Tugas M.K: SIM
Dosen : Prof. Dr. Ir. Kudang Boro Seminar MSc (CS)

Tanggal Penyerahan : 14 Juli 2011
Tanggal Presentasi : _____

TUGAS SIM

DATABASE & DATA SECURITY

(Kasus: PayPal)

Kelompok ANGGUR

Agung Wahyu Wasisto	**P056100032.35E**
Anita Wijayanti	**P056100072.35E**
Indra Setia Dewi	**P056100222.35E**
Mahesa Umbara	**P056090562.33E**
Mohamad Taufik	**P056100282.35E**
Nurdin Nurhayadi Kosasih	**P056091631.44**
Taufiq Kurniawan	**P056100382.35E**

MB-IPB

PROGRAM PASCASARJANA MANAJEMEN DAN BISNIS

INSTITUT PERTANIAN BOGOR

2011

Table of Contents

Daftar Gambar

BAB I. PENDAHULUAN

1.1 Latar Belakang

Informasi tidak hanya sekedar produk sampingan, namun sebagai bahan yang menjadi faktor utama yang menentukan kesuksesan atau kegagalan, oleh karena itu informasi harus dikelola dengan baik. Informasi adalah data yang diolah menjadi bentuk yang lebih berguna, lebih berarti dan bermanfaat bagi penggunanya. Sebelum menjadi informasi, data yang berkualitas, kemudian diolah melalui suatu model untuk menghasilkan informasi. Model yang digunakan untuk mengolah data tersebut disebut model pengolahan data atau dikenal dengan siklus pengolahan data (siklus informasi).

Kualitas informasi tergantung pada empat hal yaitu akurat, tepat waktu, relevan dan ekonomis. Informasi harus bebas dari kesalahan-kesalahan dan tidak menyesatkan bagi pengguna yang menerima dan memanfaatkan informasi tersebut. Akurat juga berarti informasi harus jelas mencerminkan maksudnya. Dalam prakteknya, mungkin dalam penyampaian suatu informasi banyak terjadi gangguan (noise) yang dapat merubah atau merusak isi dari informasi tersebut. Informasi dikatakan akurat jika mengandung komponen, yaitu sebagai berikut :

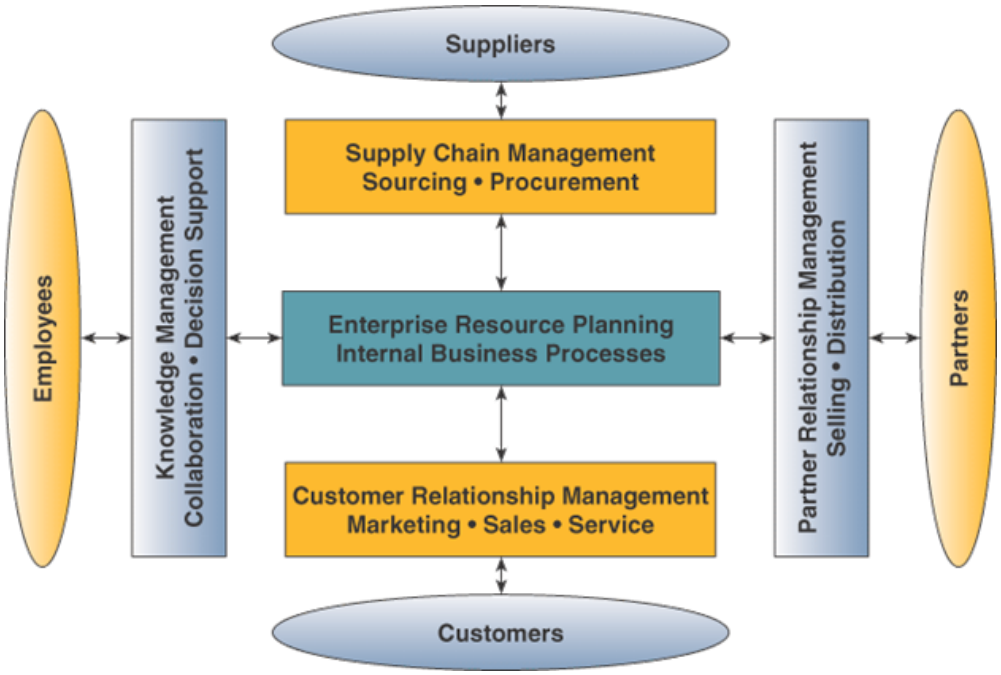
- *Completeness*, berarti informasi yang dihasilkan atau dibutuhkan harus memiliki kelengkapan yang baik, karena bila informasi tidak lengkap akan mempengaruhi dalam pengambilan keputusan.
- *Correctness*, berarti informasi yang dihasilkan atau dibutuhkan harus memiliki kebenaran.
- *Security*, berarti informasi yang dihasilkan atau dibutuhkan harus memiliki keamanan.

Informasi yang diterima harus tepat pada waktunya, informasi yang usang (terlambat) tidak mempunyai nilai yang baik bagi pengguna tertentu, sehingga bila digunakan sebagai dasar dalam pengambilan keputusan akan berakibat fatal. Saat ini mahalnya nilai informasi disebabkan harus cepatnya informasi tersebut didapat, sehingga diperlukan teknologi-teknologi mutakhir untuk mendapatkannya, mengolah dan mengirimkannya. Informasi harus mempunyai relevansi atau manfaat bagi si pengguna. Relevansi informasi untuk satu pengguna tertentu dengan yang lainnya berbeda. Informasi yang dihasilkan mempunyai manfaat yang lebih besar dibandingkan dengan biaya mendapatkannya. Sebagian besar informasi tidak dapat tepat ditaksir keuntungannya dengan satuan nilai uang tetapi dapat ditaksir nilai efektivitasnya.

Penggunaan internet dan jaringan serta teknologi informasi lainnya bagi perusahaan atau organisasi adalah suatu keniscayaan .untuk mendukung komunikasi dan kerjasama perusahaan, dan berbagai proses yang dijalankan baik di jaringan perusahaan ataupun dengan pelanggan dan mitra bisnis. Perusahaan mengembangkan aplikasi lintas fungsi perusahaan

terintegrasi yang melintasi batas fungsi tradisional bisnis agar dapat merekayasa ulang dan meningkatkan proses bisnis di semua lintas fungsi perusahaan. *Software-software* yang banyak dipakai adalah ERP, CRM dan SCM dari SAP, Peoplesoft atau Oracle. Software ini berfokus untuk mendukung proses bisnis terintegrasi yang terlibat dalam operasional bisnis.

Arsitektur aplikasi perusahaan menggambarkan hubungan antar aplikasi perusahaan lintas fungsi yang memberikan kerangka kerja konseptual untuk membayangkan berbagai komponen dasar proses dalam *interface* dari *e-business*. ERP (*Enterprise Resource Planning*) berfokus pada efisiensi produk internal perusahaan, distribusi dan proses keuangannya. CRM (*Customer Relationship Management*) berfokus pada proses dan mendapatkan dan mempertahankan pelanggan yang berharga meliputi pemasaran, penjualan dan layanan. PRM (*Partner Relationship Management)* bertujuan mendapatkan dan memelihara para minatra untuk meningkatkan penjualan dan ditribusi produk. SCM (*Supply Chain Management*) fokus pada pengembangan *resources* dan proses mendapatkan yang efisien dan efekif. *Knowledge Management* berfokus pada alat untuk mendukuing kerjsa sama kelompok dan pengambilan keputusan.



Gambar 1. *Enterprise Application Architecture*

Tulang punggung lintas fungsi perusahaan. Integrasi dan otomatisasi fungsi produksi, logistik, distribusi, keungan dan SDM. ERP menyajikan data real time integrasi atas proses bisnis yagn disatukan dari ERP dan DBMS. Hal ini sangat bermanfaat terutama untuk kualitas dan efisiensi, penurunan biaya, pendukung keputusan, kelincahan perusahaan. Tentunya implementasi ERP besar-besaran ini bukan tanpa resiko. Berbagai penyebab kegagalannya adalah meremehkan kerumitan perencanaan, pengembangan dan pelatihan yang dibutuhkan untuk mempersiapkan sistem baru yang radikal, cara yang terlalu cepat dalam proses konversi, belum adanya pengujian yang cukup atas data.

CRM bertujuan memberikan data seorang pelanggan secara lengkap terhadap organisasi yang dan karyawan yang berhadapan langsung dengan pelanggan, memberikan pelanggan tentang pandangan lengkap tentang perusahaan. CRM termasuk Teknologi Informasi sistem lintas fungsi yang mengintegrasi dan mengotomatisasi proses-proses layanan pelanggan dalam penjualan, pemasaran dan layananan pelanggan (*Customer Satisfaction*). CRM juga mengintegrasikan proses ini dengan database operasi bisnis lainnya melalui web. CRM bermanfaat untuk mengidentifikasi pelanggan terbaik, personalisasi dan penyesuaian secara realtime terhadap siklus keinginan dan kebutuhan pelanggan penelusuran kontak, menyediakan layanan superior disetiap titik kontak pelanggan. Kegagalan CRM biasanya disebabkan karena 50% perusahaan merasa CRM tidak memberi hasil yang menjanjikan. 20% perusahaan yang disurvei malah mengatakan CRM merusak hubungan dengan pelanggan lama. Hasil dari penelitian CRM alasannya adalah kurangnya pemahaman dan persiapan.

SCM membantu mengelola rantai pasokan dengan efisien. Membantu mendapatkan produk pada tempat yang tepat, waktu yang tepat dan jumlah yang tepat. SCM memperkirakan permintaan, mengendalikan persediaan dan meningkatkan jaringan hubungan antara perusahaan dengan pelangggan, pemasok, distributor dan mitra perusahaan. SCM ini merupakan sistem lintas fungsi yang menggunakan TI yang bertujuan menciptakan jaringan yang cepat, efisien, berbiaya rendah dan membuat produk perusahaan beranjak dari konsep menuju pasar. Manfaat SCM adalah pemrosesan yang lebih cepat dan akurat, mengurangi inventori, lebih cepat ke pasaran, mengurangi biaya transaksi dan material, hubungan strategis dengan supplier.

Pemakaian teknologi komputer sebagai salah satu aplikasi dari teknologi informasi sudah menjadi suatu kebutuhan, karena banyak pekerjaan yang dapat diselesaikan dengan cepat, akurat, dan efisien. Dengan berkembangnya teknik telekomunikasi dan sistem pengolahan data yang berkaitan erat dengan komunikasi antar pengguna komputer yang satu dengan komputer yang lain yang berfungsi untuk menyalurkan data sehingga masalah keamanan merupakan salah satu aspek penting dari suatu sistem informasi. Kerawanan yang paling berbahaya pada perusahaan besar yang memiliki jaringan luas adalah pada aplikasinya. Sistem keamanaan telah banyak terfokus pada antivirus dan keamanan jaringan, tapi bagian yang amat merisaukan adalah transaksi bisnis yang memiliki data yang sangat berharga (*valuable*). Sistem keamanan pada Aplikasi merupakan tren masa depan yang dapat dikatakan sebagai era baru setelah era anti Virus dan era keamanan jaringan. Bisa dikatakan bahwa SSL (*Secure Socket Layer*) dan data enkripsi saja tidak cukup dikarenakan hal tersebut hanya melindungi infomasi selama transmisi tetapi data ini tetap bisa digunakan oleh sistem yang harus diubah ke media yang bisa dibaca. Keganjilannya juga data tidak disimpan pada format terenkripsi dan yang lebih ganjil lagi adalah data dapat dengan mudah diakses dari beberapa aplikasi tanpa adanya sistem keamanan yang memadai. Selain itu juga penggunaan firewall tidak cukup untuk mengamankan data dan aplikasi dikarenakan Port tertentu (80 dan 443) bisa terlewati dari firewall .

