

Model Penerimaan Aplikasi Elektronik Laporan Harta Kekayaan Penyelenggaraan Negara (E-LHKPN) Pada Pejabat Aparatur Sipil Negara Di Lingkungan Universitas Cenderawasih

Lisnawati Simanungkalit (slisnawati815@gmail.com), Meinarni Asnawi (meiasnawi91@gmail.com), Anthonius C.W (anthoniuscitra@gmail.com)

Program Studi Magister Akuntansi Universitas Cenderawasih

Abstract

The purpose of this study aims to determine the acceptance model of the State Administration of Wealth Report (E-LHKPN) application to state civil servants in the Cenderawasih University environment. The model used to explain the acceptance of the E-LHKPN system is the Technology Acceptance Model (TAM) with four latent variables.

The type of data used in this research is quantitative data obtained from online questionnaires using google form. The type of sampling used is non-probability sampling technique / census, where the sample is distributed to all officials who are required to report in the Cenderawasih University Environment. The number of samples as many as 127 must report, calculated using the Structural Equation Modeling (SEM) analysis technique which is one of the analysis techniques using the Partial Least Square (PLS) 7.0 analysis tool program, using the WarpPLS software.

Based on the data analysis, the results obtained are as follows: perceived ease of use has a significant effect on perceived benefits of use, perceived ease of use has a significant effect on behavioral attitudes, perceived benefits of use have a significant effect on behavioral attitudes, perceptions of ease of use have an indirect effect on behavioral attitudes mediated by benefits.

Keywords: Perceived Ease of Use, Perceived Usefulness, Behavioral Attitudes, Mediation perceived Usefulness.

Abstrak

Penelitian ini bertujuan untuk mengetahui model penerimaan aplikasi Laporan Harta Kekayaan Penyelenggaraan Negara (E-LHKPN) pada pejabat aparatur sipil Negara di Lingkungan Universitas Cenderawasih. Model yang digunakan untuk menjelaskan penerimaan sistem E-LHKPN adalah Technology Acceptance Model (TAM) dengan empat variabel laten.

Jenis data yang digunakan dalam penelitian ini adalah data kuantitatif yang diperoleh dari kuesioner online menggunakan google form. Jenis pengambilan sampel yang digunakan adalah non probability sampling dengan teknik sampel jenuh/sensus, dimana sampel dibagikan kepada seluruh pejabat wajib lapor di lingkungan Universitas Cenderawasih. Jumlah sampel sebanyak 127 wajib lapor, dihitung menggunakan teknik analisis Structural Equation Modeling (SEM) yang merupakan salah satu teknik analisis dengan menggunakan program alat analisis Partial Least Square (PLS) 7.0, menggunakan software WarpPLS.

Berdasarkan analisis data hasil yang diperoleh sebagai berikut : persepsi kemudahan penggunaan berpengaruh signifikan terhadap persepsi manfaat penggunaan, persepsi kemudahan penggunaan berpengaruh signifikan terhadap sikap perilaku, persepsi manfaat penggunaan berpengaruh signifikan terhadap sikap perilaku, persepsi kemudahan penggunaan berpengaruh secara tidak langsung terhadap sikap perilaku dimediasi manfaat penggunaan.

Kata kunci: persepsi kemudahan penggunaan, persepsi manfaat penggunaan, sikap perilaku, mediasi manfaat penggunaan.

PENDAHULUAN

Masalah keamanan merupakan salah satu aspek penting dari sebuah sistem informasi, masalah keamanan ini sering kali kurang mendapat perhatian dari para pemilik dan pengelola sistem informasi. Dalam hal ini juga menjadi kebutuhan pokok bagi masyarakat untuk meningkatkan produktivitas keseharian mereka dengan akses yang cepat dalam memperoleh informasi, yang membuat kemajuan teknologi informasi dan komunikasi menjadi pengubah pola hidup masyarakat dan memicu terjadinya perubahan sosial, budaya, ekonomi, pertahanan, keamanan, dan penegakan hukum.

