Internet

Pengertian Internet

Pada jaman sekarang kita dituntut untuk mengerti tentang manfaat dari jaringan karena jaringan adalah sebuah interkoneksi yang menghungkan kita untuk mengetahui dunia. Bukan hanya untuk itu saja tapi jaringan sangan penting untuk kita bergaul dan untuk mengetahui persaingan dalam sebuah bisnis.

Internet yang berasal dari kata Interconnection Networking yang mempunyai arti hubungan komputer dengan berbagai tipe yang membentuk sistem jaringan yang mencakup seluruh dunia (jaringan komputer global) dengan melalui jalur telekomunikasi seperti telepon, radio link, satelit dan lainnya.

Dalam mengatur integrasi dan komunikasi jaringan komputer ini digunakan protokol yaitu TCP/IP. TCP (Transmission Control Protocol) bertugas memastikan bahwa semua hubungan bekerja dengan benar, sedangkan IP (Internet Protocol) yang mentransmisikan data dari satu komputer ke komputer lain. TPC/IP secara umum berfungsi memilih rute terbaik transmisi data, memilih rute alternatif jika suatu rute tidak dapat di gunakan, mengatur dan mengirimkan paket-paket pengiriman data.

Untuk dapat ikut serta menggunakan fasilitas Internet, biasanya kita harus berlangganan ke salah satu ISP (Internet Service Provider) yang ada di kota kita. ISP ini biasanya disebut penyelenggara jasa internet ataupun kita dapat menggunakan fasilitas dari Telkom yakni Indihome.

Dengan memanfaatkan internet, pemakaian komputer di seluruh dunia dimungkinkan untuk salingberkomunikasi dan pemakaian bersama informasi dengan cara saling kirim e-mail, menghubungkan ke komputer lain, mengirim dan menerima file, membahas topik tertentu pada newsgroup dan lain-lain.

Fasilitas dan Istilah dalam Internet

Fasilitas-Fasilitas yang dapat di manfaatkan dengan menggunakan internet, diantaranya :

1. Electronic Main atau e-mail.
   Email adalah surat atau pesan elektronik yang dikirimkan dan diterima oleh dan antar individu atau komputer. Email bekerja seperti mesin penjawab telpon, walaupun kita tidak sedang online dengan internet kita masih bisa menerima email dari seluruh penjuru dunia.
   Saat ini, email tidak hanya berisi teks saja tetapi sudah bisa dilampiri dengan grafik, gambar foto dan juga suara bahkan animasi. Email juga dapat digunakan untuk berkirim surat secara langsung kepada beberapa orang sekaligus. Berkirim dan menerima email, saat ini sudah menjadi hal yang umum dilakukan orang di internet. Kita bisa berkomunikasi dengan siapa saja di seluruh dunia dengan fasilitas email ini, asalkan sudah memiliki alamat email tertentu.
   contoh alamat email : up@uniga.ac.id, steam2002@gmail.com
2. Discussion Group.
   Biasanya kita gunakan email untuk orang-orang yang sudah kita kenal dengan baik, akan tetapi kita juga dapat gunakan email untuk saling bertukar informasi, berdiskusi dan berdialog dengan orang lain. Kita dapat berpartisipasi dalam diskusi dan debat dengan topik yang beragam mulai dari hobi sampai pada permasalahan komputer atau malah masalah hiburan dan artis.
   - Maling List.
     Mailing List atau sering disebut milis di kalangan neter Indonesia, adalah salah satu jenis discussion group di Internet. Anggota milis dapat berkomunikasi dengan mengirimkan email pada list address. Setiap email yang masuk kemudian akan dikirim balik ke setiap member milis tersebut. Untuk menjadi member sebuah milis dimulai dengan mengirim email ke subsription address. Setelah menjadi member kita bisa menerima email dari yang lain dan juga mengirimkan email ke milis.
     Contoh alamat milis :
     list address : dgweb@yahoogroups.com
     langganan : dgweb-subscribe@yahoogroups.com
     berhenti : dgweb-unsubscribe@yahoogroups.com