Sistem keamanan data dan kerahasiaan data merupakan salah satu aspek penting dalam perkembangan dunia telekomunikasi, khususnya komunikasi yang menggunakan

komputer dan terhubung ke jaringan. Beberapa teknik pengamanan data adalah *Internet Firewall*: berfungsi untuk mencegah akses dari pihak luar ke sistem internal. *Firewall* bekerja dengan 2 cara, yaitu dengan menggunakan *Filter* dan *Proxy*. Filter digunakan untuk menyaring komunikasi agar terjadi seperlunya saja. *Proxy* berarti mengizinkan pemakai dari dalam untuk mengakses internet seluas-luasnya. Teknik pengamanan berikutnya adalah Kriptografi: adalah seni menyandikan data, ada 2 proses yaitu: Enkripsi dan Dekripsi, Enkripsi adalah program mengubah data asli menjadi data sandi. Dekripsi adalah proses mengembalikan data sandi ke aslinya. Data hasil penyandian disebut *Chiper Teks*. Proses Enkripsi dilakukan sebelum data dikirim, sedangkan merubah menjadi data asli dilakukan setelah data dikirim.

Teknik pengamanan juga bisa menggunakan *Secure Socket Layer* (SSL): pengiriman data melalui transmisi yang disandikan atau pengiriman data dengan cara menyandikan data. Hal ini dilakukan agar komputer-komputer yang berada pada pengiriman dan penerimaan data tidak dapat membaca isi data. Kompetensi profesi IT adalah tentang memenuhi kebutuhan atau permintaan perusahaan baik lokal maupun global. Dalam memahami kebutuhan kompetensi tersebut maka perlu suatu formalisasi yang lebih baik dan tepat mengenai pekerjaan profesi yang berkaitan dengan keahlian dan fungsi dari tiap jabatannya. Kompetensi mencakup pengetahuan, keterampilan dan pengalaman yang diperlukan untuk melakukan pekerjaannya. Hal ini menimbulkan kebutuhan untuk dibentuknya suatu standar dengan sertifikasi IT. Visi dari standar kompetensi profesi TI di Jepang yaitu untuk mencapai keunggulan dalam bidang Teknologi Informasi melalui pengembangan profesional TI bersertifikat mengikuti standar dunia yang diakui dan mempercepat pembangunan ekonomi melalui penyebaran baik di dalam negeri maupun di luar negeri dengan pengetahuan yang sangat terlatih dan berkualitas.

1.2 Identifikasi Masalah

Dari uraian latar belakang di atas , dalam penulisan makalah ini dapat diidentifikasi permasalahannya yaitu :

a. Mengidentifikasi kebutuhan database dan data security (*Backward Analysis*)

b. Mengidentifikasi *Bussiness functions* : CRM, E-Commerce dan SCM

c. Mengidentifikasi kerawanan data pada transaksi bisnis

d. Mengidentifikasi metode pengamanan data

e. Mengidentifikasi isu kode etik nasional dan internasional

BAB II. TINJAUAN PUSTAKA

2.1 Pengertian Database

Database adalah kumpulan file-file yang saling berelasi. Relasi tersebut ditunjukkan dengan kunci dari tiap file yang ada. Satu database menunjukkan satu kumpulan data yang dipakai dalam satu lingkup perusahaan. Bila terdapat file yang tidak dapat dihubungkan dengan file yang lain berarti file itu bukan dalam satu kelompok database, ia akan dapat membentuk database sendiri.

Di dalam Wikipedia (2010) database, pangkalan data atau basis data adalah kumpulan informasi yang disimpan di dalam komputer secara sistematik sehingga dapat diperiksa menggunakan suatu program komputer untuk memperoleh informasi dari basis data tersebut.

Subhan (2007) mencontohkan beberapa pemakaian aplikasi database sehari-hari :

• Transaksi pembelian dari Mall/Supermarket
• Transaksi pembelian atas pemakaian kartu kredit
• Tempat penampungan data pesanan bagi agen travel
• Mengolah data asuransi
• Penggunaan Internet
• Pelajaran di Kampus

Adapun perangkat lunak yang digunakan untuk mengelola dan memanggil kueri (*query*) basis data disebut sistem manajemen basis data (*database management system*, DBMS). Dalam Kristanto (1994) disebutkan bahwa kumpulan file yang saling berkaitan bersama dengan program untuk pengelolaannya disebut DBMS. Database adalah kumpulan datanya, sedangkan program pengelolanya berdiri sendiri dalam paket program komersial untuk membaca data, mengisi data, menghapus, dan melaporkan data dalam database. Jadi, satu DBMS terdiri dari Database dan Set Program pengelola untuk menambah data, menghapus, mengambil, dan membaca data. DBMS merupakan software (dan hardware) yang khusus didesain untuk melindungi dan memanage database. Dengan menggunakan DBMS, maka kita dapat :

- Mendefinisikan data dan hubungannya.
- Mendokumentasikan struktur dan definisi data
- Menggambarkan, mengorganisasikan dan menyimpan data untuk akses yang selektif/dipilih dan efisien.
- Hubungan yang sesuai antara user dengan sumber daya data.
- Perlindungan terhadap sumber daya data akan terjamin, dapat diandalkan, konsisten dan benar.
- Memisahkan masalah *Logical* dan *physical* sehingga merubah implementasi database secara fisik tidak menghendaki user untuk merubah maksud data (*Logical*).

- Menentukan pembagian data kepada para user untuk mengakses secara *concurent* pada sumber daya data.

Istilah "basis data" berawal dari ilmu komputer. Meskipun kemudian artinya semakin luas, memasukkan hal-hal di luar bidang elektronika, artikel ini mengenai basis data komputer. Catatan yang mirip dengan basis data sebenarnya sudah ada sebelum revolusi industri yaitu dalam bentuk buku besar, kuitansi dan kumpulan data yang berhubungan dengan bisnis.

Konsep dasar dari basis data adalah kumpulan dari catatan-catatan, atau potongan dari pengetahuan. Sebuah basis data memiliki penjelasan terstruktur dari jenis fakta yang tersimpan di dalamnya: penjelasan ini disebut skema. Skema menggambarkan obyek yang diwakili suatu basis data, dan hubungan di antara obyek tersebut. Ada banyak cara untuk mengorganisasi skema, atau memodelkan struktur basis data: ini dikenal sebagai model basis data atau model data. Model yang umum digunakan sekarang adalah model relasional, yang menurut istilah layman mewakili semua informasi dalam bentuk tabel-tabel yang saling berhubungan dimana setiap tabel terdiri dari baris dan kolom (definisi yang sebenarnya menggunakan terminologi matematika). Dalam model ini, hubungan antar tabel diwakili dengan menggunakan nilai yang sama antar tabel. Model yang lain seperti model hierarkis dan model jaringan menggunakan cara yang lebih eksplisit untuk mewakili hubungan antar tabel.

Istilah *basis data* mengacu pada koleksi dari data-data yang saling berhubungan, dan perangkat lunaknya seharusnya mengacu sebagai *sistem manajemen basis data* (*database management system/DBMS*). Jika konteksnya sudah jelas, banyak administrator dan programer menggunakan istilah basis data untuk kedua arti tersebut.

2.2 Perangkat lunak basis data

Perangkat lunak basis data yang banyak digunakan dalam pemrograman dan merupakan perangkat basis data yang *high level* adalah :

- *Microsoft SQL Server*
- *Oracle*
- *Sybase*
- *Interbase*
- *XBase*
- *Firebird*
- *MySQL*
- *PostgreSQL*
- *Microsoft Access*
- *dBase III*
- *Paradox*
- *FoxPro*
- *Visual FoxPro*
- *Arago*
- *Force*
- *Recital*
- *dbFast*
- *dbXL*
- *Quicksilver*
- *Clipper*
- *FlagShip*
- *Harbour*
- *Visual dBase*
- *Lotus Smart Suite Approach*

Selain perangkat lunak di atas, terdapat juga perangkat lunak pemrograman basis data *low leve*l, diantaranya Btrieve dan Tsunami Record Manager.

Database dibutuhkan di suatu organisasi/ perusahaan untuk memenuhi kebutuhan para pemakai diseluruh jenjang perusahaan. Banyak perusahaan menggunakan database untuk mendukung operasional perusahaan, bahkan beberapa perusahaan sangat mengandalkan database sebagai kunci operasi perusahaan, sehingga beberapa perusahaan memiliki media penyimpanan database yang besar dan menyimpan jumlah data yang sangat banyak atau VLDB (*Very Large Database*). Beberapa perusahaan tersebut antara lain :

Basisdata terbesar berdasarkan ukuran rilis tahun 2005 kategori Data Warehouse								
No.	Perusahaan/Organisasi	Ukuran (GB)	DBMS	Platform	Arsitektur sistem	Vendor basisdata	Vendor sistem	Vendor penyimpanan data
1	Yahoo!	100.386	Oracle	UNIX	Centralized/SMP	Oracle	Fujitsu Siemens	EMC
2	AT&T	93.876	Daytona	UNIX	Federated/SMP	AT&T	HP	HP
3	KT IT-Group	49.397	DB2	UNIX	Centralized/Cluster	IBM	IBM	Hitachi
4	AT&T	26.713	Daytona	UNIX	Federated/SMP	AT&T	Sun	Sun
5	LGR - Cingular Wireless	25.203	Oracle	UNIX	Centralized/SMP	Oracle	HP	HP
6	Amazon.com	24.773	Oracle RAC	Linux	Centralized/Cluster	Oracle	HP	HP
7	tanpa nama	19.654	DB2	UNIX	Centralized/MPP	IBM	IBM	ECM
8	UPSS	19.467	SQL Server	Windows	Centralized/SMP	Microsoft	Unisys	EMC
9	Amazon.com	18.558	Oracle RAC	Linux	Centralized/Cluster	Oracle	HP	HP
10	Nielsen Media Research	17.685	Sybase IQ	UNIX	Centralized/SMP	Sybase	Sun	EMC

Dalam Anonim (2011), ada beberapa hal yang harus diperhatikan dalam operasi database yaitu :

1. *Entry dan update*

   Langkah pertama pengoperasian pada database adalah entry dan menyimpan data.