Keamanan informasi adalah bagaimana kita dapat mencegah penipuan (cheating) atau, paling tidak, mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik. Selain itu keamanan sistem informasi bisa diartikan sebagai kebijakan, prosedur, dan pengukuran teknis yang digunakan untuk mencegah akses yang tidak sah, perubahan program, pencurian, atau kerusakan fisik terhadap sistem informasi. Sistem pengamanan terhadap teknologi informasi dapat ditingkatkan dengan menggunakan teknik-teknik dan peralatan-peralatan untuk mengamankan perangkat keras dan lunak komputer, jaringan komunikasi, dan data, Kemudian mendefinisikan kontrol sebagai seperangkat mekanisme yang dirancang untuk memotivasi individu mencapai tujuan yang diinginkan. Sebuah mekanisme untuk menyelaraskan tujuan dan aspirasi organisasi dengan kapabilitas, aktivitas karyawan dan kinerja.

Pengendalian internal untuk keamanan sistem informasi juga dapat dilihat sebagai praktik, prosedur, kebijakan, dan struktur tanggung jawab dalam organisasi yang membantu mengelola risiko dan melindungi aset informasi, Kontrol internal memainkan peran penting dalam keamanan sistem informasi dalam suatu organisasi. Banyak pelanggaran keamanan terjadi karena kurangnya struktur pengendalian internal yang tepat dalam organisasi. Kurangnya kontrol yang efektif dapat menyebabkan berbagai masalah termasuk pelanggaran keamanan atau subversikontrol atau karyawan. Ketidakmampuan untuk menentukan kontrol yang efektif menyebabkan masalah keamanan.

Dalam penelitian ini, kami mendefinisikan tujuan pengendalian internal berbasis nilai untuk keamanan sistem informasi. Nilai-nilai individu memainkan peran penting dalam mengembangkan tujuan keputusan yang berakar pada nilai-nilai individu, memberikan pemahaman yang lebih dalam inisiatif organisasi dalam konteks keputusan. Sejak individu nilai-nilai penting dalam mengembangkan tujuan, dalam makalah ini kami mengembangkan tujuan pengendalian berbasis tentang nilai-nilai manajer TI.

Memasukkan nilai-nilai individu dalam tujuan pengendalian membantu dalam tiga cara : Pertama, tujuan yang dibuat dengan nilai-nilai individu membantu dalam membunikan control faktor kontekstual. Kedua, tujuan pengendalian internal memberikan kerangka teoritis untuk investigasi yang lebih ketat di bidang ini. Ketiga, tujuan kontrol yang didorong oleh nilai membantu menyelaraskan tujuan individu dan organisasi. Inisiatif tersebut mengurangi kesenjangan antara manajemen filosofi tentang kontrol dan interpretasi karyawan yang sama.

KAJIAN PUSTAKA

Keamanan Sistem Informasi

Pengertian Keamanan Sistem Informasi adalah Manajemen pengelolaan keamanan yang bertujuan mencegah, mengatasi, dan melindungi berbagai sistem informasi dari resiko terjadinya

tindakan ilegal seperti penggunaan tanpa izin, penyusupan, dan perusakan terhadap berbagai informasi yang di milik.

Banyak tokoh-tokoh yang memberikan definisi tentang kriminologi, antara lain sebagai berikut:

- a) Menurut G. J. Simons, keamanan informasi adalah bagaimana kita dapat mencegah penipuan (cheating) atau, paling tidak mendeteksi adanya penipuan di sebuah sistem yang berbasis informasi, dimana informasinya sendiri tidak memiliki arti fisik.
- b) Menurut Sarno dan Iffano keamanan informasi adalah suatu upaya untuk mengamankan aset informasi terhadap ancaman yang mungkin timbul. Sehingga keamanan informasi secara tidak langsung dapat menjamin kontinuitas bisnis, mengurangi resiko-resiko yang terjadi, mengoptimalkan pengembalian investasi (return on investment).

Manfaat Keamanan Sistem Informasi

Pada perusahaan yang memiliki sumberdaya yang besar berupa bahan baku, sumberdaya manusia, maupun barang jadi sudah saatnya menggunakan sistem komputerisasi yang terintegrasi agar lebih efisien dan efektif dalam memproses data yang dibutuhkan. Sistem Informasi dalam suatu perusahaan bertujuan untuk mencapai tiga manfaat utama yaitu:

1. Kerahasiaan yaitu untuk melindungi data dan informasi dari penggunaan yang tidak semestinya oleh orang-orang yang tidak memiliki otoritas. Sistem informasi eksekutif, sumberdaya manusia, dan sistem pengolahan transaksi adalah sistem-sistem yang terutama harus mendapat perhatian dalam keamanan informasi.
2. Ketersediaan yaitu supaya data dan informasi perusahaan tersedia bagi pihak-pihak yang memiliki otoritas untuk menggunakannya.
3. Integritas yaitu untuk seluruh system informasi harus memberikan atau menyediakan gambaran yang akurat mengenai sistem fisik yang mereka wakil.

