan pasword seperti halnya Kerberos.

## **Cakupan Akses Kontrol**

### ▶ *Dictionary Attack*

Terdapat beberapa program yang memungkinkan penyerang (atau administrator proaktif) untuk mengidentifikasi atribut user. Program ini umumnya menggunakan kata-kata atau kombinasi dari karakter, dan program menerapkan nilai-nilai tersebut untuk usaha logon ke sistem.

Setelah kombinasi yang benar teridentifikasi, penyerang masuk ke sistem dan terotentikasi. Karena banyak sistem memiliki batasan yang menuliskan bagaimana banyak usaha login diterima, tipe aktivitas yang sama dapat terjadi pada file password yang terkena serangan. Program ini mengenkripsi kombinasi karakter dan membandingkannya dengan masukan terenkripsi dalam file password. Jika kecocokan ditemukan, maka program telah berhasil membuka password.

Countermeasure dari serangan ini adalah jangan membiarkan password dikirim melalui text secara jelas, enkripsi password dengan algoritme enkripsi atau fungsi-fungsi hash, terapkan token dengan password one-time, gunakan password yang sulit ditebak, rotasi password secara teratur, pakai IDS untuk mendeteksi tipe perilaku yang mencurigakan, gunakan serangan kamus untuk menemukan password lemah yang dibuat user, gunakan karakter khusus, dan lindungi file-file password.

### ▶ *Brute Force Attack*

Ada beberapa tipe serangan brute force, namun kesemuanya merupakan serangan yang secara kontinyu mencoba input-input berbeda untuk mencapai tujuan tertentu. Dalam pendugaan password, penyerang akan mencoba variasi karakter yang berbeda untuk mendapatkan kombinasi yang benar.

Serangan ini juga dipakai pada wardialing efforts. Daftar panjang nomor telepon dimasukan dalam program wardialing dengan harapan menemukan modem yang dapat dieksploitasi untuk mendapatkan akses ilegal. Program digunakan melalui banyak nomor telepon dan membuang nomor-nomor yang dipakai sebagai voice call dan layanan mesin fax. Penyerang biasanya mengakhiri dengan memegang nomor-nomor yang kemungkinan bisa dieksploitasi untuk mendapatkan akses ke sistem atau jaringan.

Countermeasure serangan ini yaitu jalankan serangan brute force untuk mengetahui kelemahan yang ada, pastikan hanya nomor-nomor telepon tertentu yang bersifat publik, menerapkan metode kontrol akses yang ketat, monitor & audit aktivitas anomali, pakai IDS untuk mengamati aktivitas mencurigakan, dan tentukan batasan-batasan penguncian.

### ▶ *Spoofing at Login*

Program yang menampilkan layar login palsu dapat dibuat oleh penyerang, dimana menipu user untuk masuk ke sistem. User diminta username dan password, yang akan disimpan oleh penyerang untuk diakses di lain waktu. User tidak tahu jika ini bukan layar login sebenarnya karena kelihatannya sama persis. Pesan kesalahan palsu muncul yang menunjukkan bahwa user salah memasukan kredensialnya.

Pada point ini, program login palsu keluar dan memberikan kendali ke operating system yang tentunya akan menampilkan permintaan username dan password. User

berasumsi bahwa ia melakukan kesalahan ketik dan tidak menyadari jika penyerang telah mengetahui atribut dirinya.

Countermeasure dari serangan ini adalah sistem dapat dikonfigurasi untuk menampilkan jumlah usaha login yang gagal yang bisa menunjukkan pada user tentang apa yang terjadi. Jika login pertama gagal dan sebenarnya merupakan program si penyerang maka usaha login kedua tidak akan dilaporkan sehingga user patut curiga tentang apa yang baru saja terjadi. Selain itu penjaminan trusted path dapat dipakai.