2. *Backup dan recovery*

Sekali database diimplementasikan, salah satu fungsi yang harus dipelihara adalah tersedianya data setiap saat untuk para user. Backup adalah pekerjaan menduplikasikan record-record database atau menyimpan perubahan-perubahan pada database. *Recovery* adalah proses untuk memperbaiki kembali database dari kerusakan yang dialaminya. kerusakan ini umumnya adalah kerusakan fisik pada penyimpanan sekunder.

3. *Reorganization*

Dalam sistem database pada suatu saat dapat diadakan pembersihan database terhadap record-record yang tidak digunakan secara aktif lagi. Hal ini dimaksudkan untuk mempercepat akses pada database yang terganggu dengan banyaknya record-record yang tidak / jarang digunakan itu, record-record yang tidak aktif tersebut dapat dipindahkan dan disimpan dalam suatu file. Proses pembersihan record-record tidak aktif itu dinamakan reorganization, metode *reorganization* ini tergantung dari model database yang dipilih.

4. *Restructuring*

Pada suatu lingkungan yang dinamis setelah suatu periode berjalan pasti dirasakan kebutuhan perubahan, contoh :

- Penambahan/penghapusan suatu data elemen, perubahan ukuran/size suatu data elemen, pertukaran data elemen antar file tersebut.
- Perubahan metode akses.
- Proses perubahan model internal dan sekaligus logikal.

5. *Monitoring, performance and tuning*

- Evaluasi secara periodik terhadap unjuk kerja sistem database, dapat pada ketepatan data atau kelambatan unjuk kerja.
- Kekurangan-kekurangan ini hendaknya diperbaiki dan dilaraskan/tuning.

6. *Security*

Sekurity data sangat penting dalam sistem database, artinya mengontrol pengaksesan data dalam database terhadap orang-orang yang tidak berwenang, sehingga mencegah :

- Penyingkapan rahasia.
- Perubahan data.
- Perusakan / penghapusan data.

2.3 Data Security

Di masa kini dimana penggunaan internet dan perangkat digital semakin beragam dan semakin terjangkau, kita mendapatkan banyak kemudahan, baik mendapatkan informasi maupun mengirimkan informasi. Namun dibalik kemudahan tersebut banyak terdapat

ancaman keamanan data. Menurut Laudon (2009) ancaman keamanan di lingkungan *e-commerce* adalah :

1. Program-program yang tidak diinginkan
2. *Malicious Code*
3. *Phising* dan pencurian identitas
4. *Hacking dan cybervandalisme*
5. Penipuan dan pencurian kartu kredit.
6. *Spoofing dan Spam*
7. *Denial of Service dan Distirbuted Denial of Services Attack*
8. *Sniffing*
9. Serangan dari dalam (*Insider Attacks*)
10. Server yang pembuatannya kurang bagus dan *client software*

Menurut Data Security Handbook (2008), ancaman keamanan data dapat dibagi menjadi 2 yaitu *Technical Threat* dan *Administrative and Physical Threat.* Yang termasuk technical threat adalah : serangan virus, *worm, trojan horses, botnets, blended threats, IP Spoofing atau data interception, spam, spyware, denial of service attacks.* Yang termasuk *Administrative and Physical Threat* adalah kurangnya pelatihan keamanan data, tidak ada password, kurangnya penerapan *security policy, social engineering*, rencana lamanya menyimpan data, sumberdaya manusia, dan external media. Selain itu menurut Tehan (2009) dalam bukunya *Data Security Breaches*, data sangat rawan untuk dicuri. Kasus pencurian data yang paling umum terjadi penipuan melalui *credit card*. Lalu yang paling serius adalah terancamnya akses dan kontrol terhadap data yang kita miliki karena ulah para hackers, dan orang-orang yang bertugas mengumpulkan informasi rahasia dengan dalih sebagai petugas perwakilan lembaga tertentu (*social engineers*).

Dalam Cisco (2001) beberapa metode pengamanan data yang umum adalah penerapan *password, enkripsi, firewalls, antivirus, intrusion detection system, security policy*, dan kontrol akses.

Sementara itu menurut Arianto (2011), metode pengamanan data yang bisa digunakan ada bermacam-macam, tergantung kebutuhan dan kondisi yang ada dan mengurangi resiko yang mungkin timbul. Beberapa tindakan pengamaan sistem data pada komputer diuraikan berikut ini :

1. *Administrative Security*

   Pengamanan data secara administratif (*administrative security)* perlu dilakukan untuk menjaga kemungkinan gangguan keamanan data yang datangnya dari "orang dalam" atau kerja sama orang dalam dengan orang luar. Aturan-aturan, kebijakan, pelatihan, dan disiplin yang berkaitan dengan pengamanan sistem komputer perlu diadakan. Aturan yang menetapkan hak-akses serta sanksi pelanggaran kemanan sistem harus dibuat bersama dan ditaati bersama. Kebijakan tentang akses file dalam organisasi, akses informasi ke luar (internet), serta bagaimana menerima data/informasi dari luar

perlu ditetapkan. Pelatihan staff tentang tatacara dan aturan perlindungan sistem komputer harus selalu diadakan secara reguler.

2. *Network Security*

Setiap sistem jaringan memiliki kelemahan-nya masing-masing sehingga perlu segera diteliti dan dicarikan cara untuk menutupi lubang-lubang kemanan-nya (*security holes*). Kelemahan bisa muncul dari sistem operasi jaringan yang digunakan, sehingga kerap sekali para pencipta perangkat lunak sistem operasi melakukan perbaikan-perbaikan (*operating system pacth*) atau pemugaran (*update, new release*) terhadap produk-nya. Setiap proses instalasi software baru dari pengguna jaringan harus di-dokumen-tasikan, demikian pula setiap operasi dan akses perlu dicatat (logbook), sehingga bila timbul hal hal yang tidak di-inginkan, administrator jaringan bisa melakukan pelacakan. Setiap asset baik data, perangkat lunak (*software*), maupun perangkat keras (*hardware)* perlu diberi perlindungan berlapis. Perangkat keras diperlengkapi dengan berbagai pengamanan seperti kunci, gembok, dan bila perlu pengamanan satpam pada gedung dan ruangan. Perangkat lunak diberi pengaman kunci userID, password, kunci akses (*access-key*) dan sebagainya. Akses dari luar jaringan maupun akses dari dalam ke luar harus melalui satu pintu (*proxy server*) yang diberi pengamanan (*firewall*), sehingga dapat mengurangi serangan keamanan

3. *Anti Virus*

Virus baru terus bermunculan sehingga sistem komputer harus selalu mendapat proteksi yang cukup agar dapat terhindar dari kejadian yang tidak diharapkan. Harap dimaklumi bahwa infeksi virus berjalan tanpa permisi dan tanpa sepengetahuan pemilik sistem komputer, disamping itu jenisnya sangat beragam. Serangan virus pertama yang populer adalah virus Morris yang menyerang sistem jaringan Departemen Pertahanan Amerika Serikat pada tahun 1988 serta berbagai instalasi jaringan perguruan tinggi, kerugian finansial mencapai $98 juta. Sejak itu program anti virus pun mulai digalakkan untuk meminimalkan akibatnya.

Virus dapat dikategorikan dalam berbagai jenis, antara lain sebagai berikut:

- Virus berupa "*file infector*" yaitu virus yang mengikut pada file-file program seperti file-file bertipe: .COM, dan .EXE. Ketika program ini dijalankan maka virus menyebar. Virus ini dapat merusak file file yang dibutuhkan file program, seperti .SYS, .OVL, .PRG, .MNU dan file-file sistem lainnya.
- Virus "*boot-record*" yaitu virus yang bersembunyi di sektor dimana boot-record direkam, ketika komputer di-boot maka virus menyebar. Salah satu cara virus ini menyebar adalah melalui disket yang memiliki boot-record, ketika dipakai untuk mem-boot sistem maka virusnya masuk ke *boot-sector* dari hard-disk, dan selanjutnya merusak sistem operasi.

- Virus "*macro*" yaitu virus yang merupakan "*scrip*t" program yang ikut pada file apa saja seperti file Word, file Exel, file e-mail, dan sebagainya, dan menyebar ketika file ini diakses, dibaca, atau di-copy.

Beberapa kelompok virus adalah sebagai berikut:

- Boot sector
- Macro
- Worms
- Companion
- Link
- Multipartite
- Partition sector
- Polymorphic
- Trojan horses
- Memory resident (TSR)
- Parasitic
- IRC Worms

Beberapa situs informasi virus adalah sebagai berikut:

- *Data Fellow Virus Information Center : www.datafellows.com/vir-info/*
- *International Computer Security Association : www.icsa.net/*
- *IBM Antivirus Online : www.av.ibm.com/*
- *Symantec AntiVirus Research Center : www.symantec.com/avcenter/*
- *Network Associates Virus Alerts: www.nai.com/asp_set/anti_virus/alerts/intro.asp*
- *Virus Bulletin : www.virusbtn.com/*
- *CERT at Carnegie-Mellon University: www.cert.org/*
- *CIAC (Computer Incident Advisory Capability) : www.ciac.org/*

Anti virus diciptakan untuk mencegah meluasnya infeksi virus dan untuk memperbaiki file-file yang telah ter-infeksi. Berbagai perusahaan software menciptakan anti virus, diantaranya yang populer adalah:

- *Norton Anti Virus*
- *McAfee VirusScan*
- *CA Innoculan*
- *Personal Anti Virus*
- *Trend-Micro Pccillin*

Satu hal yang perlu diperhatikan: anti virus dibuat hanya untuk mendeteksi dan mencegah jenis atau kategori virus yang pernah ada, dan tidak bisa mendeteksi jenis atau kategori virus baru. Anti virus harus selalu di-update secara reguler agar bisa mendeteksi virus-virus baru.

4. Firewall

Firewall berarti dinding api, biasanya dibuat pada bangunan besar untuk mencegah menjalarnya api dari satu bagian gedung ke bagian lainnya. Firewall pada jaringan komputer adalah perangkat lunak yang dipasang pada komputer server sehingga

dapat melindungi jaringan dari serangan yang datangnya dari luar. *Firewall* dirancang untuk:

- Mengatur dan mengawasi lalulintas data dari luar ke dalam jaringan dan juga sebaliknya, semua aliran data harus melewati firewall, yang tidak melalui firewall harus dicegah.
- Menetapkan kebijakan keamanan jaringan sehingga yang bisa lewat hanya yang mempunyai hak.
- Mencegah penyusupan dari luar agar tidak bisa mengganggu jaringan

Ada tiga macam *firewall,* yaitu: *packet filtering router, circuit level gateway, dan application level gateway*. *Packet filtering router* memeriksa semua lalulintas data melalui suatu aturan yang diterapkan pada router jaringan, semua paket data yang tidak memenuhi aturan akan di-blok tidak boleh lewat. Hal-hal yang diperiksa antara lain alamat IP sumber maupun alamat IP yang dituju, nomer port yang digunakan, dan sebagainya.