Jenis Ukuran-Ukuran Keamanan Sistem Informasi

Untuk melindungi sumberdaya organisasi, suatu perusahaan harus menerapkan beragam jenis ukuran keamanan. Ukuran keamanan yang memadai yaitu:

- a. Melindungi fasilitas komputernya dan fasilitas fisik lainnya
- b. Menjaga integritas dan kerahasiaan file data.
- c. Menghindari kerusakan serius atau kerugian-kerugian karena bencana ukuran keamanan focus pada:
 1. Keamanan fisik
 2. Keamanan data/informasi.

Keamanan fisik dikelompokkan atas:

1. Keamanan untuk sumberdaya fisik selain fasilitas komputer
2. Keamanan untuk fasilitas perangkat keras komputer. Ukuran keamanan spesifik Untuk setiap keamanan fisik dan keamanan data/informasi, maka ukuran-ukuran keamanan harus ditetapkan untuk melindungi dari akses yang tidak diotorisasi/dijijinkan, perlindungan terhadap bencana, perlindungan terhadap kerusakan atau kemacetan, perlindungan dari akses yang tidak terdeteksi, perlindungan terhadap kehilangan atau perubahan-prubahan yang tidak seharusnya dan pemulihan atau rekonstruksi data yang hilang.

METODOLOGI PENELITIAN

Jenis dan Sumber Data

Bagian ini menjelaskan bagaimana melakukan penelitian, dimana ada rincian tentang materi atau bahan, peralatan, urutan langkah yang harus dilakukan secara sistematis, logis sehingga bisa dijadikan pedoman, jelas dan mudah untuk menyelesaikan permasalahan, analisis hasil dan kesulitan yang dihadapi. Dalam penelitian ini, metode yang digunakan adalah metode penelitian kualitatif, dimana data yang diperoleh berdasarkan hasil kuesioner yang disebarkan kepada responden dalam menyebarkan kuesioner.

Teknik Pengumpulan Data

Teknik pengumpulan data yang penulis lakukan adalah teknik studi pustaka, yaitu suatu teknik pengumpulan data dengan mempergunakan dokumen, catatan, laporan, dan bahan yang relevan dengan permasalahan yang dibahas.

Metode Analisis Data

Berdasarkan data primer dan data sekunder yang telah diperoleh, kemudian menggabungkan data tersebut. Dan menggunakan metode deskriptif kuantitatif dalam menganalisis data yang ada untuk menghasilkan kesimpulan. Data tersebut kemudian dituliskan secara deskriptif untuk memberikan pemahaman yang jelas dan terarah dari hasil penelitian.

HASIL DAN PEMBAHASAN

Hasil Penelitian

Hasil kami menunjukkan bahwa penting untuk berkonsentrasi pada kontrol organisasi juga untuk peraturan keamanan yang lebih baik. Beberapa tujuan kami yang berarti seperti Meningkatkan kejelasan bisnis proses, "Memastikan Audit efektivitas kontrol," Memberikan pelatihan, "Menerapkan kecaman dan Kembangkan kemampuan untuk secara berkala meninjau kontrol pont terhadap peran yang mencakup kontrol birokrasi dalam manajemen kontrol keseluruhan untuk keamanan. Temuan ini konsisten dengan penelitian dalam aspek organisasi dari controls di mana penekanan 15 ditempatkan pada keamanan efektif struktur tata kelola untuk pengelolaan lingkungan pengendalian secara keseluruhan (Rezmerski et al, 2004; Whitman, 2003 Warkentin, dan Johnston, 2006).

Tapi ada rasa kehati-hatian yang berlebihan bergantung pada kontrol birokrasi dan kehilangan kesempatan untuk berkomunikasi secara formal peran kegiatan tingkat manajemen tersebut. Kepatuhan terhadap regulasi, misalnya, bisa jadi digunakan untuk meningkatkan secara fundamental struktur kontrol atau bisa saja menjadi checklist lain untuk manajemen nilai-nilai responden menunjukkan bahwa harus ada keterlibatan senior manajemen ke dalam merancang dan menerapkan kontrol sedemikian rupa sehingga "arah diberikan kepada organisasi.