Trusted path memberi tahu user bahwa ia melakukan komunikasi langsung ke operating system. Windows NT menggunakan sekuens tombol CTRL-ALT-DEL untuk menampilkan layar login operating system (beberapa program tampilan palsu dapat dipanggil juga melalui fungsi tombol tersebut).

### ***Information Access & Security Policy***

#### 1. Introduction

Information is a vital asset to any organisation, and this is especially so in a knowledge-driven organisation such as the University, where information will relate to learning and teaching, research, administration and management. This policy is concerned with information held in the University and used by members of the University in their official capacities, for example as staff or students. It relates to both computer-based and paper-based information. The policy defines the responsibilities of individuals with respect to information use and to the provision and use of information processing systems.

#### 2. Information Access & Security principles

The University has adopted the following principles, which underpin this policy :

- ▶ Information will be protected in line with relevant laws and University policies, notably those relating to data protection and freedom of information.
- ▶ Information should be available to all who have a legitimate need for it.
- ▶ Information must be classified according to an appropriate level of availability: public, open (within the University), confidential, strictly confidential or secret.
- ▶ Integrity of information must be maintained; information must be accurate, complete, timely and consistent with other information.
- ▶ All who have access to information have a responsibility to handle it appropriately according to its classification.
- ▶ Nominated staff of the University are responsible for ensuring that appropriate procedures and systems for the processing and holding of information are in place and are effective.
- ▶ Information will be protected against unauthorised access, inappropriate for its classification.
- ▶ Data backup and recovery and business continuity plans will be produced, tested and maintained, to ensure that vital information services are available within defined service levels.

- ▶ Compliance with this policy will be enforced. Breaches of information security controls must be reported to and will be investigated by the Information Security Officer.

Appropriate information access and security involves knowing what information exists, permitting access to all who have a legitimate need and ensuring the proper and appropriate handling of information.

### 3. Definition

- ▶ *Information*

Information takes many forms and includes data stored on computers, transmitted across computer networks, printed, written, sent by post or fax, or stored on tapes or discs. Information may be either structured according to some defined format, or unstructured.

- ▶ *Access*

Access refers to mechanisms, whether legitimate or not, by which individuals gain access to information. The policy defines legitimate access and prescribes action to be taken to deal with unauthorised access.

- ▶ *Security*

Security refers to mechanisms and procedures designed to ensure that appropriate controls on information access are in place and are effective.

- ▶ *Confidentiality*

Confidentiality requires protection of information from unauthorised disclosure or intelligible interception (see below).

- ▶ *Integrity*

Integrity involves safeguarding the accuracy, completeness and consistency of information and of computer software.

- ▶ *Availability*

Availability involves ensuring that information and vital services are available to users when required.

- ▶ *Intelligible interception*

Intelligible interception is interception of information in such a way that it is readable; encryption of data may prevent intelligible interception.

- ▶ *Information assets*

Information (as defined above), computer software and hardware, computer systems

This Information Access and Security policy may be summarised as the preservation of confidentiality, integrity and availability, in line with the principles set out in BS7799.

### 4. Legal obligations and University policies

The policy should be read in conjunction with contracts of employment, university policies relating to the usage of information and systems, and relevant legislation, including :

- ▶ Policies on data protection and freedom of information
- ▶ Policies on disclosure of criminal records
- ▶ Regulations for the use of computer facilities (incorporating the JANET Acceptable Use policy)

- ▶ Policy for the investigation of computers and disposal of computer equipment
- ▶ Data Protection Act 1998, Human Rights Act 1998, Regulation of Investigatory Powers Act 2000, Freedom of Information Act 2000, Computer Misuse Act 1990, Copyright, Design and Patents Act 1988, Official Secrets Acts 1911-1989
- ▶ The Terrorism Act 2000, The Anti-Terrorism, Crime and Security Act 2001.

#### 5. Information classification

On advice from the University's Information Access Adviser (who advises on matters including data protection, freedom of information and records management), all information in the University will be classified by those responsible for the information into one of the following categories. Any disagreement as to classification will be resolved by the University Secretary.