- Newsgroups.
  Newsgroups adalah juga salah satu discussion groups yang ada di internet. Tidak seperti milis, newsgroups menggunakan komputer jaringan khusus yang disebut sebagai UseNet. Setiap komputer terdapat beberapa newsgroup. Setiap newsgroups diatur berdasarkan satu topik general yang kemudian dibagi menjai beberapa subtopik dibawahnya.
  contoh newsgroup : rec.arts.cinema
  rec adalah topik utama, arts adalah subtopik dan cinema sub-subtopik.

3. FTP
   FTP atau File Transfer Protocol, adalah layanan internet untuk melakukan transfer file antara komputer kita dengan server di internet. Cukup banyak server di internet yang menyediakan layanan ini sehingga kita bisa mengkopi file-file di server ke komputer kita, hal ini yang disebut download. Selain itu kita juga bisa mengkopi file-file di komputer kita ke server di internet, hal ini disebut dengan upload.
4. Telnet
   Beberapa server di internet memperbolehkan kita untuk mengaksesnya dan menjalankan beberapa program yang diinstal pada komputer itu. Layanan ini disebut sebagai telnet. Penggunaan server ini sama seperti kalau kita melakukannya pada komputer di jaringan lokal. Contohnya : spacelink.msfc.nasa.gov, adalah layanan telnet gratis dari NASA tentang sejarah dan seluk beluk NASA.
5. Gopher
   Gopher adalah aplikasi perangkat lunak yang tesusun atas untaian menu sistem pencarian dan penemuan kembali. Situs Gopher adalah komputer yang menampilkan menu-menu yang mewakili data dan informasi yang tersedia. Secara mendasar, menu-menu ini adalah daftar isi untuk mengolah dan menunjuk ke sebuah informasi tertentu. Layanan ini menggunakan FTP untuk pertukaran file dan Telnet untuk koneksi dengan server tertentu.
6. World Wide Web
   WWW (World Wide Web) adalah layanan internet yang paling banyak dikenal orang dan paling cepat perkembangan teknologinya. Layanan ini menggunakan link hypertext yang disebut hyperlink untuk merujuk dan mengambil halaman-halaman web dari server. Halaman web dapat berisi suara, gambar, animasi, text, dan program perangkat lunak yang menyusunnya menjadi dokumen yang dinamis. Pengguna dapat melihat World Wide Web dari sebuah browser yaitu program yang dapat menampilkan HTML (skrip halaman web).

Istilah-Istilah Yang Sering Digunakan dalam Internet, diantaranya yaitu:

1. WWW (World Wide Web), merupakan kumpulan web server dari seluruh dunia yang berfungsi menyediakan data dan informasi untuk digunakan bersama. Berbagai informasi dapat kita temukan pada WWW, seperti informasi politik, ekonomi, sosial, budaya, sastra, sejarah, teknologi, pendidikan dan sebagainya. Kita dapat mengumpamakan WWW ini merupakan perpustakaan besar yang menyediakan berbagai informasi yang dibutuhkan.
2. Web Site (Situs Web), merupakan tempat penyimpanan data dan informasi dengan berdasarkan topik tertentu. Diumpamakan situs Web ini adalah sebuah buku yang berisi topik tertentu.
3. Web Pages (Halaman Web), merupakan sebuah halaman khusus dari situs Web tertentu. Diumpamakan halaman Web ini adalah sebuah halaman khusus buku dari situs Web tertentu.
4. Homepage, merupakan sampul halaman yang berisi daftar isi atau menu dari sebuah situs Web.
5. Browser, merupakan program aplikasi yang digunakan untuk memudahkan kita melakukan navigasi berbagai data dan informasi pada WWW.