Kontrol birokrasi baik jika tujuan organisasi dikomunikasikan secara efektif "top down" dan tidak ada kehilangan transmisi. Komunikasi bisa tercapai melalui kebijakan, prosedur, keterlibatan manajemen senior, pelatihan, dan pembuatan yang efektif kesadaran tentang kontrol Kelompok kontrol ketiga bersifat informal dan menerapkan kontrol internal melalui pengembangan tujuan

bersama dan penyesuaian tujuan individu dan organisasi. Penelitian dalam keamanan sistem informasi menekankan pentingnya nilai-nilai individu, perilaku, keyakinan dan budaya organisasi dalam meningkatkan efektivitas keamanan (Magkharas dan Furnell, 2005; Stanton dkk, 2005; McHugh dan Deek 2005; Loch dan Conger, 1996).

Hasil penelitian ini adalah konsisten dengan aliran penelitian keamanan sistem informasi yang menekankan pada dampaknya aspek informal dari tata kelola keamanan. Untuk memiliki Representasi yang lebih baik dari aspek informasi atau keamanan dan struktur pemerintahan, upaya dan pengembangan lebih banyak jenis mode kontrol klan dijamin Kontrol informal bertindak di semua tahap proses bisnis dan berkontribusi pada kontrol lingkungan dengan mengedepankan pentingnya nilai, perilaku, motivasi, kepercayaan dan rasa Kepemilikan. Kurangnya penelitian dalam pengendalian internal untuk keamanan sistem informasi serius tentang aspek informal kontrol.

Data kami menunjukkan bahwa kontrol harus disertakan nilai-nilai, keyakinan dan masukan individu, untuk memastikan keefektifan semua jenis kontrol. Salah satu narasumber berkata; "Hal yang menurut orang baik, biasanya dimulai dengan orang-orang; itu tidak perlu dari sisi teknologi. kontrol yang banyak digunakan di organisasi kekurangan perspektif karyawan yang benar-benar akan mengimplementasikan kontrol. Hal ini menyebabkan kesenjangan antara alasan yang diinginkan manajemen untuk menerapkan kontrol dan interpretasi karyawan atas kontrol. Seperti yang diamati oleh salah satu responden kami, "Tidak ada yang bisa keluar dari jalur Security 'mungkin lebih cepat jika orang merasa Anda tidak bertanggung jawab jika Anda mengambil kendali dari orang-orang dan yang sampai impore, itu membuat orang-orang melompati rintangan mereka. Ini nyata bukan teknologi Bisnis, bisnis orang-orangnya yang banyak melakukan wirah technology. Saya terus-menerus mencoba tegakkan ini ".

Penelitian ini menunjukkan bahwa masih banyak lagi yang dapat dilakukan dengan sukses dalam menentukan tujuan pengendalian internal untuk keamanan sistem informasi dari sekedar mendapatkan teknologi malam dan membuat administrasi kebijakan dan prosedur di sekitarnya. Aspek-aspek ini juga penting, Menciptakan kontrol sadar lingkungan dan menyesuaikan tujuan individu karyawan dengan tujuan keamanan organisasi penting juga. Temuan kami dikuatkan oleh temuan penelitian di bidang informasi domain keamanan sistem di mana kurangnya lingkungan keamanan informal dirasakan (Adams dan Sasse, 1999, Schultz, 2002).

Beberapa tujuan fundamental penelitian ini seperti "meningkatkan kemampuan untuk meningkatkan kontrol dengan struktur otoritas organisasi Tingkatkan kejelasan dalam definisi peran dan Memaksimalkan kesadaran tentang kontrol menunjukkan pentingnya memasukkan pandangan orang dan tidak mendefinisikan tujuan pengendalian.

Beberapa tujuan sarana penelitian ini seperti "Meningkatkan persepsi positif tentang kontrol", Tingkatkan pengetahuan tentang kontrol dan Tingkatkan kemampuan untuk menggunakan informasi untuk tujuan yang dimaksudkan menunjukkan bahwa karyawan harus dijelaskan manfaat pengendalian dan harus didorong untuk menggunakan pengetahuan dan praktik sehari-hari. Pandangan baru yang diberikan oleh penelitian ini adalah pentingnya melembagakan kontrol informal tata kelola keamanan yang efektif dalam sebuah organisasi.