- ▶ *Public*  
May be viewed by anyone, anywhere in the world.
- ▶ *Open*  
Available to all members of the University, but not to others.
- ▶ *Confidential*  
Available only to specified members of the University, with appropriate authorisation.
- ▶ *Strictly Confidential*  
Access is controlled and restricted to a small number of people.
- ▶ *Secret*  
For example, subject to or obtained under the Official Secrets Act.

Much information will fall into the public or open categories, but for good reason, such as personal privacy or protection of University interests, some information will be categorised as confidential or strictly confidential.

Information may also be categorised as either current, up to date and accurate, or historic, but held for good reason as a record. Historic information may be archived (i.e. retained but removed from prime information sources and possibly stored in a pared down form). Information must be deleted when there is no valid reason for retention. Disposal must be considered when the information is first acquired, as set out in the data protection policy.

#### 6. Access to information

All information will be classified as described above. Individuals will have access to information according to its classification. Data guardians will be responsible to the Information Access Adviser for ensuring that all information is appropriately classified and for ensuring the review and maintenance of information classification. The Information Access Advisor will oversee this process and will maintain the high level matrix. The University Secretary will be the final arbiter on issues relating to information classification and access. See below for definitions of Data Guardian, Information Access Adviser and other roles.

## 7. Roles & Responsibilities

All members of the University have responsibilities with respect to information, as summarised below. One person often has more than one role. In order to fulfil these responsibilities, members of the University must :

- ▶ be aware of this policy and comply with it
- ▶ understand to which information they have a right of access
- ▶ know the information for which they are guardians
- ▶ know the information systems and computer hardware for which they are responsible

### *Members of the University as information users*

All members of the University will be users of information. This carries with it a responsibility to abide by this policy and related policies and laws. No individual should be able to access information to which they do not have a legitimate access right. Systems should be in place to provide controls, but not withstanding this, no individual should knowingly contravene this policy, nor allow others to do so.

Information users must be aware of the nature of the information to which they have access must handle information appropriately, especially according to its classification. Information must protect the confidentiality of information and must not deliberately or inadvertently give access to others who do not have legitimate access. Examples of inadvertent access could include leaving confidential printed material where others might see it or leaving data visible on a computer screen where others might see it.

Many members of the University will have responsibility for the confidentiality, integrity and availability of information, for example :

- ▶ Heads of department are responsible for the confidentiality, integrity and availability of information maintained by members of the department, such as students' academic records. They are responsible overall for technical aspects of departmental information systems.
- ▶ Departmental administrators, departmental IT support staff and other staff in departments will have delegated authority from heads of department.
- ▶ Data and systems managers in support services are responsible for the confidentiality, integrity and availability of corporate information, such as student, personnel and financial data.
- ▶ Project managers (or equivalent), leading projects for the development or modification of information systems, are responsible for ensuring that projects take account of the needs of information access and security and that appropriate control mechanisms are instituted and are effective, so that the confidentiality, integrity and availability of information is guaranteed.

### *Systems administrators*

Computer systems administrators are responsible for ensuring that computer systems are effectively managed, to ensure information confidentiality, integrity and availability. This includes ensuring proper user administration (access controls, security

mechanisms) and data administration (access controls, security mechanisms, backup, safe disposal etc).

*Information Services staff*

- ▶ Information Services staff are responsible for ensuring that provision of University IT infrastructure is consistent with the demands arising out of this policy.
- ▶ The Assistant Director of Information Services (Information Systems & Computing) is responsible overall for ensuring the technical delivery of policy objectives with respect to the University and for provision of advice, guidance and where appropriate, direction to Heads of Department and departmental IT Support Staff.
- ▶ The Information Security Officer is responsible for compliance, investigating actual, potential or suspected breaches of this policy, typically from a technical perspective.

*University Secretary's Office*

- ▶ The Information Access Adviser is responsible for the appropriate classification of information and that the classification scheme is publicly available.
- ▶ The University Secretary is responsible for enforcement of this policy and for disciplinary procedures resulting from non-compliance.