Manfaat Internet

Jika dilihat secara umum, internet memiliki banyak manfaat untuk mendukung aktivitas sehari hari, seperti:

1. Memberikan Informasi Untuk Kebutuhan Pribadi
   Kegunaan pertama dari internet adalah untuk memberikan informasi untuk kehidupan pribadi seperti rekreasi, kesehatan, hobi, pengembangan pribadi, sosial, rohani dan sebagainya.
2. Mempermudah Proses Sistem Akademik
   Internet tidak hanya sebatas dunia hiburan atau komunikasi, namun juga dipakai dalam bidang pendidikan khususnya untuk mengaturan sistem administrasi. Nantinya, internet bisa mempermudah proses mengurus data serta dokumen akademik di semua lembaga pendidikan.
3. Membantu Bisnis dan Usaha
   Internet juga memiliki kegunaan penting yang biasa disebut dengan Internet of Things. Ini merupakan konsep baru untuk memperluas fungsi serta manfaat jaringan internet. Fokus utamanya adalah mencakup hampir semua aspek kehidupan bersifat nyata seperti dipakai untuk bisnis dan usaha.

Revolusi Internet

Pertumbuhan internet yang sangat pesat adalah fenomena revolusioner dalam komputasi dan telekomunikasi. Internet telah menjadi jaringan yang terbesar dan terpenting dari jaringan saat ini, dan telah berevolusi menjadi jalan tol informasi(information superhighway) global.Internet semakin meluas seiring dengan semakin banyaknya bisnis, organisasi, computer, dan jaringan yang bergabung dengan Web global ini.

Ribuan jaringan bisnis, pendidikan, dan penelitian saat ini saling menghubungkan jutaan system computer dan pemakai di lebih dari 200 negara.Contohnya, pemakai internet di seluruh dunia diperkirakan antara 580 juta dan 655 juta orang pada tahun 2002, dengan perkiraan 710 juta hingga 945 juta pemakai internet pada tahun 2004.

Internet tidak memiliki system computer pusat atau pusat telekomunikasi.Setiap pesan yang dikirim memiliki kode alamat yang unik sehingga setiap server internet dapat mengirimnua ke tujusaannya. Selain itu, internet tidak memiliki kantor pusat atau badan pengatur. Kelompok individu dan anggota korporat untuk standard an nasehat internasional [seperti internet society (www.xxxx.org) dan Konsorsium World Wide Web (www.xxx.org)], mempromosikan penggunaan internet dan pengembangan standar komunikasi baru. Standar umum ini adalah kunci dari aliran bebas pesan antara berbagai computer dan jaringan di banyak organisasi dan internet service providers (Isp) dalam system ini.

Pengamanan Jaringan dan Etika

Jaringan

Keamanan jaringan adalah bentuk pencegahan atau deteksi pada hal yang bersifat gangguan dan akses tak seharusnya pada Sistem Jaringan Komputer. Langkah-langkah pencegahan membantu menghentikan pengguna yang tidak sah yang disebut “penyusup” untuk mengakses setiap bagian dari sistem jaringan komputer. Tujuan Keamanan jaringan komputer adalah untuk mengantisipasi resiko jaringan komputer berupa bentuk ancaman fisik maupun logic baik langsung ataupun tidak langsung mengganggu aktivitas yang sedang berlangsung dalam jaringan komputer.

Keamanan jaringan sangat penting dilakukan untuk memonitor akses jaringan dan mencegah penyalahgunaan sumber daya jaringan yang tidak sah. Tugas keamanan jaringan dikontrol oleh administrator jaringan. Segi-segi keamanan didefinisikan dari kelima point ini.

1. Confidentiality, mensyaratkan bahwa informasi (data) hanya bisa diakses oleh pihak yang memiliki wewenang.
2. Integrity, mensyaratkan bahwa informasi hanya dapat diubah oleh pihak yang memiliki wewenang.
3. Availability, mensyaratkan bahwa informasi tersedia untuk pihak yang memiliki wewenang ketika dibutuhkan.
4. Authentication, mensyaratkan bahwa pengirim suatu informasi dapat diidentifikasi dengan benar dan ada jaminan bahwa identitas yang didapat tidak palsu.
5. Nonrepudiation, mensyaratkan bahwa baik pengirim maupun penerima informasi tidak dapat menyangkal pengiriman dan penerimaan pesan.

