ANALISIS KEAMANAN DIREKTORI AKTIF WINDOWS SERVER 2003 PADA PT. TIARA MARGA TRAKINDO GROUP DENGAN MENGGUNAKAN CISA

Laporan Tugas Akhir

diajukan untuk melengkapi persyaratan
mencapai gelar sarjana strata satu (S1)
Program Studi Teknik Informatika

Oleh

Bil Fauzi
NIM : 41505110172

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS ILMU KOMPUTER
UNIVERSITAS MERCU BUANA
JAKARTA
2010

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini:

Nama	:	Bil Fauzi
NIM	:	41505110172
Fakultas	:	Ilmu Komputer
Program Studi	:	Teknik Informatika
Judul Skripsi	:	Analisis Keamanan Direktori Aktif Microsoft Windows Server 2003 Pada PT. Tiara Marga Trakindo Group Dengan Menggunakan CISA

Menyatakan bahwa tugas akhir ini adalah hasil buatan sendiri dan bukan jiplakan kecuali yang tercantum dalam daftar pustaka. Apabila ditemukan didalam laporan skripsi saya terdapat unsur plagiat, maka saya siap mendapatkan sanksi akademik yang terkait dengan hal tersebut

Jakarta, Agustus 2010

Penulis

Bil Fauzi

LEMBAR PENGESAHAN

Nama : Bil Fauzi

NIM : 41505110172

Judul Skripsi : Analisis Keamanan Direktori Aktif Microsoft Windows Server 2003 Pada PT. Tiara Marga Trakindo Group Dengan Menggunakan CISA

SKRIPSI INI TELAH DIPERIKSA DAN DISETUJUI

JAKARTA, Agustus 2010

Raka Yusuf,ST., MTI

Pembimbing

Devi Fitrianah, S.Kom., MTI

Koord. Tugas Akhir Teknik Informatika

Abdusy Syarif ST., MT

KaProdi. Teknik Informatika

KATA PENGANTAR

Assalamu'alaikum Wr.Wb

Puji dan syukur penulis panjatkan hadirat Allah SWT yang telah memberikan hidayah dan rahmat-Nya, sehingga penulis berhasil menyusun laporan tugas akhir dengan judul "**Analisis Keamanan Direktori Aktif Windows Server 2003 Pada PT. Tiara Marga Trakindo Group Dengan Menggunakan CISA**" untuk melengkapi persyaratan dalam mencapai gelar sarjana strata satu (S1) pada Program Studi Teknik Informatika Fakultas Ilmu Komputer Universitas Mercubuana. Penulis sangat berterima kasih kepada semua pihak yang telah membantu dan mendukung proses penyusunan laporan tugas akhir ini. Secara khusus, pihak-pihak tersebut antara lain:

1. Kedua orang tua tercinta penulis H. Joeratman Basjri dan Hj. Meyziar yang telah memberikan semangat selama kuliah dan dalam penyusunan laporan tugas akhir ini.
2. Bapak Raka Yusuf, ST, MTI., selaku dosen pembimbing yang telah memberikan waktu, saran, pikiran dan tenaga untuk membantu penulis dalam menyelesaikan laporan tugas akhir ini.
3. Ibu Devi Fitrianah, S.Kom., MTI., selaku Koordinator Tugas Akhir Program Studi Teknik Informatika Universitas Mercubuana, Jakarta

4. Bapak Abdusy Syarif, ST., MT., selaku Ketua Program Studi Teknik Informatika Universitas Mercubuana, Jakarta
5. Rekan-rekan mahasiswa Teknik Informatika Program Kelas Karyawan Angkatan VII yang terus mendukung penulis dalam menyelesaikan laporan tugas akhir ini.
6. Rekan-rekan pada PT. Tiara Marga Trakindo group, khususnya PT. Mitra Solusi Telematika yang mendukung penulis dalam penyelesaian laporan tugas akhir ini
7. Dan pihak-pihak lain yang secara tidak langsung turut membantu dalam menyelesaikan laporan tugas akhir ini.

Penulis menyadari bahwa isi laporan tugas ini masih belum mencakup seluruh aspek audit teknologi analisa keamanan informasiyang dibahas dan penulis berharap segala hal yang terdapat dalam penulisan ini dapat digunakan oleh pihak-pihak yang memerlukannya sehingga dapat membantu melakukan audit analisis keamanan informasi pada perusahaan yang lebih detil dan akurat.