8. Compliance

Compliance with this policy will be enforced according to University disciplinary procedures, which are overseen by the University Secretary. The Information Security Officer will advise the University Secretary and other senior managers on matters relating to compliance. Attention is drawn to laws and policies previously listed. Users should only access and use information for which they have appropriate authorisation and which is classified as being available to them.

Usage of information must be in an appropriate manner. Usage of systems and software must be in accordance with policies, laws and licensing constraints, and specific attention should be paid to copyright laws and licence agreements. In certain circumstances, the University will investigate the usage of information and information processing systems, and specific attention is drawn to the policy for the investigation of computers.

9. Summary of Technical Procedures

Procedures (set out in more detail in Appendix 2) will be put in place in order to ensure effective information access and security control, as follows :

- ▶ User registration procedures, authentication mechanisms and password usage for access to email and other computing facilities
- ▶ Control of and mechanisms for access to University computer networks, network system security, intrusion detection, prevention and remedial action
- ▶ Systems security procedures, including systems administration, monitoring and logging, security patches, virus protection, encryption
- ▶ Backup of computer systems
- ▶ Inventory of information assets, including equipment, software and data

- ▶ Systems change control, testing and acceptance
- ▶ Information access control for different classifications of information, database administration, regular review of user access rights
- ▶ Management of special (“super user”) systems privileges and utilities
- ▶ Disaster recovery and business continuity
- ▶ Physical security of computer rooms, networks, personal computers, computer maintenance and disposal
- ▶ Audit

The objective of these technical procedures is to ensure that :

- ▶ Information users are appropriately identified and have access to information for which they have a legitimate need
- ▶ Computer systems are appropriately managed and controlled in line with the requirements of this policy
- ▶ Information assets are identified and protected
- ▶ There is clear assignment of responsibilities

### ***Information Technology Security Policy***

The School depends upon the integrity of its computer based information and the availability of its information and communications technology (ICT) systems for its academic activity and administration. If these systems are unavailable or their information is compromised, teaching and learning may be disrupted, research delayed and administrative processes severely affected.

To protect against these risks the School has developed this Information Technology Security Policy which seeks to ensure that all School ICT systems are secured against loss caused by inadvertent or malicious actions. Every member of the School should be aware of this policy and act in a way that is consistent with their responsibilities as set out.

#### *Scope*

The Information Technology Security Policy is applicable to all existing and proposed systems and is effective from the date of issue of this policy. This includes all computers, peripheral equipment, software and data located within the School or owned by the School but located elsewhere. The manager responsible for each system must ensure that all risks are identified and all reasonable measures are taken to guard against security breaches.

All members of the School, including staff, students, visiting academics and researchers must ensure that they comply with the requirements of the Information Technology Security Policy. Any suspected breaches of security must be notified to the appropriate IT Services, MIS or Library cluster support team who will notify the named individual(s) responsible for the particular ICT system(s) affected.

#### *Physical Security*

Computing devices, such as laptops, may only be connected to the School’s network at designated connection points, (either cabled or wireless), or at another network point with the prior agreement of IT Services. Students who are resident in the Halls may connect their

computers to designated study bedroom network points. Other computer and data communications equipment may only be connected by authorised support staff.

All equipment must be maintained in good working order and all reasonable steps must be taken to meet the manufacturer's operating guidance. All equipment must be protected against fire, water, electrical fluctuations, physical damage and theft to an appropriate level commensurate with its replacement value and importance.

#### *Access Control*

With the exception of material intended for the general public, access to all ICT systems must be restricted to registered School users only. All activity involving the use of the School ICT systems or network must be capable of being traced to an individual.

School staff, students on a recognised course, applicants for courses who hold an offer, visiting academics, retired staff, alumni and other persons nominated by a senior officer of the School may be registered with a Username and password. Usernames must only be used by the person to whom they were issued and for the purpose for which they were issued.

