Keamanan Sistem World Wide Web

Sejarah singkat WWW

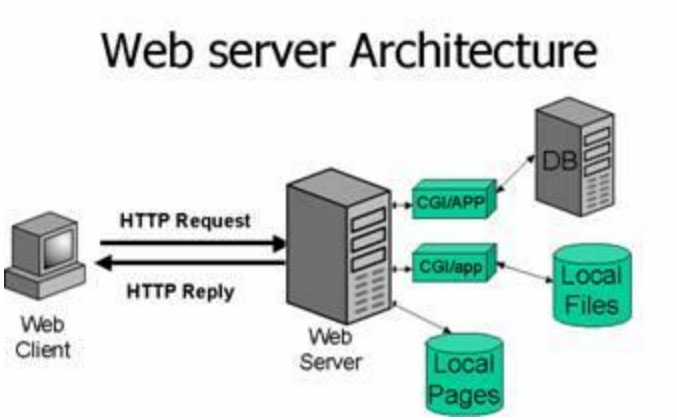
- Dikembangkan oleh Tim Berners-Lee ketika bekerja di CERN(Swiss). Untuk membaca atau melihat sistem WWW digunakan tools yang dikenal dengan istilah *browser.*

- Sejarah browser dimulai dari NeXT. Selain NeXT, saat itu ada browser yang berbentuk text seperti “line mode” browser. Kemudian ada Mosaic yang multi-platform (Unix/Xwindow, Mac, Windows) dikembangkan oleh Marc Andreesen dkk ketika sedang magang di NCSA.

- Arsitektur sistemWeb terdiri dari dua sisi: Server dan client.
  - Server (apache, IIS)
  - Client
- - IE, Firefox, Netscape, Mozilla, Safari, Opera, Galeon,
- kfm, arena, amaya, lynx, K-meleon
- • Terhubung melalui jaringan
- • Program dapat dijalankan di server (CGI,[java] servlet)
- atau di sisi client (javascript, java applet
  - Memungkinkan untuk mengimplementasikan sistem secara tersentralisasi

- Client hanya membutuhkan web browser (yang ada disemua komputer), thin client
- Update software bisa dilakukan di server saja, tanpa perlu mengubah sisi client
- Browser di sisi client dapat ditambah dengan “plugin” untuk menambahkan fitur (animasi, streaming audio & video); Macromedia Flash / Shockwave
- Mulai banyak aplikasi yang menggunakan basis web Aplikasi baru
- Blog
- Authentication
- Selain menyajikan data-data dalam bentuk statis, sistem Web dapat menyajikan data dalam bentuk dinamis dengan menjalankan program. Program ini dapat dijalankan di server (misal dengan CGI, servlet) dan di client (applet, Javascript).
- Server WWW menyediakan fasilitas agar client dari tempat lain dapat mengambil informasi dalam bentuk berkas (file), atau mengeksekusi perintah (menjalankan program) di server. Fasilitas pengambilan berkas dilakukan dengan perintah “GET”.

- Mekanisme untuk mengeksekusi perintah di server dapat dilakukan dengan "CGI" (Common Gateway Interface), Server Side Include (SSI), Active Server Page (ASP), PHP, atau dengan menggunakan *servlet (seperti pernggunaan Java Servlet).*



informasi yang ditampilkan di server diubah (dikenal dengan istilah *deface)*

- informasi yang semestinya dikonsumsi untuk kalangan terbatas (misalnya laporan keuangan, strategi perusahaan, atau database client) ternyata berhasil disadap oleh orang lain.
- server diserang (misalnya dengan memberikan *request* secara bertubi-tubi) sehingga tidak bisa memberikan layanan ketika dibutuhkan (*denial of service attack);*