Jakarta, Agustus 2010

Penulis

ABSTRAK

Keamanan sistem informasi merupakan aspek yang sangat penting bagi kelangsungan bisnis perusahaan. Dengan adanya perkembangan teknologi informasi proses bisnis semakin tergantung terhadap dunia teknologi informasi. Akses digital dan kemampuan jaringan yang dapat menjangkau seluruh pelosok akan mempermudah proses bisnis perusahaan dalam melakukan kegiatan bisnisnya. Sayangnya pesatnya perkembangan teknologi informasi juga dapat dimanfaatkan oleh pihak-pihak yang tidak bertanggung jawab untuk melakukan aksi-aksi kejahatan. Perilaku meretas sistem untuk mencuri data atau mendapatkan akses informasi sudah berkembang dengan pesat.. Teknologi direktori aktif sendiri dirancang untuk mempermudah kinerja dari para administrator dikarenakan sistem dirancang secara hirarki. Kemudahan ini juga berarti mempermudah untuk memperkuat keamanan sistem direktori aktif terhadap isu-isu serangan yang akan timbul.

Parameter teknologi keamanan dari CISA (*Certified Information Sistem Auditor*) akan digunakan untuk analisis keamanan direktori aktif yang diterapkan pada perusahaan. CISA merupakan salah satu standar keamanan yang sudah diakui oleh dunia sebagai pihak auditor sistem informasi. Skripsi ini akan menganalisis keamanan sistem direktori aktif perusahaan dan memberikan saran-saran terhadap apa yang harus diperkuat berdasarkan parameter CISA.

Kata Kunci*: CISA, Direktori aktif, Keamanan informasi.*

ABSTRACT

Information security system is critical aspect for companies business continuity. Various growth of information technology makes business process became dependable to it. Digital access and network capability to access from everywhere makes companies more easier doing their business activities. Unfortunately fast growing of information technology also used by criminal. Hacking system skill for stealing data or gaining access became more complex. Active directory technology designed to help administrator to administer their system with hierarchical method. It will makes administrator tasks more easier to strengthen their active directory security against threats and security exposures.

CISA (Certified Information Systems Auditor) security technology parameters will be use to analyze company active directory security. CISA is well known as one of security standard in the security auditing world. This analysis will analyze company active directory security and giving suggestions to strengthen it based on CISA parameters.

Keywords: *Active directory; CISA ; Information security.*

DAFTAR ISI

LEMBAR PERNYATAAN i
LEMBAR PENGESAHAN ii
KATA PENGANTAR iii
ABSTRAK v
ABSTRACT vi
DAFTAR ISI vii
DAFTAR GAMBAR x
DAFTAR TABEL xii
BAB 1 PENDAHULUAN 1
1.1 Latar Belakang Masalah 1
1.2 Tujuan Pembahasan 2
1.3 Batasan Masalah 3
1.4 Metodologi Penyelesaian Masalah 4
1.5 Sistematika Penulisan 4
BAB II LANDASAN TEORI 6
2.1 Analisa Keamanan 6
2.1.1 Keamanan Aplikasi 7
2.1.2 Keamanan Komputer 10
2.1.3 Keamanan Data 13
2.1.4 Keamanan Informasi 14
2.1.5 Keamanan Jaringan 18
2.2 Sistem Operasi 22
2.3 Direktori Aktif 23
2.4 Kriteria Perlindungan Aset Informasi 30
2.4.1 Manajemen Keamanan Informasi 31

2.4.2 Peran Kewenangan Terhadap Data 31
2.4.3 Kontrol Lingkungan 32
2.4.4 Penyimpan Aman 36
2.4.5 Metode Autentikasi 38
2.4.6 Proteksi Akses Jaringan 43
2.4.7 Metode Enkripsi 44
2.4.8 Infrastruktur Kunci Publik 49
2.4.9 Protokol Keamanan Jaringan 51
2.4.10 Rancangan Untuk Duplikasi 52
2.5 Peralatan Analisis Keamanan 54
BAB III ANALISIS 57
3.1 Manajemen Keamanan Informasi 57
3.2 Peran Kewenangan Terhadap Data 59
3.3 Kontrol Lingkungan 64
3.4 Penyimpan Aman 69
3.5 Metode Autentikasi 70
3.6 Proteksi Akses Jaringan 77
3.7 Metode Enkripsi 82
3.8 Infrastruktur Kunci Publik 84
3.9 Protokol Keamanan Jaringan 87
3.10 Rancangan Untuk Duplikasi 90
BAB IV REKOMENDASI 93
4.1 Manajemen Keamanan Informasi 94
4.2 Peran Kewenangan Terhadap Data 95
4.3 Kontrol Lingkungan 96
4.4 Penyimpan Aman 97
4.5 Metode Autentikasi 98
4.6 Proteksi Akses Jaringan 99
4.7 Metode Enkripsi 100