Jika tujuan kontrol keamanan selaras dengan tujuan individu, organisasi akan lebih aman. Hasil kami juga establish a hubungan antara efektivitas pengendalian internal dan inisiatif keamanan organisasi. Adapun banyak panggilan di masa lalu untuk menegaskan bahwa pengendalian internal penting bagi keseluruhan organisasi keamanan (Dhillon, 2001: Warkentem, 2006). Tetapi belum ada bukti yang mendukung pernyataan tersebut.

Penelitian ini menunjukkan keberhasilan program pemerintah keamanan terkait dengan efektivitas pengendalian internal. Ini adalah kontribusi untuk bidang sistem informasi literatur

keamanan dan kontrol. Secara teoritis, penelitian ini memberikan daftar sarana dan fundamental untuk menentukan tujuan pengendalian internal untuk keamanan sistem informasi.

Ini memprovokasi tujuan, didasarkan pada nilai-nilai organisasi tentang kontrol keamanan, yang dapat digunakan untuk desain kontrol yang efektif. Ini menunjukkan kontribusi teoritis untuk disiplin sistem informasi. Bagi praktisi di dunia nyata, kerangka kerja ini memberikan pedoman tentang pentingnya menggabungkan perspektif karyawan ke dalam desain kontrol untuk hasil tata kelola keamanan yang lebih baik inisiatif.

Pembahasan

Pengertian Keamanan Sistem

Keamanan system adalah sebuah system yang digunakan untuk mengamankan sebuah computer dari gangguan dan segala ancaman yang membahayakan yang pada hal ini keamanannya melingkupi keamanan data atau informasinya ataupun pelaku sistem (user). Baik terhindar dari ancaman luar, virus. Spyware atau tangan-tangan jahil pengguna lainnya dll. Sistem komputer memiliki data-data dan informasi yang berharga, melindungi data-data ini dari pihak-pihak yang tidak berhak merupakan hal penting bagi sistem operasi. Inilah yang disebut keamanan (security). Sebuah system operasi memiliki beberapa aspek tentang keamanan yang berhubungan dengan hilangnya data-data.

Keamanan Untuk Sumber Daya Fisik Non Komputer

1. Sumberdaya fisik nonkomputer misalnya kas, sediaan, surat-surat berharga sekuritas, aktiva tetap perusahaan, atau arsip-arsip dalam lemari arsip.
2. Perlindungan dari akses yang tidak diijinkan
 - a) Akses ke aktivitas fisik non komputer harus dibatasi atau dijaga dari pihak-pihak yang tidak diijinkan/diotorisasi.
 - b) Kas harus disimpan dalam kotak terkunci (brankas) dan hanya boleh diakases oleh orang-orang yang diijinkan.
 - c) Menetapkan penjaga untuk sediaan yang disimpan digudang atau aktiva yang ada digedung administrasi atau pabrik.
 - d) Membuat pagar untuk wilayah-wilayah tempat penyimpanan aktiva.
 - e) Membuat alarm, monitor TV atau lemari arsip yang terkunci.
3. Perlindungan dari Bencana
Melengkapi gudang dengan peralatan-peralatan pencegah api dan menyimpan kas pada tempat yang tahan api.
4. Perlindungan dari kerusakan dan kemacetan dengan melakukan pemeliharaan rutin atas aktiva-aktiva operasi, seperti mesin, mobil dan lain-lain.

Keamanan Untuk Perangkat Keras Komputer

1. Perlindungan dari akses orang yang tidak diijinkan
 - a) Pusat fasilitas komputer harus diisolasi, lokasi tidak bisa di publikasikan dan tidak tampak dari jalan umum.
 - b) Akses fisik ke fasilitas komputer dibatasi pada orang yang diotorisasi, misalnya operator komputer, pustakawan, penyedia pmrosesan data atau manajemen sistem informasi.
 - c) Penjaga keamanan dan resepsionis ditempatkan pada titik-titik strategis.
 - d) Memakai alat scanning elektronik.
 - e) Pintu terkunci ke ruangan komputer dan titik pemasukkan data yang hanya bisa dibuka dengan kartu berkode magnetic.
2. Perlindungan dari bencana

- a) Fasilitas komputer diatur kelembaban dan suhu ruangnya
 - b) Untuk menghindari kerusakan karena air, maka lantai dinding dan atap harus tahan air.
 - c) Membuat detector asap atau detector api
 - d) Untuk mainframe, maka sebaiknya disediakan generator ataupun UPS.
3. Perlindungan dari kerusakan dan kemacetan membuat rencana backup file.