Circuit level gateway menetapkan koneksi antara komputer didalam jaringan dengan komputer dari luar jaringan apabila telah memenuhi aturan, tidak diperbolehkan adanya koneksi *end-to-end (peer-to-peer)* tanpa melalui *gateway*.

Application level gateway merupakan kontrol akses yang dilakukan oleh administrator jaringan pada tingkat aplikasi, tingkatan pengamanan-nya biasanya lebih ketat dibanding *packet-filtering router* karena bisa di-set-up sesuai kehendak administrator.

5. *Proxy Server*

Proxy server pada dasarnya berfungsi seperti *firewall* jenis *application level gateway,* suatu server yang berada antara server jaringan dan internet. *Proxy server* melaksanakan beberapa proses aplikasi yang telah ditetapkan lebih dulu, misalnya melayani akses dari terminal ke suatu situs web, atau berfungsi sebagai "*transfer agent*" terhadap berbagai aplikasi yang memiliki akses keluar atau akses dari luar ke dalam jaringan. *Proxy server* bisa meningkatkan kerja jaringan antara lain dengan menyimpan aplikasi atau data yang sering diakses oleh user, misalkan suatu situs web sangat populer (misalnya yahoo.com atau goggle.com) maka ketika user pertama melakukan akses ke situs tersebut, maka situs itu disimpan sehingga user kedua dan seterusnya merasa lebih cepat ketika meng-akses-nya karena tidak menunggu dari server asli tetapi dari proxy server saja. *Proxy server* juga bisa bisa juga berfungsi seperti "*filte*r" dengan memberi aturan untuk tidak meng-akses situs-situs tertentu, misalnya akses ke situs pornografi dapat diproteksi, sehingga user tidak dapat mengunjungi situs-situs tersebut.

6. Enkripsi-Dekripsi

Data yang dikirim melalui jaringan tidak jarang disadap oleh orang lain untuk kepentingan tertentu, sehingga timbul usaha untuk melakukan pengkodean terhadap data

sebelum dikirim melalui jaringan agar tidak bisa dibaca oleh penyadap. Pengubahan data asli menjadi kode rahasia disebut proses data encryption atau enkripsi data. Setelah data rahasia sampai ke tujuan maka data ini dikembalikan ke bentuk aslinya, proses ini disebut data decryption. Ilmu matematik yang mendasari teknik enkripsi dan dekripsi disebut kriptologi sedangkan teknik dan sains dari proses enkripsi-dekripsi disebut kriptografi. Naskah asli disebut sebagai plaintext dan naskah rahasia (yang telah di-enkrip) disebut ciphertext. Secara garis besar ada dua kategori kriptografi, yaitu: teknik simetris dan teknik asimetris. Teknik simetris berarti kunci/kode untuk melakukan enkripsi sama dengan kunci/kode untuk melakukan dekripsi. Teknik asimetri disebut juga sebagai teknik kunci publik, menggunakan kunci yang berbeda antara enkripsi dan dekripsi.

Beberapa algoritma kunci simetri antara lain adalah:

- *Substitution Cipher*
- *Transposition Cipher*
- *Data Encryption Standard (DES)*
- *Triple DES*
- *Rivest Code 2 (RC2)*
- *Rivest Code 4 (RC4)*

Substitution Cipher pada prinsipnya adalah penggantian huruf-huruf abjad dengan huruf lain, misalnya salah satu jenis substitution cipher yang paling tua adalah Caesar cipher, dimana abjad diganti abjad yang digeser kedepan beberapa posisi, misalnya untuk kunci geser = 3 maka daftar subsitusi-nya sebagai berikut.

Abjad asli : A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
Abjad kode: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C
Plaintext : Saya kirim uang satu juta
Ciphertext : Vdbd nlulp xdqj vdwx mxwd

Rahasianya ada pada kunci geser=3, bila penerima diberitahu maka ciphertext dengan mudah dapat di-dekripsi. Transposition cipher tidak melakukan penggantian (subsitusi) abjad, tetapi mengubah posisi pembacaan huruf dalam plaintext berdasarkan suatu kunci angka atau kunci kata (keyword). Misalkan kunci kata yang digunakan adalah MANDI, maka dibuat 5 kolom sesuai dengan jumlah kolom dalam kunci, kemudian plainteks dimasukan baris per baris menempati kolom tersebut, cipehr dibaca perkolom sesuai urutan abjad kunci.

Contoh Ciphertext : arnuz amsuz kuatz siata yigyz

DES (*Data Encryption Standard*) adalah teknik enkripsi yang telah menjadi standard pemerintah Amerika Serikat pada tahun 1977. Algoritma DES dimasukkan dalam kategori cipher modern yang menggunakan algoritma rumit dengan kunci sepanjang 56 bit (8 byte). Plaintext dibagi kedalam beberapa blok (blockcipher), masing-masing 64 bit, yang kemudian setiap blok dibagi dua menjadi 32 bit blok kiri dan 32 bit blok kanan. Setiap sub-blok dipermutasi dan diberi kunci, dan proses ini dilakukan dalam 16 putaran. Algoritma DES mula-mula diciptakan oleh IBM pada tahun 1970 dengan nama Lucifer.

Triple DES adalah pengembangan dari DES dengan melakukan proses DES tiga kali dengan tiga kunci berbeda, dengan demikian tingkat kesulitan dalam menebak ciphertext menjadi semakin tinggi. Rivest Code 2 (RC2) dan Rivest Code 4 (RC4) adalah teknik enkripsi yang disebut sebagai stream-cipher, dimana pada setiap byte data dilakukan manipulasi bit. Teknik enkripsi RC ditemukan oleh Ronald Rivest yang kemudian menjadi salah satu pendiri dari perusahaan keamanan data RSA. Beberapa teknik enkripsi kunci publik yang populer adalah:

- *Diffie-Hellman*
- *RSA*
- *Rabin*
- *ElGamal*

Semua algoritma kunci publik (asimetri) menggunakan fungsi matematis untuk mengubah plaintext menjadi ciphertext. Diffie-Hellman menggunakan aritmetik modulus dimana dua kunci berbeda akan memberi hasil yang sama berdasarkan nilai modulus-nya. RSA adalah singkatan dari Rivest, Shamir, dan Adleman, tiga orang yang bekerja sama membangun suatu algoritma kunci publik. RSA merupakan algoritma kunci publik yang terkuat, dan seperti Diffie-Hellman, RSA juga menggunakan aritmetik modulus dalam komputasi enkripsi-dekripsi. Rabin adalah teknik yang merupakan salah satu variasi dari RSA, ditemukan oleh M.Rabin. ElGamal merupakan variasi dari Diffie-Hellman, ditemukan ElGamal. Salah satu aplikasi dari algoritma kunci publik adalah software PGP (Pretty Good Privacy). PGP digunakan untuk pengamanan berkomunikasi lewat e-mail, dimana e-mai di-enkripsi pada saat dikirim sehingga hanya orang yang memiliki kunci private yang bisa membaca e-mail tersebut.

7. Autentikasi

Authentikasi adalah salah satu bentuk identifikasi untuk meyakinkan bahwa orang yang sedang berkomunikasi dengan kita adalah benar adanya, bukan pemalsuan identitas. Salah satu bentuk autentikasi yang paling sering dijumpai adalah: UserID disertai dengan Password, bahwa UserID adalah pernyataan tentang siapa yang sedang akses sistem atau sedang berkomunikasi, dan Password membuktikan bahwa orang tersebut benar adanya. Hanya saja sistem UserID dan Password ini ada kelemahannya, karena ada saja cara untuk mencari tahu password seseorang sehingga bisa terjadi pemalsuan identitas. Salah

satu sistem untuk mengurangi effek pemalsuan identitas atau pencurian password adalah dengan menerapkan OTP (One Time Password), dimana satu password hanya digunakan untuk satu kali akses, akses berikutnya harus menggunakan password yang berbeda. Sistem lain yang mengamankan autentikasi adalah Passport dan Kerberos. Selain menggunakan UserID dan Password, teknik autentikasi bisa diperluas dengan kombinasi biometric, misalnya UserID ditambah dengan sidikjari, atau UserID ditambah dengan mata-retina, dan sebagainya. Pasport adalah sistem yang memperluas autentikasi dengan menambahkan nomer-account yang disebut passport untuk memasuki suatu jaringan atau mendapat pelayanan online. Sebagai contoh Microsoft menggunakan passport untuk melayani para pengunjung setia situsnya. Kerberos adalah software yang menyediakan sistem autentikasi bagi para pengguna suatu jaringan. Kerberos menggunakan algoritma kriptografi untuk menyulitkan pada penyusup ketika mencuri password.

2.4 Isu Umum tentang Keamanan Data dan Informasi

Menurut Kurniawan dkk (2009) secara umum, ada empat aspek utama yang harus diperhitungkan dalam keamanan data dan informasi, yaitu :

1. *Privacy/Confidentiality* yaitu usaha menjaga data informasi dari orang yang tidak berhak mengakses (memastikan bahwa data atau informasi pribadi kita tetap pribadi).

2. I*ntegrity* 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.

Keempat aspek ini menjadi dasar untuk melakukan pengamanan terhadap data dan informasi. Keamanan data adalah sebuah proses, yang harus dijalankan untuk mengamankan sistem dan dalam penerapannya harus dilakukan dengan menyeluruh. Sementara itu, jika dipandang dari segi organisasi maka keamanan data harus dipandang sebagai berikut agar setiap tingkatan organisasi memiliki pandangan yang sama yang pada akhirnya meningkatkan efektifitas pengamanan organisasi :

1. Keamanan informasi harus sejalan dengan misi organisasi
2. Keamanan informasi merupakan bagian integral dari praktik manajemen yang baik
3. Keamanan informasi harus efektif dalam hal harga
4. Tanggung jawab dan kewenangan keamanan informasi harus dijelaskan secara eksplisit
5. Pemilik sistem memiliki tanggung jawab keamanan diluar organisasinya

6. Keamanan informasi memerlukan pendekatan yang komprehensif dan terintegrasi
7. Keamanan informasi harus dievaluasi ulang secara periodik
8. Keamanan informasi dibatasi oleh faktor sosial.

Kurniawan dkk (2009) juga menjelaskan keamanan data dan informasi telah memiliki standar pengamanan yang tertuang di dalam beberapa Standar Internasional Keamanan Informasi, yaitu :

- ISO/IEC 27001 – Panduan sertifikasi untuk sistem manajemen keamanan informasi sebuah organisasi
- ISO/IEC 27002 – Penamaan ulang dari standar ISO 17799 yang berisi panduan dan dan prinsip dasar untuk melakukan inisiasi, implementasi, serta pengelolaan sebuah sistem manajemen keamanan informasi (ISMS)
- ISO/IEC 27006 – berisi panduan untuk sebuah organisasi untuk mengikuti proses sertifikasi keamanan informasi

BAB III. PEMBAHASAN

Berdasarkan tinjauan pustaka yang telah dibahas pada BAB sebelumnya, maka pada tugas makalah kali ini, kami bermaksud membahas mengenai data base system dan security data system yang diterapkan oleh www.agoda.com. Dalam 1 dekade terakhir, sejalan dengan berkembangnya teknologi berbasis internet, bentuk bisnis baru yang disebut *E-Commerce* menjadi semakin banyak peminatnya. Banyak pihak kini melirik *e-commerce* sebagai cara baru berbisnis yang lebih efektif dan efisien. Tentu dengan alasan secara sekilas berbisnis melalui *e-commerce* memiliki beberapa karakteristik yang berbeda dengan berbisnis cara biasa.