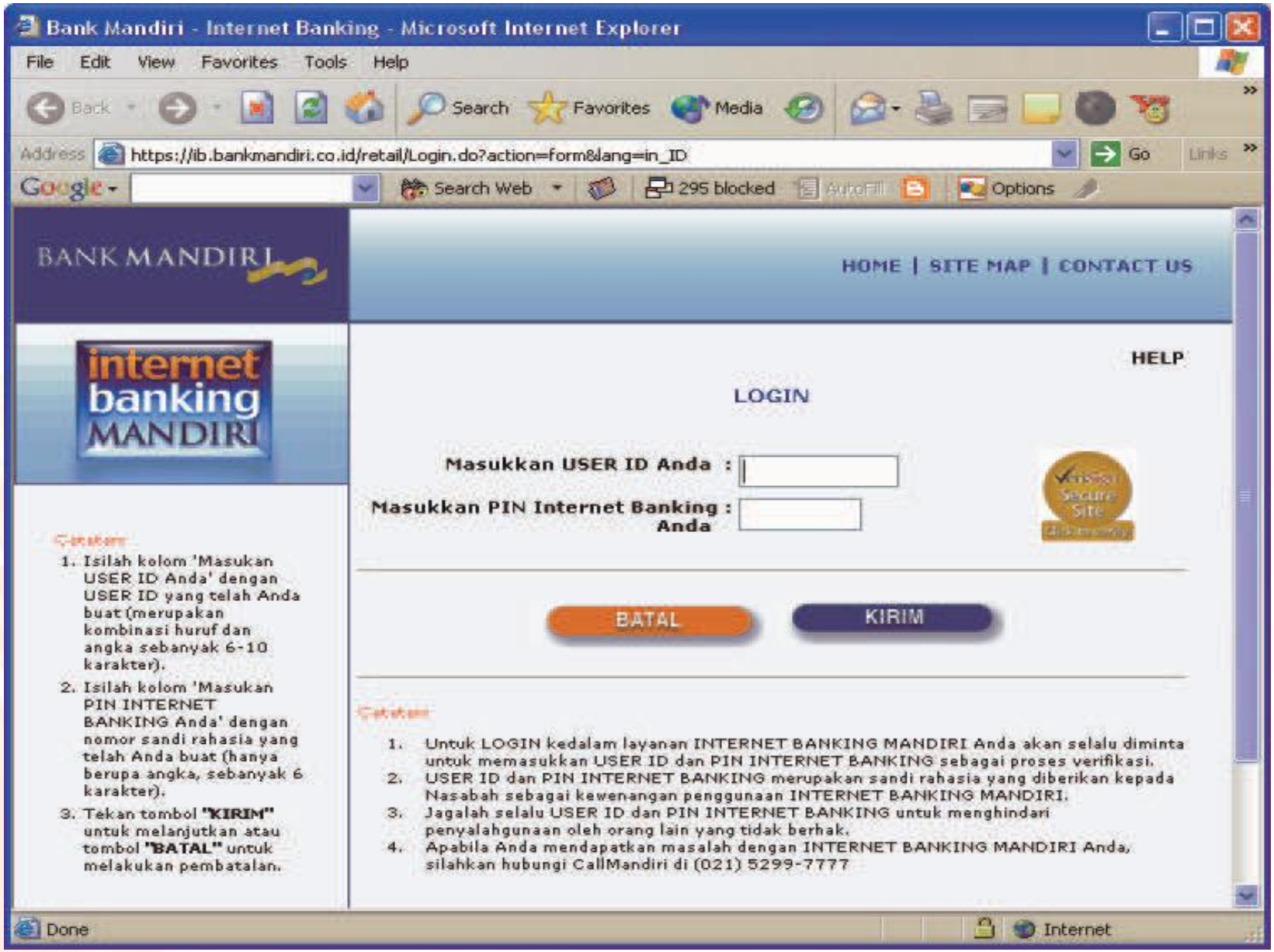
Adanya lubang keamanan di sistem WWW dapat dieksploitasi dalam bentuk yang beragam, antara lain:

Informasi Deface http://www.zone-h.org/

Membatasi akses melalui Kontrol Akses Pembatasan akses dapat dilakukan dengan:

- **Membatasi domain atau nomor IP yang dapat mengakses**; (konfigurasi Web server atau Firewall
- **Menggunakan pasangan userid & password**
- **Mengenkripsi data** sehingga hanya dapat dibuka (dekripsi) oleh orang yang memiliki kunci pembuka.
- **Secure Socket Layer** Dengan menggunakan enkripsi, orang tidak bisa menyadap data – data (transaksi)yang dikirimkan dari/ke server WWW. Salah satu mekanisme yang cukup populer adalah dengan menggunakan *Secure Socket Layer (SSL) yang mulanya dikembangkan oleh Netscape.*
- **Server WWW *Apache*** *(yang tersedia secara gratis) dapat* dikonfigurasi agar memiliki fasilitas SSL dengan menambahkan software tambahan (SSLeay – yaitu implementasi SSL dari Eric Young – atau OpenSSL1 – yaitu implementasi Open Source dari SSL).
- **Penggunaan SSL** memiliki permasalahan yang bergantung kepada lokasi dan hukum yang berlaku.