Data and document owners must ensure that School information is protected against unauthorised disclosure, alterations or loss. All information must be backed up at a frequency appropriate to its importance. Sensitive information must also be protected against unauthorised reading and copying. This applies to information on personal computers as well as servers.

#### *Responsibilities*

The Library and Information Services Committee is responsible for the development and review of this Information Security Policy. The Librarian and Director of Information Services and the School Secretary and Director of Administration are responsible for ensuring that ICT managers implement the agreed policy.

The manager responsible for each ICT system must undertake regular risk analysis to ensure that all risks are identified and all reasonable measures are taken to prevent security breaches. The System Administrator(s) of each ICT system must ensure that the required security and access control policies are operative and effective and that the systems are maintained in line with current industry best practice.

Information owners and document creators must undertake regular risk analysis for each type of sensitive information or documents in their control and liaise with the appropriate ICT manager to ensure that the required protection mechanisms are in place. All members of the School are responsible for ensuring that they guard against physical risks to ICT equipment and unauthorised access to ICT systems. Any actions which appear to contradict this Information Security Policy should be reported to the appropriate team. Where there is any doubt about who the appropriate team may be, it should be reported to the cluster support team who will notify the named individual(s) responsible for the particular ICT system(s) affected.

#### *Advice and Guidance*

The cluster support team can provide advice and guidance on most information security issues. Where necessary they will refer enquiries to other members of IT Services or MIS staff for further action. This policy should be read in conjunction with the following supporting documents.

- ▶ The School Policy Statement on the Use of Information Technology

- ▶ Conditions of Use of IT Facilities at the LSE
- ▶ JANET Acceptable Use Policy
- ▶ The Security Handbook for System Administrators
- ▶ The Guide to Sensitive Electronic Information

### ***Memilih Firewall***

Ada banyak sekali tulisan mengenai Firewall, baik berupa artikel, whitepaper, hasil riset, terlebih jika Anda mengetikkan keyword "Firewall" pada mesin pencari pilihan Anda. Anda dapat mengatakan bahwa saya tidak sepenuhnya menulis artikel ini, karena apa yang saya tulis hanya rangkuman dari banyak konsep, teknologi, ide, yang secara beruntung dapat saya pelajari dari orang lain.

Mungkin Anda pernah membaca berita di portal berita detikinet.com pada bulan November tahun 2002, atau mungkin tahun sebelumnya di detik.com. Terdapat beberapa topik berita yang berkaitan dengan isu keamanan jaringan seperti "Mass Hacking", "Perang Cyber". Ada banyak pihak yang melihat bahwa terhubung dengan Internet adalah sangat tidak aman, rawan dari penyusupan crackers, pengintai.

Cukup sulit untuk mendeskripsikan berapa besar risiko yang akan ditanggung, baik secara organisasi maupun individu, dengan terhubung ke jaringan Internet. Bagaimanapun juga, dengan tidak terhubung ke jaringan Internet akan menutup kesempatan-kesempatan untuk mengembangkan usaha, memperluas pasar, atau menanggapi persepsi dari pelanggan. Jika Anda saat ini tidak merasa menghadapi masalah-masalah tersebut, mungkin dalam kurun waktu tiga atau lima tahun kedepan, Anda akan mengalaminya, dapat diumpamakan ketika Internet sudah menjadi keharusan dalam sebuah usaha seperti penggunaan telepon, Fax, papan nama, periklanan dan lain sebagainya.