Sekilas berbisnis secara e-commerce memiliki prospek yang menarik, seperti misalnya berkesan canggih dan professional, transfer informasi lebih cepat, akses yang luas dan lebih mudah menginternasional, tidak memerlukan ruang atau lokasi khusus untuk menjalankannya, dan di saat transportasi menjadi kian penting dan kian mahal e-commerce tidak perlu membuat kita memikirkan transportasi sebagai salah satu fitur pelayanan yang harus disediakan. Sebenarnya apakah e-commerce merupakan cara berbisnis yang menguntungkan ? Aspek apakah yang dilihat di dalam *e-commerce* ? Apakah faktor-faktor yang menyebabkan suatu bisnis *e-commerce* dapat berjalan dengan sukses ? Dan bagaimana mekanisme bisnis *e-commerce* tersebut ? Pertanyaan-pertanyaan itu kami coba diskusikan dengan mengambil contoh Agoda, sebuah contoh bisnis *e-commerce* yang melayani pemesanan hotel bertarif terjangkau secara on-line. Agoda merupakan sebuah perusahaan jasa pelayanan pemesanan akomodasi secara online.

3.1. Profil Agoda

Agoda (**www.agoda.com**) merupakan layanan pemesanan hotel online yang cukup terkemuka di Asia Pasifik, yang berfokus pada mendapatkan dan menyediakan tarif hotel terendah yang tersedia di setiap tujuan di seluruh dunia. Agoda merupakan bagian dari grup Priceline.com yang ter-listing di Nasdaq (bursa saham di Amerika). Priceline.com sendiri juga merupakan perusahaan jasa travel online di Amerika dimana pelanggannya dapat memesan jasa penyewaan mobil, tiket kapal pesiar, tiket pesawat, maupun pemesanan kamar hotel dengan harga murah. Cakupan bisnis Agoda sementara ini masih di wilayah Asia-Pasifik dengan fokus layanan pemesanan hotel di lebih dari 139.000 hotel di seluruh dunia, 10.000 hotel diantaranya dapat dibooking secara cepat.

Agoda juga memiliki ratusan staf beroperasi di seluruh dunia dan layanan pelanggan multi-bahasa 24 jam. Untuk menarik mempertahankan kesetiaan pelanggannya, Agoda mempunyai program Agoda Reward Points. Program yang diluncurkan pada tahun 2004 ini memberikan poin kepada pelanggan secara otomatis sejak pemesanan pertama mereka. Poin

ini dapat digunakan di ribuan situs hotel yang memberikan kebebasan pelanggan untuk memilih hotel manapun yang mereka suka di tanggal-tanggal di mana penawaran khusus atau harga promo tidak berlaku (*tanggal blackout*).

Agoda juga bernegosiasi secara pribadi dan langsung dengan berbagai hotel untuk memastikan harga yang terendah, dan kemudian mengirimkan penawarannya kepada para pelanggan. Ribuan situs web dan mitra perjalanan memilih Agoda untuk menyediakan pemesanan hotel karena merasa dapat diandalkan, dijangkau dan terkoneksi. Sebagai penghargaan atas hal ini, Agoda telah mendapat penghargaan ***Situs Web Akomodasi Terbaik di Asia*** untuk tahun 2008 pada Penghargaan Web TravelMole untuk Asia yang pertama. Dari profile tersebut kita dapat membahas mengenai bagaimana cara Agoda mengidentifikasi kebutuhan data khususnya dari sisi E-commerce, selain itu juga pada makalah kali ini kita akan mengidentifikasi kerawanan data pada transaksi pemesanan Hotel melalui Pay Pal di www.agoda.com, serta mengidentifikasi metode pengamanan data untuk menghindari terjadinya kerusakan pada web. Selain itu juga kami coba mengangkat mengenai Isu kode etik nasional dan internasional yang berkaitan dengan internet.

3.2. Mengidentifikasi Kerawanan Data Pada PayPal

Akses yang paling mudah dan cepat pada bisnis elektronik c*ommerce* ini adalah melalui Pay pal. Di bawah ini akan dibahas secara singkat, mengenai faktor-faktor apa saja yang menjadi kunci sukses *E-commerce* pada Agoda, yaitu antara lain :

1. *Selection and Value*
2. *Performance and Service*
3. *Look and Feel*
4. *Advertising and incentives*
5. *Personal attention*
6. *Community relationship*
7. *Security and reliability*

Bila ditilik Agoda yang kini di 5 besar bisnis pelayanan akomodasi online tidak lepas dari komitmen Agoda untuk memenuhi faktor-faktor kesuksesan sebuah bisnis *e-commerce*, yaitu:

1. *Selection and Value*
   Agoda memilih hanya hotel berkelas internasional namun memiliki nilai strategis bagi para pengunjung wisatawan maupun pebisnis yang membutuhkan akomodasi. Misalnya Agoda bekerjasama dengan hotel yang berada di kota dan daerah pusat wisata dan bisnis.
2. *Performance and Service*
   Agoda menyediakan pelayanan pemesanan hotel instan dengan pilihan sebanyak 10.000 hotel di seluruh dunia bagi para pelanggan yang tidak memiliki banyak waktu untuk memesan hotel.

3. *Look and Feel*
   Website yang didesain interaktif dan berkesan professional menyebabkan para pelanggan akan melihat Agoda sebagai website yang dapat diandalkan dan memberikan kemudahan. Hal ini juga didukung oleh pelayanan call support yang akan mendukung informasi yang didapat di internet dengan kebutuhan riil pelanggan. Terkadang pelanggan yang baru akan merasa ragu-ragu dengan kehandalan pelayanan di internet sehingga merasa perlu untuk berkomunikasi secara langsung dengan pihak penyedia layanan. Di dalam hal ini Agoda memahami psikologis tersebut dengan menyediakan layanan call support yang akomodatif.

4. *Advertising and incentives*
   Agoda menyediakan insentif bagi para pelanggannya melalui mekanisme membership yang melakukan pemesanan akan mendapatkan poin yang dapat digunakan untuk menginap di salah satu hotel member agoda apabila poinnya sudah mencukupi tanpa harus membayar lagi. Bagi para hotel yang menggunakan jasa layanan agoda melalui advertising di agoda juga mendapatkan manfaat dengan image yang baik, hotel yang terpercaya dan nyaman.

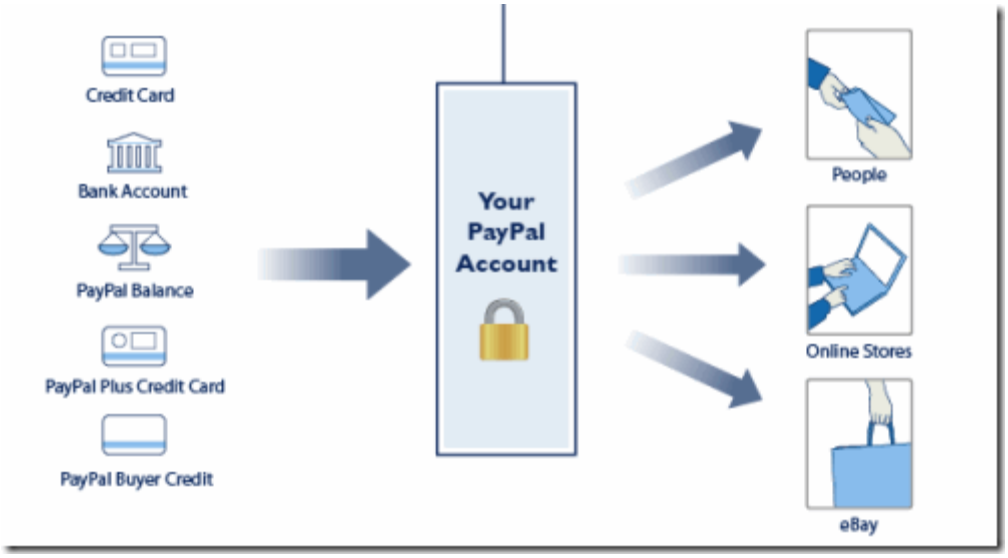
5. *Personal attention*
   Adanya customer call support 24 jam yang akomodatif.

6. *Community relationship*
   Nampaknya community relationship yang dimaintain oleh Agoda adalah member dari agoda dan para pelanggan agoda. Agoda mencoba meningkatkan retensi penggunaan pelayanan agoda dengan system imbalan dan penerapan rating hotel terhadap hotel-hotel yang berkerjasama dengan agoda.

7. *Security and reliability*
   Dalam hal pembayaran, agoda telah menerapkan system pembayaran melalui account PayPal yang lebih aman bagi kedua belah pihak (pembeli dan penjual) dibandingkan langsung dengan kartu kredit.

3.2.1. Pengertian PayPal

PayPal adalah salah satu alat pembayaran (*Payment procesors*) menggunakan internet yang terbanyak digunakan didunia dan teraman saat ini. Pengguna internet dapat membeli barang di situs e-commerce, lisensi software original, keanggotaan situs, urusan bisnis, mengirim dan menerima donasi atau sumbangan, mengirim uang ke pengguna PayPal lain di seluruh dunia dan banyak fungsi lainnya dengan mudah dan otomatis menggunakan internet. PayPal mengatasi kekurangan dalam pengiriman uang tradisional seperti Cek atau Money order yang prosesnya lambat.