4.8 Infrastruktur Kunci Publik 101
4.9 Protokol Keamanan Jaringan 101
4.10 Rancangan Untuk Duplikasi 102
BAB V PENUTUP 109
5.1 Kesimpulan 103
5.2 Saran-saran 104
DAFTAR PUSTAKA 105

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

PT. Tiara Marga Trakindo group merupakan perusahaan berskala besar nasional yang memiliki 11 group perusahaan dan lebih dari tujuh puluh kantor cabang di seluruh Indonesia. Pada setiap perusahaan berskala besar nasional permasalahan untuk mengatur para pemakai, unit-unit komputer, dan peralatan jaringan merupakan suatu kegiatan proses yang tidak pernah berhenti. Dalam mengatur proses tersebut perlu adanya suatu kegiatan yang terstruktur apalagi ketika menyangkut tugas-tugas monoton mendasar yang dilakukan tiap hari. Hal inilah yang menyebabkan lahirnya konsep dari layanan direktori yang selanjutnya akan disebut dengan direktori aktif.

Permasalahan keamanan informasi serta akses informasi internal perusahaan merupakan isu yang sering menjadi topik dan tantangan bagi para pekerja dalam bidang teknologi informasi dan para sistem administrator. Keamanan informasi bagi suatu perusahaan merupakan sesuatu yang vital dikarenakan menyangkut data strategi perkembangan arah bisnis perusahaan selama 5-10 tahun ke depan serta proses bisnis perusahaan. PT. Tiara Marga Trakindo selaku perusahaan yang memiliki lebih dari lima ribu pegawai dan lebih dari tujuh puluh kantor cabang tersebar di seluruh Indonesia juga mengalami permasalahan keamanan informasi yang sama yaitu berkembangnya jumlah karyawan mengakibatkan peningkatan penggunaan sumber daya bersama, tingkat mobilitas pegawai yang tinggi, dan harapan pada keamanan pada sistem operasi serta keamanan sistem jaringan. Hal tersebut menjadi tantangan bagi pekerja teknologi informasi internal perusahaan untuk mencegah informasi vital perusahaan jatuh ke pihak luar yang dapat dilakukan karena kelalaian manusia maupun aksi para peretas.

Hal-hal tersebut di atas menjadi alasan bagi penulis untuk melakukan analisis tingkat keamanan aset informasi internal perusahaan dengan sistem layanan direktori aktif Microsoft Windows Server 2003 Enterprise Edition Service Pack 1 yang diterapkan pada PT. Tiara Marga Trakindo group.

1.2 Tujuan Pembahasan

Tujuan pembahasan adalah untuk mengetahui sejauh mana tingkat keamanan aset informasi perusahaan dengan sistem direktori aktif Microsoft Windows Server 2003 yang di implementasi kan pada PT. Tiara Marga Trakindo grup terhadap

tindakan-tindakan kejahatan komputer seperti pencurian informasi, rancangan, rencana, dan data pelanggan perusahaan.