Computer Security




https://ibank.klikbca.com/
Headlines
SSL Server Certificate Verification
INDIVIDUAL
[HOME]
Silakan memasukkan USER ID Anda
Please enter Your USER ID
Klik BCA is secured with SSL 128 bit encryption.
cybertrust secured website
Silakan memasukkan PIN Internet Banking Anda
Please enter Your Internet Banking PIN
LOGIN
Catatan : - Anda harus menggunakan 'KeyBCA' setiap kali Anda melakukan transaksi finansial.
- Situs ini hanya dapat ditampilkan dengan menggunakan Internet Explorer ver. 6.0 keatas.
Notes : - You have to use 'KeyBCA' to do financial transaction.
- This site can be viewed only with Internet Explorer ver. 6.0 and above.

Mengetahui Jenis Server

- Informasi tentang web server yang digunakan dapat dimanfaatkan oleh perusak untuk melancarkan serangan sesuai dengan tipe server dan operating system yang digunakan.
- Informasi tentang program server yang digunakan dapat dilakukan dengan menggunakan program “telnet” dengan melakukan telnet ke port 80 dari server web.
- Program *Ogre (yang berjalan di sistemWindows) dapat* mengetahui program server web yang digunakan.
- Untuk sistem UNIX, program *lynx dapat digunakan untuk* melihat jenis server dengan menekan kunci “sama dengan” (=).

Keamanan Program CGI

- Common Gateway Interface (CGI) digunakan untuk menghubungkan sistemWWW dengan software lain di server web. Adanya CGI memungkinkan hubungan interaktif antara user dan server web. CGI seringkali digunakan sebagai mekanisme untuk mendapatkan informasi dari user melalui “fill out form”, mengakses database, atau menghasilkan halaman yang dinamis. Secara prinsip mekanisme CGI tidak memiliki lubang keamanan, program atau skrip yang dibuat sebagai CGI dapat memiliki lubang Keamanan. Program CGI ini dijalankan di server web sehingga menggunakan resources web server tersebut dan membuka potensi lubang keamanan.

Lubang Keamanan CGI

Beberapa contoh :

- CGI dipasang oleh orang yang tidak berhak
- CGI dijalankan berulang-ulang untuk menghabiskan resources (CPU, disk): DoS

Penyisipan karakter khusus untuk shell expansion
• Kelemahan ASP di sistemWindows
• Guestbook abuse dengan informasi sampah (pornografi)
• Akses ke database melalui perintah SQL (SQL injection

Keamanan client WWW

Pelanggaran Privacy

• Adanya penyimpanan data browsing pada "*cookie*" yang fungsinya adalah untuk menandai kemana user browsing.
• Adanya situs web yang mengirimkan script (misal Javascript) yang melakukan interogasi terhadap server client (melalui browser) dan mengirimkan informasi ini ke server.
• **Attack (via active script, javascript, java)**
- Pengiriman data-data komputer (program apa yang terpasang, dsb.)
- DoS attack (buka windows banyak)
- Penyusupan virus, trojan horse, spyware

BCP & DRP

Komponen BCP

Komponen BCP mencakup:

- Siapa penanggung jawab utama.
- Backup dari supplies yang dibutuhkan.
- Pengorganisasian dan penanggung jawab setiap aktifitas.
- Jaringan komputer.
- Asuransi.

BCP & DRP

Key Decision Making Personel

- Berisi daftar orang yang harus menginisiasi dan melaksanakan kegiatan recovery. Biasanya berupa daftar nomor telepon.

BCP & DRP

Key Decision Making Personel

Daftar itu sepatutnya mencakup:

- Siapa yang harus di-contact terlebih dahulu.
- Emergency telephone numbers, termasuk ketua tim.
- Telepon vendor-vendor, termasuk supplier.
- Telepon dari recovery facility.