Gambar 3.1 Skema Transaksi Paypal

Pada gambar 3.1 menjelaskan mengenai skema transaksi pada Paypal. Skema transaksi Paypal menggambarkan proses transakasi antara proses menggunakan Paypal sebagai alat pembayaran, akun Paypal dan media penggunaan Paypal. Proses menggunakan Paypal dapat melalui beberapa cara, yaitu :

- Credit Card
- Bank Account
- Paypal Balance
- Paypal Plus Credit Card
- Paypal Buyer Credit

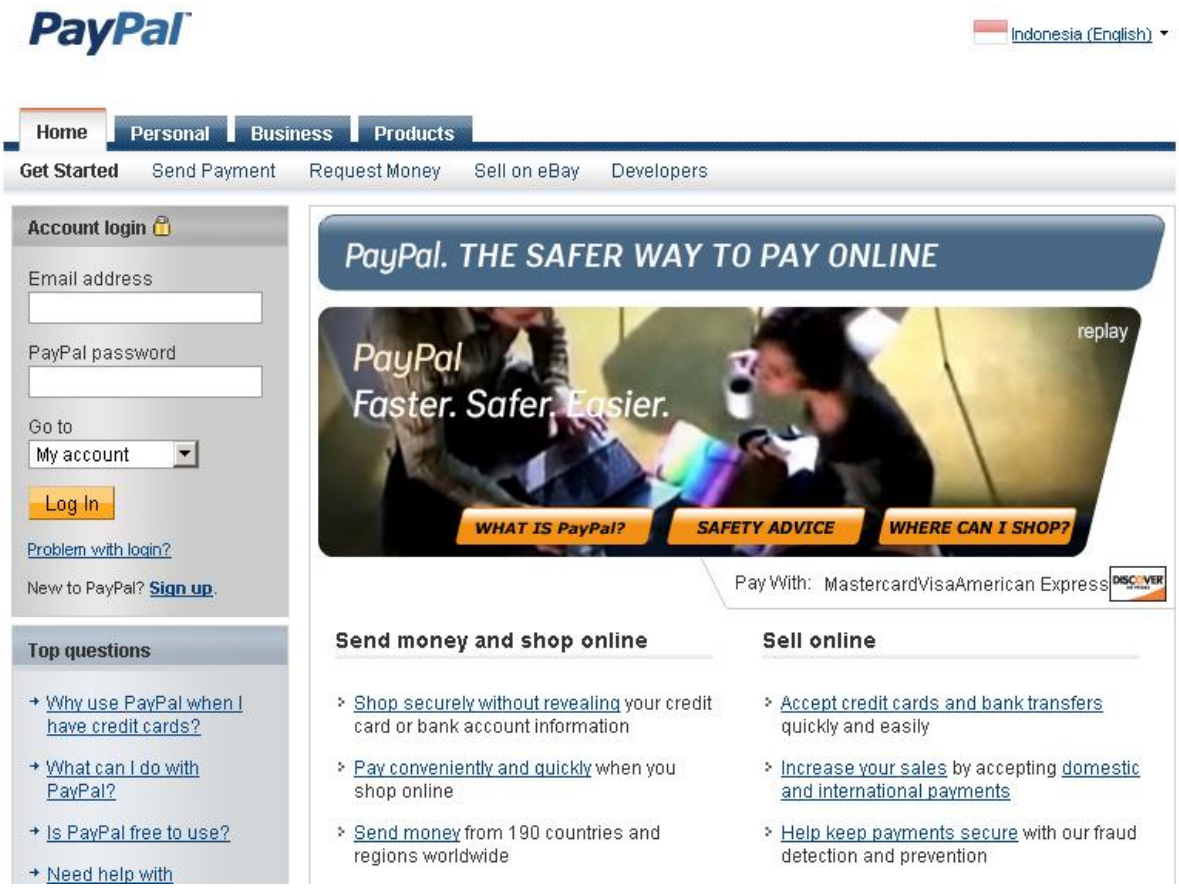
Kelima fasilitas tersebut dapat digunakan sebagai media untuk melakukan pembayaran kepada Paypal. Selanjutnya kita akan mempunyai akun pada Paypal yang dapat digunakan pada semua transaksi yang bermitra dengan Paypal. Dalam skema diatas akun menggambarkan bahwa Akun Paypal dapat digunakan kepada *people, online stores* dan *ebay.*

3.2.2. Sejarah PayPal

Perusahaan Paypal (Paypal corp.) seperti yang dikenal sekarang adalah penggabungan antara perusahaan Confinity dan X.com pada tahun 2000. Confinity didirikan pada desember 1998 oleh Peter Thiel dan Max Levchin, awalnya sebagai alat pembayaran Palm Pilot dan sebagai perusahaan kriptograpi (ilmu pembacaan sandi,

tulisan-tulisan atau angka-angka rahasia). Sedangkan X.com didirikan oleh Elon Musk pada maret 1999, yaitu perusahaan penyedia jasa perencanaan keuangan.

Kedua perusahaan lokasi pertamanya adalah kantor di 165 University Avenue di Palo Alto, California, rumah dari beberapa pemula di Silicon Valley. Ebay melihat perkembangan penggunaan Paypal dan menyimpulkan Paypal cocok sebagai salah satu alat pembayaran di ebay. Pada mei 1999 ebay membeli Billpoint dan menjadikan Billpoint sebagai alat pembayaran utama ebay saat itu dan membuat Billpoint khusus hanya untuk alat pembayaran di ebay saja, karenanya Paypal hanya tampil beberapa kali sebagai pilihan alat pembayaran di ebay dibandingkan Billpoint. Tetapi karena masyarakat lebih menyukai Paypal karena mudah dan lebih aman, pada Februari 2000 rata- rata ada 200.000 penawaran barang perhari yang menggunakan Paypal sedangkan Billpoint hanya 4.000 penawaran. Pada april 2000 lebih dari 1 juta penawaran menggunakan Paypal.



Gambar 3.2 Website Paypal

3.2.3. Keamanan Transaksi pada PayPal

PayPal lebih aman bila dibandingkan dengan alat pembayaran online yang lain. Hal ini karena pembeli yang merasa dirugikan atau tidak sesuai deskripsi yang diberitahukan,

bisa meminta uang kembali kepada penjual dalam waktu maksimal 45 hari setelah terjadi pembayaran. Jika pembeli menggunakan kartu kredit akan mendapatkan pengembalian uang chargeback dari perusahaan kartu kreditnya. PayPal juga melindungi penjual dari pengembalian uang atau komplain yang tidak benar dari pembeli sesuai pembuktian.

Perlindungan untuk penjual dirancang untuk melindungi penjual dari klaim pembeli yang mengaku telah mengirim uang yang tidak mempunyai catatan bukti pembayaran dan deskripsi transaksi, setiap pembelian dan pembayaran menggunakan PayPal selalu ada catatan bukti pembayarannya di account PayPal pengirim dan penerima uang, sebagai bukti jika benar telah terjadi pengiriman uang antara keduanya. Bisa diambil kesimpulan bahwa menggunakan PayPal lebih aman dari alat pembayaran online lain bagi pengirim dan penerima uang karena ada bukti pembayaran dan catatan deskripsi, serta dapat melakukan komplain yang benar jika terjadi sesuatu atau terhindar dari komplain yang salah.

PayPal sebagai alat pembayaran yang teraman didunia telah mengumumkan kebijakan perlindungan pembeli yang baru dan telah disempurnakan bagi para konsumen di seluruh kawasan Asia Pasifik yang ingin berbelanja online.

Kebijakan perlindungan pembeli PayPal saat ini berlaku untuk semua pengguna yang terdaftar di Asia Pasifik, termasuk Australia, China, Hong Kong, Indonesia, Jepang, Malaysia, Filipina, Singapura dan Thailand.

Dengan perlindungan pembeli Paypal ini, kini telah menjamin konsumen bahwa informasi keuangan dan transaksi e-commerce konsumen terlindungi dengan lebih baik saat membeli barang dari Internet.

Dengan menggunakan Paypal maka pembelian pada transaksi online yang baru atau belum dikenal tidak perlu khawatir akan resiko kecurangan, keamanan dan barang tidak dikirim tidak akan terjadi.

Paypal sangat fokus pada keamanan karena salah satu hasil riset Paypal dengan ACNielsen menunjukkan bahwa keamanan adalah kekhawatiran utama bagi para pembelanja online di Australia, sedangkan privasi informasi dan perlindungan konsumen merupakan dua kekhawatiran utama bagi para pembelanja di Hongkong.

3.2.4. Perbedaan Akun pada PayPal

Terdapat tiga buah jenis akun yang disediakan oleh PayPal untuk para konsumennya, diantaranya adalah sebagai berikut:

1. ***Akun Personal***

   Dengan akun tipe ini, pengguna sudah dapat mengirim dan menerima uang dan melakukan penjualan dengan eBay. Pada tipe ini, pengguna bisa menerima

pembayaran dari akun Paypal lain, namun tidak bisa menerima pembayaran dari credit atau debit card. Tidak ada biaya untuk setiap transaksi yang dilakukan pada tipe ini. Terdapat limit berapa banyak uang yang dapat diterima per bulannya. Tipe personal ini tidak cocok untuk pengguna PayPal yang merencanakan untuk berjualan produk dalam jumlah yang besar.

2. ***Akun Premier***

   Tipe ini hampir sama dengan akun Personal, bedanya pada tipe ini pengguna bisa menerima pembayaran dari credit card, debit card dan rekening bank. Pengguna juga bisa menggunakan fasilitas shopping cart dan fasilitas laporan pembayaran (payment reporting tool). Akun Premier cocok digunakan untuk penjual yang ingin menjual produknya secara reguler. Untuk pengguna yang memiliki akun personal, pengguna tersebut dapat melakukan upgrade ke akun Premier.

3. ***Akun Business***

   Tipe ini cocok digunakan untuk bisnis yang berskala besar atau online store. Pada tipe ini pengguna diperbolehkan menggunakan laporan dan tool eBay tanpa adanya persyaratan mengenai jenis transaksi. Pengguna akan dikenakan biaya dalam menggunakan akun tipe ini. Jika saat ini pengguna memiliki akun Personal atau Premier, pengguna dapat melakukan upgrade ke akun Business. PayPal tidak mengenakan biaya pada pembeli dalam mengirimkan uang ke penjual. PayPal akan mengenakan biaya kepada pengguna sebagai penjual (penerima uang) sebesar 1.9% hingga 2.9% dari jumlah uang yang diterima.

3.2.5. Cara Mendaftar PayPal

Proses pendaftaran untuk memperoleh akun PayPal memerlukan data seperti email, nama, alamat, nomor telepon, nomor kartu kredit jika pendaftar memiliki kartu kredit, dan nomor rekening bank. Langkah-langkah untuk memperoleh akun PayPal, diantaranya adalah sebagai berikut:

1. Masuk ke situs www.paypal.com
2. Klik SignUp untuk mendaftar
3. Selanjutnya ada pilihan negara dan tipe akun yang diinginkan. Setelah memilih negara dan tipe akun yang diinginkan, tekan Continue.
4. Selanjutnya masukan informasi seperti nama, alamat, nomor telepon, email. Untuk jenis mata uang disarankan memilih U.S. Dollar karena mata uang rupiah belum tersedia di PayPal. Email yang dimasukan akan menjadi usernae PayPay untuk melakukan proses login atau transaksi. Isi password dengan kombinasi huruf

dan angka, minimal delapan karakter. Pada password recovery pilih dan isikan dua pertanyaan dan jawaban pribadi untuk mendapatkan password kembali jika suatu saat pengguna lupa akan passwordnya.

5. Baca User Agreement dan Privacy Policy jika diperlukan, lau beri tanda cheklist pada pilihan Yes dan ketikan kode pengaman yang berwarna kuning pada kolom yang tersedia tanpa ada spasi.

6. Jika data yang dimasukan sudah sesuai, tekan SignUp.

7. Selanjutnya sistem akan meminta pengguna untuk memasukan nomor kartu kredit yang akan digunakan untuk memasukan dana ke akun PayPal, kemudian klik Add Card. Apabila pengguna tidak ingin memasukan data kartu kredit atau pengguna tidak mempunyai kartu kredit, klik Cancel.