Keamanan Untuk Data dan Informasi

1. Perlindungan dari akses orang yang tidak diotorisasi terhadap data
 - a. Isolasi, data dan informasi yang rahasia dan penting bagi operasi perusahaan diisolasi secara fisik untuk melindungi dari akses yang tidak diotorisasi.
 - b. Otentifikasi dan otorisasi pengguna. Misalnya dengan membuat daftar pengendalian akses (ACL), membuat password, *automatic lockout*, *callback procedure*, *keyboard lock*.
 - c. Peralatan komputer dan terminal dibatasi penggunaannya. Misalnya: suatu terminal dibatasi hanya bisa memasukkan transaksi tertentu sesuai dengan fungsinya. Bagian gudang hanya bisa memasukkan transaksi tertentu sesuai dengan fungsinya.
Bagian gudang hanya bisa memasukkan dan memutakhirkan data setelah memasukkan password atau username. Peralatan komputer dan terminal juga akan terkunci otomatis bila jam kerja telah selesai.
 - d. Enkripsi. Untuk mencegah pengganggu (intruder) memasuki jaringan komunikasi data dan menyadap data, maka data rahasia yang ditransmisikan melalui jaringan dilindungi dengan enkripsi (data dikodekan dan apabila telah sampai kode tersebut dibuka di tempat tujuan). Terdapat dua jenis enkripsi yaitu: *private key encryption* & *Public Key Encryption*.
 - e. Destruksi. Untuk mencegah pihak yang tidak diijinkan mengakses data, data rahasia harus segera dihancurkan ketika masa penggunaannya selesai.

Untuk hasil cetakan, segera dihancurkan melalui alat penghancur kertas.

- A. Perlindungan dari akses data dan informasi yang tidak bisa dideteksi
 - a. Membuat *access log* (log akses), merupakan komponen keamanan sistem pengoperasian, mencatat seluruh upaya untuk berinteraksi dengan basis data/database. Log ini menampilkan waktu, tanggal dan kode orang yang melakukan akses ke basis data. Log ini menghasilkan jejak audit yang harus diperiksa oleh auditor internal atau administrator keamanan untuk menetapkan ancaman-ancaman yang mungkin terhadap keamanan sistem informasi.
 - b. Console log cocok bagi komputer mainframe yang menggunakan pemrosesan tumpuk. Console log mencatat semua tindakan yang dilakukan sistem operasi dan operator komputer. Console log mencatat seluruh tindakan yang dilakukan sistem

- operasi dan operator komputer, seperti permintaan dan tanggapan yang dibuat selama pelaksanaan pemrosesan dan aktivitas lainnya.
- c. Perangkat lunak pengendalian akses, Beberapa perangkat lunak berinteraksi dengan system operasi komputer untuk membatasi dan memantau akses terhadap file dan data.
 - d. Log perubahan program dan sistem. Log perubahan program dan sistem dapat memantauperubahan terhadap program, file dan pengendalian. Manajer pengembangan system memasukkan kedalam log ini seluruh perubahan dan tambahan yang diijinkan terhadap program. Perubahan dan tambahan yang diijinkan terhadap program harus diperiksa internal auditor untuk memeriksa kesesuaian dengan prosedur perubahan yang disarankan.
- B. Perlindungan Dari Kerugian atau Perubahan yang tidak di harapkan Terhadap Data atau Program
1. Log (catatan) perpustakaan, memperlihatkan pergerakan dari file data, program dan dokumentasi yang digunakan dalam pemrosesan atau aktivitas lainnya.
 2. Log transaksi, mencatat transaksi individual ketika transaksi itu dimasukkan ke dalam sistem on-line untuk pemrosesan. Log ini memberikan jejak audit dalam sistem pemrosesan online. Termasuk dalam log ini adalah tempat memasukkan transaksi, waktu dan data yang dimasukkan, nomor identifikasi orang yang memasukkan data, kode transaksi dan jumlah. Perangkat lunak sistem juga meminta nomor transaksi. Secara teratur daftar log transaksi ini harus dicetak.
 3. Tombol perlindungan pada 3 ½ floppy disk
 4. Label file
 5. Memori hanya baca (read only memory)
 6. Penguncian (lockout), merupakan perlindungan khusus yang diperlukan untuk melindungi basis data/database, karena beragam pengguna dan program biasanya mengakses data secara bergantian dan terus menerus. Penguncian mencegah dua program mengakses data secara bersamaan. Akibatnya, satu program harus ditunda sampai program lain selesai mengakses. Jika kedua program diijinkan untuk memutakhirkan record yang sama, maka satu data dapat dicatat berlebihan dan hilang.