1.3 Batasan Masalah

Batasan masalah yang akan dibahas dalam skripsi ini adalah menganalisis keamanan aset informasi perusahaan berdasarkan acuan parameter audit sistem informasi (CISA), dibandingkan dengan implementasi keamanan direktori aktif Windows Server 2003 Enterprise Edition Service Pack 1 pada area jaringan lokal PT. Tiara Marga Trakindo grup dengan menggunakan matriks keputusan Stuart Pugh. Kriteria perlindungan aset informasi yang akan dianalisa adalah:

1. Perlindungan proses administratif/personal seperti:
    a. Manajemen keamanan informasi.
    b. Peran kewenangan terhadap data.
2. Implementasi perlindungan fisik seperti:
    a. Kontrol lingkungan
    b. Penyimpan aman
3. Perlindungan secara teknikal seperti :
    a. Metode autentikasi
    b. Proteksi akses jaringan
    c. Metode enkripsi
    d Infrastruktur kunci publik
    e. Protokol keamanan jaringan
    f. Rancangan untuk duplikasi

1.4 Metodologi Penyelesaian Masalah

Metodologi yang digunakan dalam skripsi ini adalah metode studi kasus dengan melakukan survei langsung di lapangan untuk pengumpulan data-data dan survei pustaka dengan cara mencari dan mengumpulkan referensi dari buku, artikel mengenai keamanan sistem informasi, keamanan sistem direktori aktif Windows Server 2003 dan materi lain yang berhubungan. Data-data yang terkumpul akan di analisa dengan metode matrik keputusan Stuart Pugh (*decision matrix*).

1.5 Sistematika Penulisan

Dalam penulisan ini, penulis membagi isi penulisan berdasarkan bidang pembahasan tertentu dengan sistematika penulisan sebagai berikut:

Bab I Pendahuluan

Bab ini menjelaskan mengenai latar belakang masalah, ruang lingkup masalah, tujuan penelitian, batasan masalah, metode penyelesaian masalah dan sistematika penulisan yang digunakan oleh penulis dalam menyusun penulisan ini.

Bab II Landasan Teori

Bab kedua ini dijelaskan mengenai teori-teori yang mendukung dan membantu penulisan ini antara lain pengertian analisa keamanan, sistem operasi, direktori aktif, istilah umum yang berhubungan dengan penulisan ini, dan kriteria pengamanan.

Bab III Analisis

Bab keempat menerangkan analisa keamanan direktori aktif Windows Server 2003 Enterprise Edition SP1 yang diimplementasikan oleh PT.

Tiara Marga Trakindo grup pada tingkat area jaringan lokal berdasarkan parameter-parameter keamanan dari audit sistem infomasi (CISA).

Bab IV Rekomendasi

Bab kelima memuat tentang rekomendasi penulis terhadap perusahaan berdasarkan hasil analisis pada bab III

Bab V Penutup

Bab kelima memuat tentang kesimpulan dari penelitian ini dan disertai saran-saran dari penulis.

BAB II

LANDASAN TEORI

2.1 `Teori Analisis Keamanan

Analisis berasal dari etimologi Yunani "analyein" yang berarti memecah. Analisis adalah suatu proses untuk memecahkan topik yang komplek atau memecah suatu wujud menjadi bahagian-bahagian yang kecil untuk mendapatkan pemahaman yang lebih baik (Webbwer dan Feinsilber, 1999:10).

Keamanan merupakan suatu kondisi yang terlindung terhadap bahaya, kehilangan dan kejahatan. Dalam pemahaman umum konsep keamanan hampir sama dengan konsep keselamatan Persamaan keduanya itu adalah adanya penekanan menjadi terlindung dari bahaya-bahaya yang berasal dari luar diri manusia. Tindakan yang dengan sengaja ataupun tidak sengaja melanggar batas kondisi keamanan akan

dianggap sebagai yang bertanggung jawab atas setiap pelanggaran keamanan yang terjadi. Keamanan dalam dunia teknologi informasi dapat diklasifikasikan menjadi:

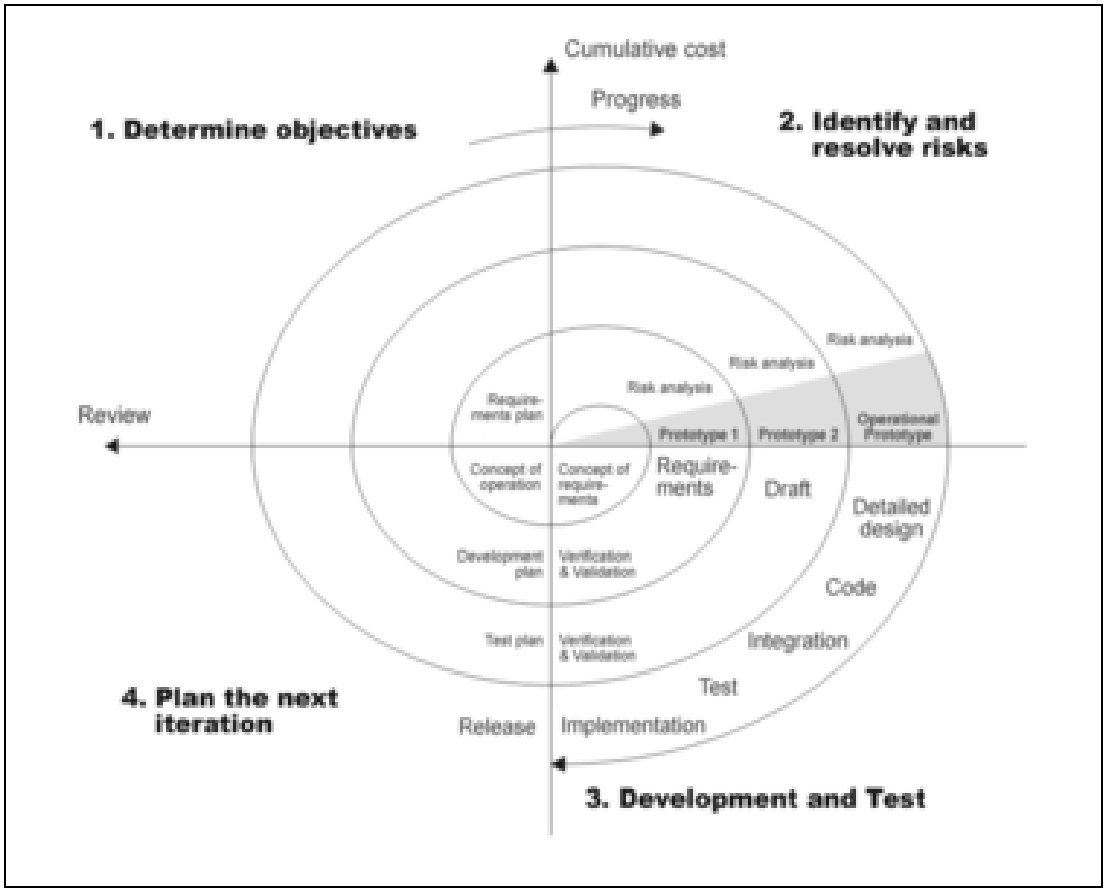
1. Keamanan aplikasi.
2. Keamanan komputer
3. Keamanan data.
4. Keamanan informasi.
5. Keamanan jaringan.

2.1.1 Keamanan Aplikasi

Keamanan aplikasi meliputi pengukuran yang diambil dari siklus proses aplikasi untuk mencegah pengecualian di dalam kebijakan keamanan aplikasi ataupun kelemahan sistem yang terjadi karena ketidak sempurnaan di dalam perancangan, pengembangan, penyebaran, peningkatan ataupun pemeliharaan aplikasi. Aplikasi hanya mengendalikan penggunaan sumber daya yang di berikan wewenang ke aplikasi tersebut bukan sumberdaya apa yang diberikan wewenang ke aplikasi tersebut. Dengan siklus pengembangan perangkat lunak (SDLC) proses perancangan pembuatan dan pengembangan aplikasi dijabarkan melalui langkah-langkah yang terarah.

Salah satu model pengembangan perangkat lunak adalah model spiral seperti yang ditunjukkan pada Gambar 2.1, diperkenalkan oleh Barry Boehm pada tahun 1988 dalam artikelnya "*A Spiral Model of Software Development and Enhancement*" Model ini bukan yang pertama membahas tentang pengembangan iteratif tetapi model yang pertama yang menerangkan permasalahan iterasi.

Menurut Boehm (1988:64) pada model spiral setiap fase yang dimulai dengan rancangan tujuan dan berakhir dengan klien sebagai pengguna aplikasi (yang bisa saja berasal dari internal) terus dilakukan peninjauan ulang. Proses analisis dan rancang bangun di terapkan pada setiap fase proyek pembuatan aplikasi, dengan tetap fokus pada tujuan akhir proyek tersebut. Model spiral merupakan gabungan fitur-fitur model purwarupa dan model Waterfall.