Kebijakan Pengguna Jaringan

Kebijakan penggunaan jaringan terbagi menjadi 3:

1. Kebijakan Organisasi, adalah suatu kebijakan organisasi, istansi atau lembaga dalam ruang lingkup keamanan jaringan untuk akses pada sistem jaringan di tempat tersebut. Diantara contoh dari kebijakan organisasi adalah :
    a. Tata kelola sistem computer
    b. Pengaturan kerapian pengkabelan
    c. Pengaturan akses Wi-Fi
    d. Manajemen data organisasi
    e. Sinkronisasi antar sub-organ
    f. Manajemen Sumber Daya
    g. Maintenance & Checking berkala
2. Etika Menggunakan Jaringan, setiap kita melakukan suatu kegiatan pasti ada aturan atau etika yang harus dilakukan, karena jika tidak bisa berdampak negatif bagi kita sendiri maupun orang lain. Begitu juga saat menggunakan jaringan kita juga harus memperhatikan etika- etika yang berlaku. Diantaranya etika tersebut adalah:
    a. Memahami Akses Pengguna
    b. Memahami kualitas daya Organisasi
    c. Pengaturan penempatan sub-organ
3. Kebijakan Mengakses Komputer, dalam suatu kebijakan pengguna jaringan, tidak jarang juga terdapat kebijakan pengguna saat mengakses komputer, diantaranya adalah :
    a. Manajemen pengguna
    b. Manajemen sistem computer
    c. Manajemen waktu akses

Kemungkinan Ancaman dan Serangan Terhadap Keamanan jaringan

Saat kita saling terhubung dalam suatu jaringan baik jaringan kecil maupun besar, pasti terdapat ancaman ataupun seranagan yang bisa terjadi. Sehingga kita diharuskan untuk lebih berhati- hati saat berkomunikasi menggunakan jaringan. Diantara ancaman atau serangan yang bisa terjadi darikeamanan jaringan adalah :

1. Serangan Fisik Terhadap Keamanan Jaringan.
   Kebanyakan orang beranggapan bahwa serangan terhadap keamanan jaringan cenderung pada non-hardwarenya saja, tetapi sebenarnya serangan tersebut bisa terjadi pada hardware itu sendiri. Sebagai contoh saat jaringan kita dihack oleh orang lain, maka software baik data, file ataupun aplikasi akan rusak yang bisa juga menyebabkan hardware kita tidak bekerja secara normal, sehinggan hardware kita akan mengalami kerusakan. Serangan fisik terhadap keamanan jaringan dapat menyebabkan beberapa kerugian, diantaranya :
   a. Terjadi gangguan pada Kabel
   b. Kerusakan Harddisk
   c. Konsleting
   d. Data tak tersalur dengan baik
   e. Koneksi tak terdeteksi
   f. Akses bukan pengguna
2. Serangan Logic Terhadap Keamanan jaringan
   Serangan logic pada keamanan jaringan adalah hal yang paling rawan terjadi, sehingga kita harus lebih memperhatikan lagi security dalam jaringan kita. Diantara serangan yang bisa terjadi adalah :
   a. SQL Injection adalah Hacking pada sistem komputer dengan mendapat akses Basis Data pada Sistem.
   b. DoS (Denial of Service) adalah Serangan pada Sistem dengan mengabiskan Resource pada Sistem.
   c. Traffic Flooding adalah Serangan pada keamanan jaringan dengan membanjiri Traffic atau lalu lintas jaringan.
   d. Request Flooding adalah Serangan dengan membanjiri banyak Request pada Sistem yang dilayani Host sehingga Request banyak dari pengguna tak terdaftar dilayani oleh layanan tersebut.
   e. Deface adalah adalah Serangan pada perubahan tampilan
   f. Social Engineering adalah Serangan pada sisi sosial dengan memanfaatkan kepercayaan pengguna. Hal ini seperti fake login hingga memanfaatkan kelemahan pengguna dalam socialmedia.
   g. Malicious Code adalah Serangan dengan menggunakan kode berbahaya dengan menyisipkan virus, worm atau Trojan Horse.
      - Virus: Program merusak yang mereplikasi dirinya pada boot sector atau dokumen.
      - Worm: Virus yang mereplikasi diri tidak merubah fle tapi ada di memory aktif.
      - Trojan Horse: Program yang sepertinya bermanfaat padahal tidak karena uploaded hidden program dan scipt perintah yang membuat sistem rentan gangguan.
   h. Packet Sniffer adalah Serangan Menangkap paket yang lewat dalam sebuah Jaringan.