Hal penting yang harus diingat ketika berurusan dengan keamanan di Internet adalah adanya persamaan antar isu keamanan di Internet dengan isu keamanan lainnya di dunia nyata. Memang benar, keamanan di Internet adalah hal baru, namun sangat perlu mendapat perhatian khusus demi berlangsungnya kegiatan ber-Internet sebagaimana yang diharapkan. Ingat, jika Anda terhubung dengan jaringan Internet, maka Anda adalah obyek yang sangat rentan untuk mendapatkan serangan, penyusupan, korban dari social-engineering, fraud, dan semua hal-hal buruk yang mungkin terjadi. Saya sangat menyayangkan ketika sebuah perusahaan yang telah menginvestasikan dana sedemikian besar untuk penyediaan infrastruktur, namun tidak dilindungi jaringannya dengan firewall. Sebagai konsistensi dalam keamanan jaringan, Anda harus mempunyai pengetahuan dalam bidang manajemen dan pandangan arsitektural terhadap kegiatan bisnis yang Anda jalani, tanpanya, Anda mungkin hanya mempunyai sebuah sistem pengaman yang statis.

Mungkin hal yang paling merugikan pada sebuah bisnis yang tengah berlangsung adalah penghentian kegiatan untuk sementara waktu (downtime). Untuk beberapa kasus, downtime dapat berakibat fatal pada bisnis terutama pada bisnis yang memiliki aktifitas non-stop - rumah sakit, bank, bursa saham. Sebelum melangkah lebih jauh, saya mengajak Anda untuk berpikir kembali mengenai :

1. Apa saja yang harus dilindungi ?
2. Seberapa mungkin orang lain akan merusak/mencuri/memanipulasinya ?
3. Apa efek yang ditimbulkan jika mereka berhasil ?

Untuk menjadi catatan, kerusakan potensial yang sangat tinggi dapat saja terjadi jika tidak terhubung dengan jaringan Internet. Beberapa perusahaan yang merasa tidak nyaman jika terhubung dengan jaringan Internet, menempuh cara dengan mengizinkan karyawan, mitra kerja, atau pihak lain untuk melakukan akses "dial-in".

Seringkali, perusahaan-perusahaan yang sangat ketat melindungi dirinya dengan firewall atau "tanpa terhubung ke Internet sama sekali" mempunyai modem yang dapat dipergunakan untuk dial-out ketempat lain atau ke provider. Hal ini juga berpotensi untuk mengundang attack. Menganalisa kebutuhan Salah satu metode efektif untuk menentukan jenis Firewall yang dibutuhkan adalah dengan menganalisa kebutuhan-kebutuhan berorientasi pada services yang diberikan atau digunakan. Services yang umum digunakan adalah :

- ▶ World WideWeb (WWW) - termasuk diantaranya adalah File Transfer Protocol (FTP), Web-Proxy.
- ▶ Electronic Mail (e-mail)
- ▶ Remote Connection - Secure Shell (SSH), Telnet.

Berdasarkan services yang digunakan, sebaiknya Anda menentukan apakah Anda membutuhkan perlakuan khusus terutama dikaitkan dengan isu keamanan. Tentukan pula jika Anda membutuhkan jenis audit dan pencatatan terhadap segala aktifitas berdasarkan services tersebut. Sebagai contoh, jika Anda mempunyai sebuah kebijakan keamanan (security policy) yang tidak mengizinkan karyawan melakukan FTP keluar, maka Anda seharusnya juga mempunyai policy yang sama dengan melarang karyawan mengirimkan attachment keluar, atau mengirimkan surat berisi floppy disk menggunakan pos. Konsistensi terhadap keamanan adalah kuncinya.

Selain itu, perlu dipertimbangkan juga kelangsungan dari penggunaan Firewall ini dikemudian hari. Jika Anda menginstall Firewall saat ini, apakah masih dapat terus digunakan selama 4 atau 5 tahun kedepan? Artinya, Anda tentu tidak akan menggunakan hardware yang sama dalam jangka waktu tersebut - lifecycle dari peralatan jaringan umumnya sangat pendek – namun pastikan bahwa arsitektur dasar yang Anda tempatkan akan bisa bertahan dalam jangka yang panjang.