Gambar 2.1 Proses siklus pembuatan perangkat lunak pada pemodelan spiral Boehm

Penjelasan model spiral pada gambar 2.1 dapat diuraikan sebagai berikut:

1. Persyaratan sistem yang akan dirancang harus di jelaskan dengan sedetil-detilnya. Hal ini biasanya melibatkan wawancara sejumlah pengguna yang mewakili semua pengguna internal atau eksternal dan aspek-aspek lainnya pada sistem yang berjalan.
2. Rancangan pendahuluan harus dibuat lebih dahulu untuk sistem yang baru.
3. Purwarupa sistem yang baru dibangun melalui rancangan pendahuluan. yang biasanya berupa sistem yang terurut kebawah, dan mewakili perkiraan karakteristik dari produk akhir.
4. Purwarupa kedua ditingkatkan melalui empat prosedur, yaitu prosedur pertama evaluasi purwarupa pertama dalam hal kelebihan, kelemahan, dan resiko. Prosedur kedua menjelaskan persyaratan purwarupa kedua. Prosedur ketiga merencanakan dan merancang purwarupa kedua. Keempat membangun dan menguji purwarupa kedua.
5. Pihak pelanggan memiliki opsi untuk dapat membatalkan keseluruhan proyek jika resiko dianggap terlalu besar. Faktor resiko tersebut bisa melibatkan biaya pengembangan yang melebihi, salah perhitungan biaya operasi, atau faktor lainnya yang pada penilaian pelanggan akan menjadi tidak puas terhadap hasil produk.
6. Purwarupa yang berjalan akan dievaluasi sesuai dengan purwarupa sebelumnya, dan jika diperlukan purwarupa yang lain di kembangkan sesuai dengan prosedur pada nomor empat.diatas.
7. Langkah-langkah sebelumnya tetap diulangi sampai pelanggar merasa puas bahwa purwarupa sudah mewakili produk akhir yang diharapkan.
8. Sistem final dibangun berdasarkan purwarupa yang telah diperhalus.

9. Sistem final sepenuhnya di evaluasi dan di uji. Pemeliharaan rutin akan tetap diselenggarakan terus menerus untuk mencegah kegagalan pada segala besar dan meminimalkan waktu tidak aktif.
10. Sistem final dipergunakan oleh pihak pengguna. Perulangan proses dapat terjadi jika ada permintaan untuk penambahan modul aplikasi sistem.

2.1.2 Keamanan Komputer

Keamanan komputer terdiri dari beberapa bahagian yaitu keamanan sistem operasi, keamanan arsitektur komputer, keamanan desain dan keamanan menyalin kode.

Beberapa sistem operasi yang sangat kuat keamanannya berdasarkan pada teknologi sistem operasi kernel (komponen terpenting dari sistem operasi yang mengatur sumber daya sistem, dan komunikasi antar komponen perangkat keras dengan perangkat lunak) yang menjamin bahwa beberapa peraturan keamanan akan selalu dijalankan pada lingkungan pengoperasian. Salah satu contoh peraturan keamanan komputer adalah model Bell-LaPadula. Pada model ini strategi yang digunakan pada model ini berdasarkan pada merangkaikan fitur-fitur perangkat keras mikroprosesor yang khusus yang selalu melibatkan unit pengaturan memori sampai pada implementasi kernel sistem operasi yang benar. Hal tersebut menjadi dasar bagi keamanan sistem operasi dimana jika beberapa bahagian yang kritikal dirancang dan diimplementasi dengan benar, dapat dipastikan hampir tidak mungkin dilakukan penerobosan oleh elemen-elemen berbahaya (Landwehr, 1981:8).

Keamanan arsitektur dapat dijabarkan sebagai perkakas rancang yang menerangkan bagaimana kendali keamanan (tindakan balasan keamanan) di posisikan, dan bagaimana hubungannya terhadap keseluruhan arsitektur teknologi informasi. Kendali-kendali ini bertujuan untuk mempertahankan atribut kualitas sistem, seperti kerahasiaan, integritas, ketersedian, dapat bertanggung jawab dan dapat dijamin. Pada kata yang lebih sederhana arsitektur komputer merupakan rancangan dimana pengukuran keamanan harus di terapkan jika rencana tersebut menjabarkan solusi yang spesifik maka dahulukan untuk membangun rencana itu dan baru melakukan analisa resiko. Jika rencana lebih pada menjabar pada desain umum tingkat tinggi maka rencana pembuatan keamanan arsitektur tersebut harus berdasarkan pada analisa ancaman.