BCP & DRP

Key Decision Making Personel

- Telepon penyelenggara jasa telekomunikasi.
- Telepon dari orang yang menyimpan backup data.
- Telepon asuransi.
- Telepon orang-orang kontrakan (jika yang melakukan recovery bukan orang operasional), terutama jika alternate facility ada di daerah lain.

BCP & DRP

Backup of Required Supplies

- Harus ada pula persediaan kertas-kertas (berlogo perusahaan) dan formulir-formulir perusahaan agar siap untuk dipakai.

BCP & DRP

Organization & Assignment of Responsibilities

- Ada tim-tim yang bertugas melakukan fungsi tertentu dalam BCP, dan dipimpin seorang *team leader*.

BCP & DRP

Organization & Assignment of Responsibilities

Tim-tim:

- Emergency action team:
  - Tugas utamanya adalah seperti “pemadam kebakaran”, dan bertugas untuk menyelamatkan jiwa
- Damage assessment team:
  - Harus bisa mengkalkulasi dampak bencana.
  - Bisa memperkirakan kapan lokasi bisa kembali normal

BCP & DRP

Organization & Assignment of Responsibilities

- Emergency management team:
  - Berkewajiban mengkoordinasikan aktifitas tim-tim lainnya.
  - Melakukan decision making: apakah akan menjalankan DRP atau tidak
  - Termasuk menangani masalah hukum dan public relations.
- Off site strorage team
  - Packing dan shipping dari media dan records ke offsite facility.

BCP & DRP

Organization & Assignment of Responsibilities

- Software team:
  - Restore operation system
- Applications team:
  - Pergi ke recovery site dan menginstall kembali aplikasi komputer
- Emergency operations team:
  - Shift operators & shift supervisors yang harus menjalankan recovery site (alternate facility)

BCP & DRP

Organization & Assignment of Responsibilities

- Salvage team
  - Melakukan analisis lebih mendalam terhadap dampak bencana
  - Menentukan apakah akan memperbaiki lokasi yang kena bencana, atau melakukan proses relokasi
  - mengisi form klaim asuransi
- Relocation team
  - Mengembalikan dari recovery site ke lokasi awal atau ke lokasi baru yang permanen

BCP & DRP

Jaringan Komputer

- Meliputi jaringan cadangan, link telekomunikasi, rute cadangan, alat komunikasi

Asuransi

- BCP harus mencakup masalah asuransi dan cara klaim-nya juga

BCP & DRP

Pemilihan Strategi Pemulihan

Asuransi

- Diperlukan bila terjadi kecelakaan
- Namun dengan adanya rencana yang memadai, maka biaya premi asuransinya biasanya lebih kecil
- BCP harus mencakup masalah asuransi dan cara klaim-nya juga

BCP & DRP

Pemilihan Strategi Pemulihan

Beberapa yang mungkin diasuransikan antara lain:

- Peralatan dan fasilitas IT
- Fasilitas backup yang ada
- Data
- Business interuption cost: kerugian akibat berhentinya aktifitas perusahaan
- Valuable papers & records, akibat hilangnya surat-surat berharga

BCP & DRP

Pemilihan Strategi Pemulihan

Data Recovery Center

- Menduplikasi fasilitas pemrosesan informasi
- Hot DRC
  - Fasilitas alternatif yang memiliki sarana sama seperti data center yang sebenarnya.
  - Sistem dengan aplikasi, link komunikasi yang sama sudah terpasang dan tersedia di lokasi DRC
  - Data dibackup menggunakan koneksi live antara data center dan lokasi DRC
  - Operasional bisnis kan berjalan pada saat itu juga
  - Untuk aplikasi yang *critical,* misalnya perbankan, bursa efek
  - Namun biayanya sangat mahal.

BCP & DRP

Pemilihan Strategi Pemulihan

- Warm DRC
  - fasilitas alternatif yang memiliki sarana yang lebih sedikit.
  - Misalnya ada listrik, jaringan, telepon, meja-meja, printer, tetapi tanpa komputer yang mahal.
  - Kadang-kadang ada komputer, tetapi less processing power.
  - misalnya backup sebuah website dengan komputer dan bandwidth yang lebih rendah
- Cold DRC
  - fasilitas yang memiliki prasarana penunjang untuk operasi komputer, misalnya ruangan yang memiliki listrik dan AC. Tapi belum ada komputernya, namun siap dipasangi komputer.