### *Mengenal jenis Firewall*

Sebuah Firewall seharusnya menjadi sebuah pagar antara dua jaringan, diisi oleh suatu sistem yang banyak mengizinkan beberapa dari sejumlah jenis koneksi untuk lewat. Aspek penting dari sebuah Firewall adalah bagaimana ia melindungi dirinya sendiri dari serangan: sebuah Firewall tidak boleh dengan mudah ditembus, karena jika mudah ditembus maka penyusup akan sangat mudah menguasai jaringan yang ada dibelakangnya.

Bentuk sederhana dan paling populer dari metode firewall adalah "router screening". Kebanyakan dari router komersial telah memiliki kemampuan untuk memilah traffic - mengizinkan hanya traffic yang perlu dan melakukan pemblokiran terhadap traffic yang dianggap tidak perlu. Screening router beroperasi hanya pada level jaringan, dan digunakan untuk menentukan boleh atau tidaknya content lewat berdasarkan header paket TCP/IP. Cukup cepat, fleksibel, dan cenderung murah, namun mereka mempunyai kekurangan untuk menyediakan informasi audit secara detail tentang traffic yang lewat.

Bentuk kedua dari Firewall adalah "dual-homed gateway" dimana sebuah sistem dengan dua Network Interfaces (NIC) yang diletakkan pada jaringan yang dilindungi dan jaringan yang di luar. Firewall akan berfungsi sebagai "proxy" yang mengatur request kepada jaringan

yang ada diluar untuk diteruskan kepada pengguna. Proxy firewalls - juga disebut sebagai "application firewalls" - sangat atraktif karena proxy mampu memberikan informasi audit dari data yang diteruskan. Juga dirasakan oleh para ahli keamanan jaringan sebagai metode yang lebih aman karena proxy dapat dikustomisasi menjadi lebih spesifik untuk mengenali attack yang umum dari host yang ada dibelakangnya.

Beberapa waktu terakhir, sejumlah firewall yang menggunakan metode "dynamic packet filtering" muncul dipasaran. Sebuah dynamic packet filter firewall sama seperti sebuah penggabungan proxy firewall dan screening router. Bagi end-user, firewall jenis ini hanya beroperasi pada level jaringan, namun pada faktanya firewall ini mampu menjumlahkan traffic

yang lewat, seperti yang dimiliki oleh proxy firewall. Ketika seorang pengguna terhubung keluar, firewall jenis ini akan mencatat waktu dan mengijinkan data yang diminta untuk masuk kedalam, juga menjumlahkan durasi berapa lama koneksi berlangsung. Dynamic packet filtering adalah teknologi dinamis yang sangat menjanjikan diwaktu mendatang. packet filtering adalah teknologi dinamis yang sangat menjanjikan diwaktu mendatang.

#### *Bikin atau Beli?*

Secara tipikal Firewall membutuhkan waktu sekurang-kurangnya satu jam setiap minggunya untuk maintenance. Jika Firewall terhubung dengan jaringan Internet, maka dibutuhkan seseorang yang bertindak sebagai maintainer sama halnya seperti postmaster, webmaster, dan FTP maintainer, dengan waktu kerja penuh.

Untuk berhemat, Anda dapat membangun Firewall sendiri dengan menggunakan aplikasi opensource yang tersedia banyak di Internet. Tersedia banyak panduan membangun Firewall sendiri di Internet ataupun toko buku. Sebagai contoh, penggunaan Operating System dan aplikasi Firewall yang umum digunakan: Linux dengan IPTables, FreeBSD dengan IPF atau IPFW, dan OpenBSD dengan PF.

Penting untuk menentukan apakah Anda akan membeli Firewall komersil atau membangun sendiri. Faktor penentunya adalah waktu dan uang. Jika Anda mempunyai waktu yang cukup serta karyawan yang mampu, membangun sendiri Firewall mungkin akan menghemat banyak pengeluaran. Namun jika Anda mempunyai budget cukup untuk pembelian dan pemeliharaan maka ada banyak pilihan produk Firewall komersial yang beredar dipasaran. Sebelum membeli maka sebaiknya...