8. Pengguna akan menerima email konfirmasi bahwa pengguna telah mendaftar dan untuk mengaktifkan akun PayPal. Buka email dari PayPal tersebut dan klik link konfirmasi yang terdapat didalamnya untuk konfirmasi kepemilikan akun PayPal.

9. Setelah itu pengguna akan dibawa kembali ke situs PayPal dan sistem akan meminta pengguna untuk memasukan password, setelah itu pengguna akan masuk ke halaman My Account.

10. Jika pengguna sudah memasukan data kartu kredit di halaman My Account akan muncul bacaan Expanded Option. Baca instruksinya dan tekan tombol Get Number untuk menjadi Verified member PayPal.

11. Untuk mendaftar menjadi Verified member PayPal, tekan tombol Get Number untuk mendapatkan empat digit kode keamanan dari PayPal yang akan dikirimkan ke dalam pernyataan bulanan kartu kredit pengguna dan akan dikenakan biaya sebesar $ 1,95 untuk keperluan ini. Jika sudah mendapatkan empat digit kode keamanan tersebut dari pernyataan bulanan kartu kredit, login dengan account PayPal kemudian pada halaman My Account klik bagian Active Account-Complete Expanded User Enrollment. Setelah memasukan empat digit kode keamanan tersebut, akun PayPal akan menjadi Verified member dan akan ditambahkan $ 1,95 ke dalam akun PayPal pengguna.

3.2.6. Cara Verifikasi Akun PayPal Menggunakan Rekening Bank

Cara verifikasi akun PayPal dapat menggunakan kartu kredit, rekening bank atau Virtual Credit Card (VCC). Langkah-langkah untuk melakukan verifikasi akun PayPal dengan menggunakan rekening bank adalah sebagai berikut

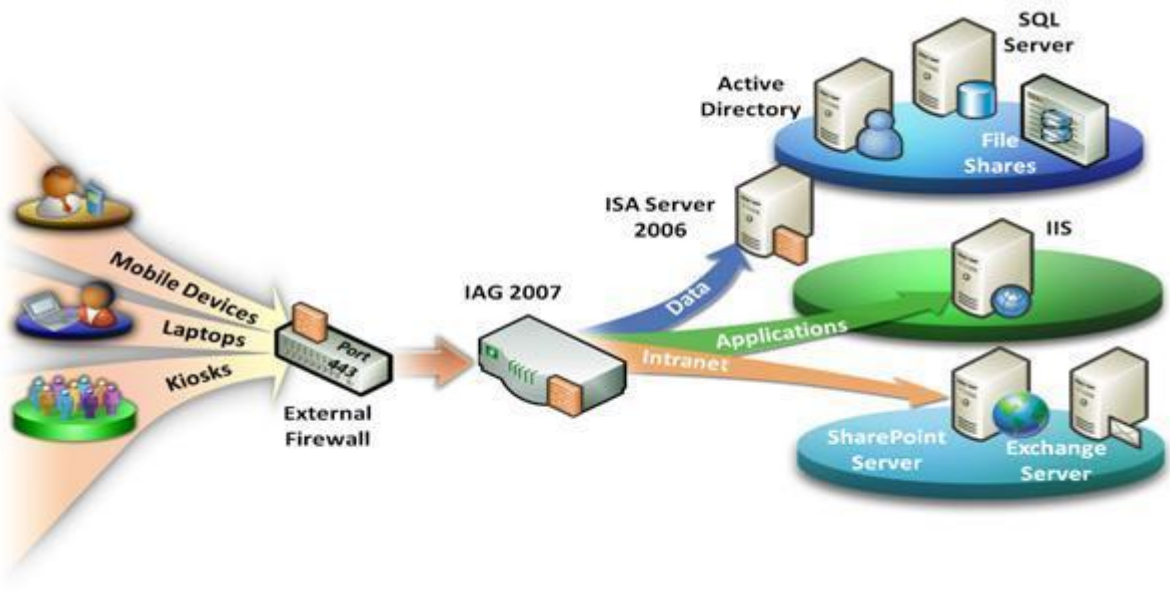
1. Untuk melakukan verifikasi, klik Get Verified pada halaman My Account.
2. Setelah itu, klik pilihan Link My Bank Account kemudian isi formulir yang disediakan. Pastikan nama yang diisikan pada formulir sama dengan nama di rekening bank. Isi nama bank penerima dan kode bank penerima.
3. Kemudian klik Add Bank Account setelah data yang dimasukan benar dan lengkap.
4. Setelah itu, akan muncul konfirmasi dari PayPal bahwa pengguna telah melakukan verifikasi akun PayPal dengan menggunakan rekening bank.
5. Tunggu dua sampai tiga hari. PayPal akan mengirimkan deposit ke rekening pengguna. Kemudian masukan dua buah deposit tersebut untuk memverifikasi akun PayPal. Setelah itu, akun PayPal sudah terverifikasi secara gratis dan bisa menggunakannya untuk proses transaksi online.

3.3. Mengidentifikasi Metode Pengamanan Data

3.3.1. Keamanan Data pada Web

3.3.1.1. Secure Socket Layer (SSL)

SSL adalah protokol client-server, yang dalam hal ini web browser adalah client dan website adalah server. Client yang memulai komunikasi, sedangkan server memberi respon terhadap permintaan client. SSL pertama kali dikembangkan oleh Netscape communications pada tahun 1994. SSL beroperasi antara protokol komunikasi TCP/IP (Transmission Control Protocol/Internet Protocol). Gambar 3.3. berikut adalah skema Secure Socket Layer.



Gambar 3.3. *Secure Socket Layer (SSL)*

Kebanyakan transmisi pesan di Internet dikirim sebagai kumpulan potongan pesan yang disebut paket. IP bertanggung jawab untuk merutekan paket (lintasan yang dilalui oleh paket). Pada sisi penerima, TCP memastikan bahwa suatu paket sudah sampai, menyusunnya sesuai nomor urut, dan menentukan apakah paket tiba tanpa mengalami perubahan.Jika paket mengalami perubahan atau ada data yang hilang, TCP/IP meminta pengiriman ulang. TCP/IP tidak memiliki pengamanan komunikasi yang bagus. TCP/IP tidak dapat mengetahui jika pesan diubah oleh pihak ketiga (man-in-the-middle attack).

SSL Memiliki dua buah sub protokol yang berjalan saat SSL dijalankan pada web browser, yaitu:

1. SSL handshaking, yaitu sub-protokol untuk membangun koneksi (kanal) yang aman untuk berkomunikasi (Gambar II-6). Sampai di sini, proses pembentukan kanal yang aman sudah selesai. Bila sub-protokol ini sudah terbentuk, maka

   http:// pada URL berubah menjadi https:// (http secure).

2. SSL record, yaitu sub-protokol yang menggunakan kanal yang sudah aman. SSL Record membungkus seluruh data yang dikirim selama koneksi

Di tempat penerima, sub-protokol SSL Record melakukan proses berkebalikan: mendekripsi data yang diterima, mengotentikasinya (dengan MAC), mendekompresinya, lalu merakitnya. Protokol SSL membuat komunikasi menjadi lebih lambat. Piranti keras, seperti kartu peripheral component interconnect (PCI) dapat dipasang ke dalam web server untuk memproses transaksi SSL lebih cepat sehingga mengurangi waktu pemrosesan.

3.3.1.2. MD5

Untuk mengidentifikasi keamanan pada data yang ditampilkan dan disimpan pada system Paypal melalui internet ini, maka Agoda menggunakan system MD5. Dalam kriptografi, MD5 (Message-Digest algortihm 5) adalah fungsi hash kriptografik yang digunakan secara luas dengan hash value 128-bit. MD5 telah dimanfaatkan secara bermacam-macam pada aplikasi keamanan dan MD5 juga umum digunakan untuk melakukan pengujian integritas sebuah file.

MD5 di desain oleh Ronald Rivest pada tahun 1991 untuk menggantikan hash function sebelumnya, MD4. Pada tahun 1996, sebuah kecacatan ditemukan dalam desainnya, walau bukan kelemahan fatal, pengguna kriptografi mulai menganjurkan menggunakan algoritma lain, seperti SHA-1 (klaim terbaru menyatakan bahwa SHA-1 juga cacat). Pada tahun 2004, kecacatan-kecacatan yang lebih serius ditemukan menyebabkan penggunaan algoritma tersebut dalam tujuan untuk keamanan jadi makin dipertanyakan. Gambar 3.2. Menjelaskan Skema MD5 Melindungi Server.

Hash-hash MD5 sepanjang 128-bit (16-byte), yang dikenal juga sebagai ringkasan pesan, secara tipikal ditampilkan dalam bilangan heksadesimal 32-digit. Berikut ini merupakan contoh pesan ASCII sebagai masukan dan hash MD5 yang dihasilkan :

MD5("The quick brown fox jumps over the lazy dog") =

9e107d9d372bb6826bd81d3542a419d6

Bahkan perubahan yang kecil pada pesan akan menghasilkan hash yang benar-benar berbeda, misalnya pada kata "dog", huruf d diganti menjadi c:

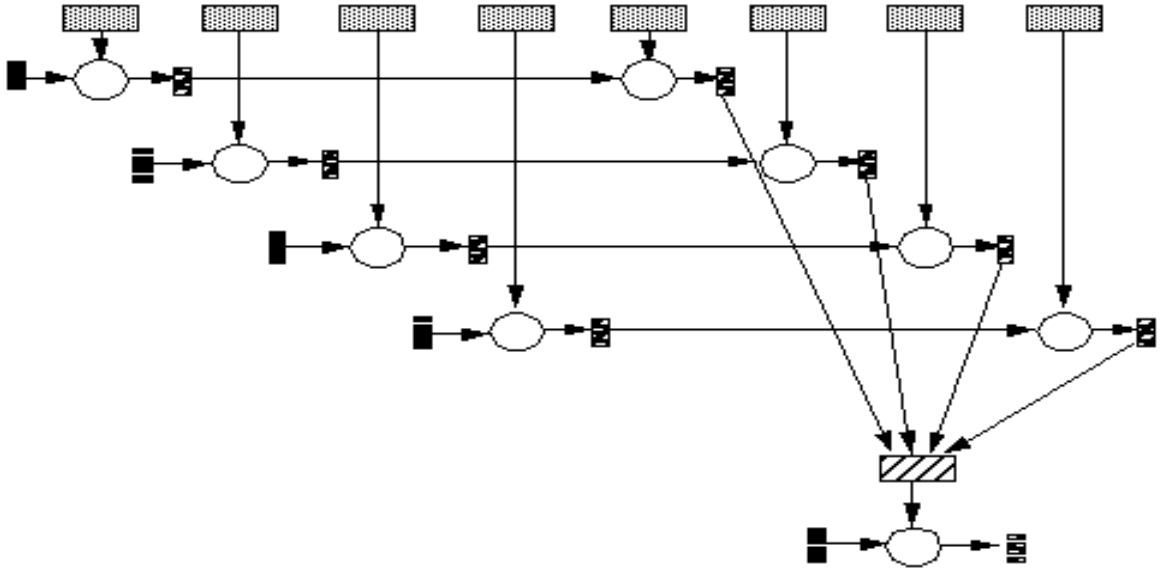
MD5("The quick brown fox jumps over the lazy cog") =

1055d3e698d289f2af8663725127bd4b

Hash dari panjang-nol ialah:

MD5("") = d41d8cd98f00b204e9800998ecf8427e

Dapat disimpulkan bahwa berapapun panjang kata atau kalimat yang dienkripsi melalui MD5, hasilnya akan mengeluarkan serangkaian huruf dan angka hasil enkripsi dengan panjang 32 karakter.