BCP & DRP

Pemilihan Strategi Pemulihan Telekomunikasi

- Jaringan cadangan
  - Bila jaringan yang satu bermasalah, maka jaringan cadangan akan digunakan
- Rute alternatif
  - Mengunakan media komunikasi alternatif, misalnya bila link antar cabang menggunakan vsat, maka alternatifnya menggunakan line telpon
  - Melalui jalur yang berbeda
- Link komunikasi jarak jauh lebih dari satu
  - Agar bila terjadi masalah, masih memiliki link yang lainnya.
- alat komunikasi
  - Agar bisa saling berkomunikasi, misalnya HT

BCP & DRP

Pemilihan Strategi Pemulihan

Strategi business continuity antara lain:

- Tidak melakukan apa-apa sampai *recovery facility* sudah 'on'.
- Melakukan prosedur manual.
- Memfokuskan diri pada proses yang penting saja: customer, products, dsb.
- Menggunakan PC untuk *data capture* (pencatatan saja) dengan pengolahan minimal. Pengolahan baru dilakukan setelah *recovery facility* sudah bekerja.

BCP & DRP

Pertimbangan dalam BCP

Saat membangun BCP

- Harus melibatkan seluruh perusahaan, tidak hanya bagian IT saja. Kalau tidak ada BCP lapisan perusahaan, maka BCP dari sistem informasi harus menyertakan bagian lain yang terkait dengan BCP
- Staf-staf yang diperlukan untuk menjalankan fungsi bisnis yang penting saat terjadi bencana.

BCP & DRP

Permasalah Fasilitas Altenatif

- Configuration – apakah konfigurasi hardware & software sudah tepat?
- Audit - Apakah kita boleh mengaudit alternate site/facility?
- Testing - Apakah testing diperkenankan
- Reliability: sepatutnya vendor pun harus bisa menjamin kehandalannya

BCP & DRP

Recovery Plan Testing

- Untuk membukti bahwa BCP bekerja, maka BCP harus diuji. Tes dilakukan saat gangguan pada operasi dinilai kecil, misalnya weekend. Seluruh anggota recovery team harus ikut

BCP & DRP

Recovery Plan Testing

Yang dilakukan dalam pengujian BCP:

- Memeriksa kelengkapan dan ketepatan dari BCP
- Mengevaluasi kinerja dari orang-orang yang terlibat dalam uji coba
- Menilai cara training dan program penyadaran staf-staf lain
- Mengevaluasi koordinasi antara tim BC dan external entity, seperti vendor, supplier dan penyelenggara jasa lainnya.
- Mengukur kapasitas situs alternatif.
- Mengukur tingkat *retrieveablitiy* dari informasi penting.
- Mengukur kinarja operasional dari bisnis secara umum.

BCP & DRP

Recovery Plan Testing

Tahap pengujian:

- Pre-test
  - Persiapan sebelum pengujian, misalnya memasang kabel-kabel di alternate facility atau membawa peralatan komunikasi ke alternate facility. Jadi esensinya memastikan bahwa fasilitas alternatif selalu siap

BCP & DRP

Recovery Plan Testing

Tahap pengujian:

- Test
  - Seluruh kegiatan operasional untuk mendukung business objectives tertentu dilaksanakan. Misalnya: data entry, telephone calls, information systems processing, penanganan order, workflow, dsb
- Post-Test
  - Mengembalikan alat-alat yang perlu dikembalikan ke tempatnya semula. Tapi yang paling penting adalah analisis formal dan perbaikan-perbaikan BCP

BCP & DRP

Pemeliharaan dan Perubahan BCP

- BCP jangan dibiarkan bertahun-tahun tanpa ditinjau kembali

Perubahan bisa disebabkan karena:

- Aplikasi baru telah dikembangkan
- Perubahan strategi bisnis, menyebabkan aplikasi yang dianggap kritis berubah
- Perubahan hardware & software

BCP & DRP

Pemeliharaan dan Perubahan BCP

Untuk melakukan maintenance BCP dapat dilakukan antara lain:

- Periodic review.
- Komentar terhadap hasil review.
- Melakukan pengujian BCP terjadual maupun mendadak.
- Melakukan updating BCP.
- Updating BCP, termasuk daftar nama & nomor telepon.

TERIMA KASIH