Memilih Firewall dapat diibaratkan memilih mobil. Diasumsikan sebagai mobil karena sebagian besar dari kita pernah melakukannya, sebelum membeli biasanya kita akan mengumpulkan informasi sebanyak mungkin dan meminta pendapat beberapa orang terhadap suatu jenis mobil yang hendak kita pilih. Cara terbaik untuk memilih Firewall yang tepat untuk keperluan Anda adalah dengan mencari sebanyak mungkin informasi mengenai Firewall dan mengedukasikan diri Anda pada topik seputar Firewall. Berikut adalah point yang sebaiknya Anda pertimbangkan sebelum Anda membeli.







#### ► *Keamanan*

Pikirkan kembali apa keinginan Anda, dan perkirakan bagaimana Firewall akan membantu kelangsungan bisnis Anda. Cobalah cari masukan dari orang lain yang lebih mengerti mengenai Firewall, dan tanyakan pendapat mereka. Cari referensi sebanyak mungkin.

- ▶ *Vendor*  
Cari tahu berapa lama mereka menjual produk Firewall yang mereka tawarkan, tanyakan referensi yang bisa Anda dapatkan. Mintalah selalu detail produk yang ditawarkan.
- ▶ *Dukungan teknis*  
Perkirakan berapa banyak karyawan yang akan ditugaskan untuk mengurus Firewall, juga hitung berapa operational-cost yang diperlukan. Bagaimana kebijakan perusahaan Anda mengenai upgrade dan downtime pada services. Juga pertimbangkan berapa lama perusahaan akan mengupgradenya dengan yang baru.
- ▶ *Dokumentasi*  
Mintalah salinan dokumentasi sebagai pegangan. Hal yang sama berlaku pada laporan audit dari firewall.
- ▶ *Operasional*  
Periksa apakah Firewall tersebut berikut hardware atau hanya sebuah software yang siap install. Juga periksa kebutuhan-kebutuhan Firewall tersebut, seperti network interface cards, cabling, dan lain-lain. Cari tahu apakah Firewall tersebut manageable, dan seberapa amankah jika Anda melakukan remote management.

Kebanyakan Firewall dijual sebagai bagian dari paket jasa konsultasi. Ketika sebuah Firewall dijual, biasanya instalasi dan dukungan teknis diberikan tergantung bagaimana negosiasi dan harga yang disetujui. Sepintas Anda mungkin tidak merasakan perbedaan antara menggunakan Firewall atau tidak. Benar, karena Firewall seharusnya berada pada stealthmode, Anda seharusnya tidak merasakan adanya perubahan signifikan dari Firewall. Firewall bekerja dengan menghalau paket yang tidak diinginkan dan mem-bypass paket yang diijinkan. Alangkah baiknya jika secara berkala Anda melakukan pemeriksaan rutin terhadap log yang dihasilkan oleh Firewall. Percaya atau tidak, Anda akan dikejutkan dengan berapa banyak percobaan intrusion atau worms yang melindungi jaringan Anda.

**Referensi :**

-  <http://budi.insan.co.id/courses/ec7010/dikmenjur-2004/joni-report.pdf>
-  [http://bebas.vlsm.org/v06/Kuliah/MTI-Keamanan-Sistem-Informasi/2005/122/122P-02-final1.0-access\\_control\\_systems\\_and\\_methodology.pdf](http://bebas.vlsm.org/v06/Kuliah/MTI-Keamanan-Sistem-Informasi/2005/122/122P-02-final1.0-access_control_systems_and_methodology.pdf)
-  <http://www.bris.ac.uk/WorkingGroups/CITG/IASPolicy.pdf>
-  <http://www.cert.or.id/~budi/books/handbook.pdf>
-  <http://www.lse.ac.uk/itservices/PoliciesPlans/Information%20Technology%20Security%20Policy.pdf>
-  <http://www.magnesium.net/~negative/text/memilih-firewall.pdf>