Data

Sebuah informasi harus aman, dalam arti hanya diakses oleh pihak – pihak yang berkepentingan saja sesuai dengan sifat dan tujuan dari informasi tersebut. Privacy Information (Security), sebuah informasi harus aman, dalam arti hanya diakses oleh pihak – pihak yang berkepentingan saja sesuai dengan sifat dan tujuan dari informasi tersebut. Aspek utama dalam keamanan data dan informasi adalah :

1. Privacy/Confidentiality, yaitu usaha menjaga data informasi dari orang yang tidak berhak mengakses (memastikan bahwa data atau informasi pribadi kita tetap pribadi)
2. Integrity, yaitu usaha untuk menjaga data atau informasi tidak diubah oleh yang tidak berhak.
3. Authentication, yaitu usaha atau metoda untuk mengetahui keaslian dari informasi, misalnya apakah informasi yang dikirim dibuka oleh orang yang benar (asli) atau layanan dari server yang diberikan benar berasal dari server yang dimaksud.
4. Availability, berhubungan dengan ketersediaan sistem dan data (informasi) ketika dibutuhkan.

Pihak yang memiliki peranan dan tanggung jawab dalam penerapan usaha pengamanan sistem informasi adalah:

1. Jajaran Manajemen Senior
2. Manajer Fungsional
3. Manajer keamanan informasi / computer
4. Staf ahli teknologi
5. Organisasi pendukung
6. Pengguna atau user

Ancaman terhadap keamanan data dan informasi

1. Hardware Dicuri atau dirusak
2. Software Program dihapus di copy atau dimodifikasi
3. Data File dihapus, dirusak, dicuri, disadap, dimodifikasi
4. Jaringan komunikasi diputus, Informasi dimodifikasi

Jenis-jenis ancaman terhadap Keamanan Data dan Informasi

1. Error dan kesalahan data. Dalam pengolahan data kita sering melakukan kesalahan input dan adanya error pada system
2. Penipuan dan pencurian data. Adanya pihak-pihak tertentu yang ingin memanfaatkan data dan informasi untuk hal-hal negatif yangakan merugikan pihak pemilik data atau informasi.
3. Sabotase pegawai. Dalam hal ini semua pegawai dalam satu perusahaan sepakat untuk tidak bertanggung akan akan kebaradaan informasi atau data yang penting dalam perusahaan itu.
4. Kegagalan dukungan infrastruktur. Infrastuktur atau fasilitas untuk keamanan data dan informasi kurang memadai
5. Serangan hacker jahat. Adanya serangan hacker ke pusat database dan informasi kita. Dimana para hacker disini biasanya akan mengacaukan,mengubah, menghapus data-data kita dan tentunya akan sangat merugikan kita.
6. Program berbahaya

Cara meningkatkan keamanan informasi:

1. Bantuan pengguna (user support)
2. Dukungan perangkat lunak (software support)
3. Manajemen konfigurasi
4. Backup
5. Kontrol media
6. Dokumentasi
7. Perawatan (maintenance)