Pemulihan Dan Rekonstruksi Data Yang Hilang

- a. Program pencatatan vital, yaitu program yang dibuat untuk mengidentifikasi dan melindungi catatan komputer dan nonkomputer yang penting untuk operasi perusahaan, seperti catatan pemegang saham, catatan karyawan, catatan pelanggan, catatan pajak dan bursa, atau catatan tersedia.
- b. Prosedur backup dan rekonstruksi. Backup merupakan tindakan (copy) duplikasi dari dokumen, file, kumpulan data, program dan dokumentasi lainnya yang sangat penting bagi perusahaan. Prosedur rekonstruksi terdiri dari penggunaan backup untuk mencipta ulang data atau program yang hilang.
- b. Prosedur backup dan rekonstruksi. Backup merupakan tindakan (copy) duplikasi dari dokumen, file, kumpulan data, program dan dokumentasi lainnya yang sangat penting bagi perusahaan. Prosedur rekonstruksi terdiri dari penggunaan backup untuk mencipta ulang data atau program yang hilang.

PENUTUP

Kesimpulan

Dalam dunia komunikasi data global dan perkembangan teknologi informasi yang senantiasa berubah serta cepatnya perkembangan software, keamanan merupakan suatu isu yang sangat penting, baik itu keamanan fisik, keamanan data maupun keamanan aplikasi. Perlu kita sadari bahwa untuk mencapai suatu keamanan itu adalah suatu hal yang sangat mustahil, seperti yang ada dalam dunia nyata sekarang ini. Tidak ada satu daerah pun yang betul-betul aman kondisinya, walau penjaga keamanan telah ditempatkan di daerah tersebut, begitu juga dengan keamanan sistem komputer. Namun yang bisa kita lakukan adalah untuk mengurangi gangguan keamanan tersebut. Dengan disusunnya Makalah ini semoga dapat memberikan gambaran gambaran Sistem Keamanan Komputer dan dapat meminimalisir terjadinya gangguan pada system yang kita miliki serta sebagai referensi kita untuk masa yang akan datang yang semakin maju dan berkembang.

Saran

Demi kesempurnaan makalah ini, saran kami jagalah system keamanan komputer atau PC anda dari segala macam ancaman yang telah penulis paparkan diatas dengan berbagai keamanan yang dapat setidaknya meminimalisir segala macam ancaman kepada sistem PC anda.

DAFTAR PUSTAKA

- Adams, A., dan Sasse, MA "Pengguna bukanlah musuh. Asosiasi untuk Mesin Komputasi," Komunikasi iCM (42:12) 1999, hlm 4046.
- Aeran, A Tinauam komprehensif tentang Ancaman Orang Dalam dan Kontrol mereka, "Royal Holloway. Tence A Gordon. dan Loeb, MP "Mengeraluasi Keamanan Informmasi Inestments
- Menggunakan Analytic HieProses Iara, Commication dari.iCM e8: 2) 2005, hlm 79-85.
- Kardinal, LB, Sitkin,5, dan Long, CP Balancing dan Kebalancmg dalam Penciptaan dan Errolusi Pengendalian Organisasi, Organisasi Science (1S: 4) 2004, hlm +11431
- Catton, WRTelauk Menjelajalhi unfuk Mengukur HNIai uman," .imerikan Sosiologica Reniev(19: 1) 1954, hlm 49-55
- <http://rahman.staf.narotama.ac.id/2013/02/27/sistem-keamanan-komputer/>
- <http://verololy.blogspot.com/2012/11/pengertian-sistem-keamanan-jaringan.html>
- <http://afinaa.wordpress.com/2010/02/26/sistem-keamanan-komputer/>