Gambar 3.4. Skema MD5 Dalam Melindungi Web Server

3.3.2. Keamanan Data Pada DataBase Web

3.3.2.1. Scan komputer

Komputer yang terinfeksi oleh jenis virus, trojan, malware tertentu dapat:

- Mengirimkan informasi username dan password ke alamat hacker
- Download file web Anda dan memodifikasinya lalu diupload kembali, file yang dimodifikasi bisa digunakan untuk menjebol web dan server

Solusinya, scan komputer secara berkala menggunakan software antivirus yang up-to-date.

3.3.2.2. Username dan Password

- Ganti password cpanel dan database secara berkala.
- Jangan gunakan username dan password cpanel untuk akses database, buat username dan password database tersendiri.
- Jangan gunakan password yang sama dengan username, dan kombinasikan password dengan karakter huruf, angka dan tanda baca.

3.3.2.3. CMS dan Extension

- Banyak web dibuat menggunakan CMS, ada baiknya memilih CMS yang aktif seperti CMS Joomla dan WordPress.
- Upgrade CMS, template, component, module, plugins dan extension ke versi terbaru
- Jangan gunakan component, module, plugins dan extension yang tidak pernah diupdate oleh developernya.
- Uninstall dan remove template, component, module, plugins dan extenstion yang tidak digunakan. Semakin sedikit menggunakan tambahan di CMS Anda semakin aman web Anda.
- Jangan gunakan software bajakan atau nulled, biasanya software tersebut telah disusupi oleh kode jahat yang bisa digunakan untuk hack web dan server Anda.

3.3.2.4. File dan folder

- Hapus file dan folder yang tidak dikenal di hosting. Anda bisa bandingkan file dan folder tersebut dengan CMS dan software yang asli atau dengan backup.
- Pastikan permission (hak akses) file adalah 644 dan untuk folder adalah 755

- Permission File config yang berisi informasi username dan password db (configuration.php di Joomla, wp-config.php di WordPress) di set menjadi 444
- Proteksi folder admin anda dengan password (Password Protect Directories)
- Tambahkan rule ke robot.txt dan .htaccess supaya search engine tidak bisa mengakses ke direktori admin atau direktori yang tidak diinginkan.

3.3.2.5. Backup

- Backup, backup dan backup. Backup file dan database web dan download ke komputer, jangan hanya disimpan di server saja.
- Backup sebelum melakukan perubahan

3.4. Isu Kode Etik Nasional dan Internasional

Internet e-commerce berbasis sampingan, keuntungan besar, menimbulkan ancaman banyak karena yang menjadi apa yang populer disebut tak berwajah dan tanpa batas. Beberapa contoh masalah etika yang muncul sebagai akibat dari perdagangan elektronik. Semua contoh berikut ini baik masalah etika dan isu-isu yang unik terkait dengan perdagangan elektronik.

Masalah etika: Jackie Gilbert Bette Ann Stead mengatakan isu-isu etis berikut terkait dengan e-commerce, antara lain sebagai berikut :

3.4.1. Privasi

Privasi telah dan terus menjadi masalah yang signifikan yang menjadi perhatian bagi calon pelanggan sekarang dan perdagangan elektronik. Berkenaan dengan interaksi web dan e-commerce dimensi berikut paling menonjol:

1. terdiri Privasi tidak diganggu, memiliki kekuatan untuk mengecualikan; individu privasi adalah hak moral.
2. Privacy adalah "suatu kondisi yang diinginkan sehubungan dengan memiliki informasi oleh orang lain tentang dirinya sendiri pada observasi / mengamati dari dirinya sendiri oleh orang lain" 2) keprihatinan Keamanan Selain masalah privasi, isu-isu etis lain yang terlibat dengan perdagangan elektronik. Internet menawarkan kemudahan belum pernah terjadi sebelumnya akses ke array yang luas barang dan jasa. Arena berkembang pesat dari "klik dan mortir" dan media dunia maya namun sebagian besar tidak diatur telah mendorong kekhawatiran tentang kedua privasi dan keamanan data.
3. isu etika lainnya Produsen Bersaing dengan Perantara Online "Disintermediasi," berarti menghilangkan perantara seperti pengecer, grosir, agen penjualan di luar dengan mendirikan sebuah Website untuk menjual langsung kepada pelanggan.

4. Disintermediasi meliputi (1) musik yang didownload langsung dari produsen (2) penulis mendistribusikan pekerjaan mereka dari situs web mereka sendiri atau melalui penulis-koperasi. Dengan perkembangan teknologi komputer, World Wide Web telah menjadi media koneksi untuk dunia jaringan. Komputer dari lokasi yang terpisah secara geografis dapat berbicara dengan satu sama lain melalui Internet. Seperti halnya teknologi baru, ada positif dan negatif yang terkait dengan penggunaan dan Adopsi. Akhirnya, e-marketplace dapat berfungsi sebagai agen informasi yang memberikan pembeli dan penjual dengan informasi tentang produk dan peserta lain di pasar.

   E-commerce menciptakan peluang baru untuk bisnis, tetapi juga menciptakan peluang baru bagi pendidikan dan akademisi. Tampaknya bahwa ada potensi yang sangat besar untuk menyediakan pendidikan e-bisnis. Sebagaimana dibahas sebelumnya tentang media yang berbeda dari e-commerce seperti TV, PC atau Mobile media baru ini akan menjadi keasyikan utama bagi pemasar selama beberapa tahun yang terutama bagaimana untuk menggabungkan mereka dalam sebuah batu bata yang terintegrasi dan klik bauran pemasaran.

Namun, teknologi berubah dengan cepat terus membawa barang baru dan jasa ke pasar disertai dengan strategi baru untuk menjualnya. Oleh karena itu, juga dapat disimpulkan bahwa isu-isu etika baru yang berhubungan dengan bisnis akan muncul. isu etika baru harus diidentifikasi dan langkahlangkah segera dan tindakan harus diambil. Awalnya, pengguna internet baru akan enggan untuk melakukan segala jenis bisnis online, karena alasan keamanan sebagai perhatian utama mereka. E-commerce memberikan kesempatan yang luar biasa dalam bidang yang berbeda tetapi membutuhkan aplikasi hati-hati untuk masalah-masalah perlindungan konsumen.

Pertumbuhan e-commerce juga akan tergantung untuk sebagian besar pada sistem keamanan TI yang efektif yang teknologi dan ketentuan hukum yang diperlukan perlu menempatkan dan diperkuat terus-menerus. Sementara banyak perusahaan, organisasi, dan masyarakat di India yang mulai memanfaatkan potensi e-commerce, tantangan kritis tetap harus diatasi sebelum e-commerce akan menjadi aset bagi orang awam.

BAB IV. KESIMPULAN

Dari penjabaran dan penjelasan kami di atas, kami dapat memberikan kesimpulan sebagaiberikut:

- PayPal merupakan alat pembayaran online yang populer bagi para pelaku bisnis online
- PayPal dipercaya secara meluas hampir di seluruh dunia

Paypal sudah sangat aman sebagai e-payment, dengan berbagai fitur-fitur yang merekasediakan untuk para penggunanya salah satunya berupa paypal security key, akan tetapi fitur itu akan lebih maksimal jika para user juga bisa menjaga dalam pemakaian akun paypal mereka. Demikianlah penjabaran demi penjabaran yang kami sampaikan mengenai Paypal, semoga dapat memberikan manfaat bagi para pembaca maupun bagi kami, ada kiranya kami mohon maaf atas segala kekurangan dan kesalahan dalam makalah kami, yang mana kekurangan dan kesalahan tersebut sangat kami sadari, tidak lupa juga kamib erharap akan adanya kritik dan saran yang membangun dari para pembaca, untuk kebaikan kami di masa yang akan datang.

Daftar Pustaka

Anonim. 2010. Belanja Online dengan PayPal Kini Lebih Aman. Diakses pada tanggal 14 Juli 2011. http://teknologi.vivanews.com/news/read/162421-belanja-online-dengan-paypal-kini-lebih-aman

Anonim. 2011. Website Paypal. www.paypal.com

American Bar Association. 2008. Data security handbook. ABA Publishing. USA.

Arianto, Devid. 2011. Pengamanan Data. Diunduh dari : http://elkomb.indonesianforum.net/t23-pengamanan-data

Cisco System. 2001. A Beginner's Guide to Network Security. USA.

http://id.wikipedia.org/wiki/Basis_data

http://ilmukomputer.org/2009/03/02/pengenalan-database/

Kurniawan, Andi dkk. 2009. Keamanan Data dan Informasi. Diunduh dari : http://ibehbandito.wordpress.com/keamanan-data-dan-informasi/

Kristanto, Harianto. 1994. Konsep dan Perancangan Database. Andi Yogyakarta

Laudo, Kenneth and Carol G. Traver. 2009. E-Commerce : Business, Technology, Society. Pearson International Edition.

mhs.stiki.ac.id/boysagi/Software/bdl/bukudb11.doc

Subhan, Mohamad. 2007. Pengenalan Database. Komunitas e-Learning Ilmu Komputer.

Tehan, Rita. 2009. Data Security Breaches. Novinka. USA.

http://lucamerolla.wordpress.com/2011/06/16/stand-alone-hornetq-security-database-modul

http://yusronz.wordpress.com/2011/03/29/resume-2-data-availibility-performance-management/

http://wongclax.wordpress.com/tisp-trik/arsitektur-dan-prototipe-keamanan-database-multilevel/#comment-27

http://blog.greensql.com/2009/12/28/database-security-database-firewall-why-should-i-use-it/#comment-321

http://www.miroconsulting.com/blog/index.php/2011/06/30/data-encryption-following-recent-security-breaches/#comment-14981

http://www.security-database.com/toolswatch/IMG/pdf/Security-Database_Best_IT_Tools_for_2009.pdf

http://blogs.mcafee.com/corporate/ceo-perspectives/mcafee-acquires-leading-provider-of-database-security-technology/comment-page-1#comment-159068

http://christopherickes.com/web-app-development/pdo-prepared-statements-binding-methods/#comment-14

http://technology.amis.nl/blog/7796/an-evening-with-oracle-database-security-expert-pete-finnigan/comment-page-1?rcommentid=480191&rerror=htmllang%3Den&rchash=7224a95eceacfc121e9fa85b85b8fc70

http://bryanlangdon.com/blog/wp-comments-post.php