WEB

Web merupakan suatu tempat mempresentasikan informasi dalam bentuk teks, gambar, suara, dll dalam bentuk hypertext dan dapat diakses oleh perangkat lunak yang disebut browser. Kegunaan dari web tidak hanya untuk browsing, tetapi juga untuk melayani end user melalui antarmuka browser mereka. Komponen Web menggunakan berbagai protokol dan layanan untuk memberikan konten yang diinginkan end user. Banyak pemilik website tidak memperhatikan keamanan website karena:

1. Menganggap bahwa perusahaan mereka masih kecil dan tidak mungkin ada hacker yang mau melirik.
2. Hacker menggunakan tools/software otomatis untuk menemukan situs yang memiliki kriteria kelemahan-kelemahan tertentu.

Web Browser adalah program / aplikasi yang digunakan untuk membuka halaman web. Website adalah brand, pintu depan, bahkan sebagian merupakan wadah/media yang pertama kali menghubungkan perusahaan dengan customer. Semakin besar interaksi customer dengan website, makin tinggi kebutuhan keamanan untuk website tersebut. Mengapa demikian? Karena akan semakin tingginya serangan hacker yang berdampak buruk pada relasi bisnis, baik itu bussiness to bussiness maupun bussiness to consumer. Hacker dapat menyisipkan malware yang bekerja mengambil data customer.

Web Server adalah perangkat lunak server yang berfungsi menerima permintaan HTTP/HTTPS dari klien dan mengirimkan hasilnya dalam bentuk halaman web (dokumen HTML). Pada dasarnya tugas web server adalah :

1. Menerima permintaan (request) dari client
2. Mengirimkan apa yang diminta oleh client (response).

Sistem Kerja Web

1. User mengakses website berupa URL melalui Web Browser (media untuk menuju URL yang diakses),
2. Web Browser mengirimkan permintaan berupa HTTP Request kepada Web Server melalui layer TCP/IP
3. Web Server memberikan Web Files yang di-request (jika ada) melalui HTTP Response melalui layer TCP/IP
4. Web Browser menerima Web Files, dan kemudian dikirimkan kepada User berupa Display.

Sistem Kerja Web Server

1. Client (user) meminta suatu halaman ke server untuk ditampilkan dikomputer client. Misalnya dengan mengetikkan suatu alamat/URL di browser http://www.google.com.
2. Melalui protokol http, dicarilah komputer bernama www.google.com.
3. Jika ditemukan, maka seolah-olah terjadi permintaan, “hai google, ada client yang minta halaman utama, ada dimana halamannya?”. Inilah yang disebut request.
4. Dari sisi server, web server mendapat permintaan halaman utama google dari client, si server akan mencari halaman sesuai permintaan.
5. Jika ditemukan, maka halaman yang diminta akan dikirimkan ke client,
6. Jika tidak ditemukan, maka server akan memberi pesan “404. Page Not Found”, yang artinya halaman tidak ditemukan.

Penanganan Ancaman Pada Web

1. Mencegah user yang tidak sah untuk mengakses data sensitif.
    a. Otentikasi: mengidentifikasi user untuk menentukan apakah mereka adalah orang yang berwenang

    b. Akses kontrol: mengidentifikasi sumber daya yang membutuhkan perlindungan dan siapa saja yang memiliki akses kepada mereka.
2. Mencegah penyerang mencuri data selama transmisi. Enkripsi (biasanya dengan Secure Sockets Layer)
3. Mengumpulkan informasi user ID dari end user ("log in").
    a. biasanya melalui dialog / antarmuka browser.
    b. informasi user ID biasanya mengacu pada username dan password.
4. Memindahkan informasi user ID ke server web. Tidak aman (HTTP) maupun aman (HTTPS = HTTP melalui SSL)
5. Verifikasi ID dan password .
    a. Realms menyimpan username, password, dll, dapat diatur dengan cara LDAP, RDBMS, dll
    b. Validasi: cek di server web jika user ID & password match dengan yang ada di Realms.
6. Menjaga otentikasi user sebelumnya untuk operasi HTTP selanjut