Keamanan desain dalam rekayasa perangkat lunak berarti bahwa perangkat lunak tersebut telah di rancang dari awalnya untuk menjadi aman. Praktek-praktek yang jahat selalu dianggap serius yang kemudian dijadikan perhatian untuk segera ambil tindakan meminimalisasi dampak yang dapat timbul ketika celah keamanan ditemukan. Sebagai contoh ketika berurusan dengan masukan pengguna, ketika user harus mengetik namanya, dan nama itu kemudian akan digunakan pada suatu prosedur program, tindakan hati-hati harus diambil untuk menghindari saat pengguna memasukkan nama yang kosong, program tidak menjadi kondisi istirahat (*break*).

Pada keamanan desain harus tetap diperhatikan semuanya harus berjalan dengan pemberian hak istimewa yang terbatas (pembatasan akses pengguna). Sebagai contoh server web yang berjalan pada user administratif (root atau admin) memiliki hak istimewa untuk memindahkan berkas-berkas, pengguna yang tidak seharusnya berada di

server web. Hal ini dikarenakan cacat/kekurangan pada program dapat menyebabkan keseluruhan sistem dalam bahaya. Dengan kata lain, server web yang berjalan dalan lingkungan yang diisolasi dan hanya yang memiliki hak istimewa untuk menggunakan jaringan dan fungsi sistem berkas tidak dapat berkompromi ke sistem yang sedang berjalan kecuali keamanan disekitar lingkungan tersebut sudah aman. Sistem autentikasi log masuk yang sempurna adalah yang tidak mengizinkan semuanya untuk masuk sama sekali karena dapat mengancam sistem. Beberapa desain sistem tidak akan pernah sempurna, desain kata sandi, biometrik ataupun yang sejenis tidak akan pernah sempurna.

Pada keamanan penyandian jika lingkungan pengoperasian tidak berdasarkan pada sistem operasi yang aman dan sistem operasi yang tidak aman itu mampu untuk memelihara ranah, mampu melindungi kode aplikasi dari tindakan subversi (tindakan yang tersistematis untuk menjatuhkan sistem yang berjalan) jahat, mampu melindungi sistem dari kode yang subversif, dan memiliki level keamanan yang tinggi merupakan sesuatu hal yang tidak mungkin. Jika sistem operasi yang aman tersebut memungkinkan dan pernah di implementasikan maka kebanyakan sistem komersil jatuh dalam kategori sekuriti yang rendah dikarenakan bergantung pada fitur-fitur yang tidak didukung oleh sistem operasi yang aman.

Dalam lingkungan komersial, umumnya kelemahan perangkat lunak yang berasal dari beberapa jenis kekurangan penyandian yang sudah dikenal sebelumnya. Kekurangan perangkat lunak yang biasa dijumpai termasuk *buffer overflows*, format *string vulnerabilities*, *integer overflow* dan *code/command injection*. Beberapa bahasa

pemrograman seperti C dan C++ cukup mudah diserang terharap cacat perangkat lunak tersebut, bahasa pemrograman Java lebih tahan terhadap cacat tersebut, tetapi tetap memiliki kecenderungan untuk dapat dilakukan injeksi kode/perintah dan cacat perangkat lunak lainnya yang dapat memfasilitasi terjadinya subversi. Sampai saat ini belum ada cara untuk menyediakan berbagai tingkat ketahanan subversi yang dapat diandalkan atau tingkat kombinasi dari penyandian aman.

2.1.3 Keamanan Data

Menurut Vardiansyah (2008:3) data adalah catatan atas kumpulan fakta. Data merupakan bentuk jamak dari datum, berasal dari bahasa latin yang berarti sesuatu yang diberikan. Dalam penggunaan sehari-hari data berarti suatu pernyataan yang diterima secara apa adanya. Pernyataan ini adalah hasil pengukuran atau pengamatan suatu variabel yang bentuknya dapat berupa angka, kata-kata, atau citra. Keamanan data berarti memastikan bahwa data itu selalu aman terhadap tindakan pengrusakan dan akses mendapatkan data itu sepenuhnya terkendali. Keamanan data juga membantu untuk melindungi hak privasi dan data pribadi. Salah satu contoh aturan yang jelas tentang keamanan data dapat ditemukan pada undang-undang keamanan data (DPA) yang berlaku di negara Inggris. Prinsip-prinsip keamanan data tersebut adalah:

1. Data hanya boleh dipergunakan untuk tujuan yang spesifik sama seperti tujuan data tersebut dikumpulkan.
2. Data tidak boleh dibuka ke pihak lain tanpa adanya ijin dari individu yang bersangkutan, terkecuali ada keabsahan hukum atau alasan lain yang sesuai dengan

keabsahan hukum untuk membagi informasi tersebut (contohnya untuk tindakan pencegahan dan deteksi kejahatan). Tindakan pihak lain untuk membuka data pribadi tanpa adanya kewenangan merupakan tindakan yang menyinggung.

3. Setiap individu memiliki hak yang sama untuk menahan akses informasi mengenai diri mereka, namun harus dilepas demi hukum (sebagai contoh, menahan informasi untuk pencegahan dan deteksi kejahatan)
4. Informasi pribadi dapat disimpan selama diperlukan dan diperbaharui
5. Informasi pribadi dapat tidak bisa di sebarkan diluar daerah area ekonomi Eropa kecuali pribadi tersebut telah menijinkan atau perlindungan data telah cukup tersedia, sebagai contoh harus melampirkan formulir kontrak untuk memerintahkan transmisi data.
6. Beberapa subjek pengecualian bagi organisasi yang hanya melakukan proses yang sederhana, dan penggunaan dilingkungan domestik, semua entiti yang memproses informasi personal harus didaftarkan ke komisaris informasi.
7. Entiti yang menahan informasi personal diperlukan untuk memastikan takaran keamanan cukup terpenuhi. Hal tersebut meliputi pengukuran keamanan secara teknis (seperti firewall) dan pengukuran keamanan organisasi (seperti pelatihan pegawai).

2.1.4 Keamanan Informasi

Setiap instansi pemerintahan, militer, korporat, institusi keuangan, rumah sakit dan bisnis pribadi pasti memiliki informasi rahasia mengenai karyawan, pelanggan,

produk, penelitian dan status keuangan. Hampir kesemua informasi itu pada masa sekarang dikumpulkan, diproses, dan disimpan pada perangkat komputer dan di transmisikan melintasi jaringan ke komputer lainnya. Jika informasi rahasia mengenai bisnis pelanggan, keuangan, atau produk baru jatuh ketangan kompetitor dapat menyebabkan perusahaan tersebut kehilangan bisnis, terkena tuntutan hukum bahkan sampai kebangkrutan bisnis. Perlindungan informasi rahasia merupakan suatu persyaratan bisnis, dan pada beberapa kasus merupakan persyaratan secara kode etik dan keabsahan.

Prinsip kerahasian, integritas dan ketersedian informasi merupakan prinsip dasar keamanan informasi (Gurpreet, 2007:30). Ketiga hal ini umumnya dikenal sebagai CIA (*Confidential, Integrity, Availability*) Triad (lihat gambar 2.2)

Gambar 2.2 Komponen keamanan informasi

Pada gambar 2.2 diatas proses kerahasiaan, integritas dan ketersediaan dapat di uraikan menjadi tiga porsi yaitu perangkat lunak, perangkat keras dan komunikasi dengan tujuan untuk mengidentifikasikan dan menerapkan standar keamanan informasi pada tingkat industri, seperti mekanisme keamanan dan pencegahan pada tiga tingkatan yaitu tingkat fisik, individu dan organisasi. Secara esensi prosedur dan kebijakan di diterapkan sebagai pemberitahuan ke semua pihak (para administrator, pengguna dan operator) bagaimana menggunakan produk teknologi informasi untuk memastikan keamanan informasi di dalam suatu perusahaan/organisasi.

Komponen pertama dari keamanan informasi dalam segitiga CIA adalah kerahasiaan (*confidentiality*). Kerahasiaan merupakan suatu kepunyaan yang tidak boleh disebarkan kepada individu atau sistem yang memiliki kewenangan terhadapnya. Sebagai contoh transaksi kartu kredit melalui Internet memerlukan nomor kartu kredit di transmisikan dari pihak pembeli ke pihak penjual dan pihak penjual ke jaringan pemrosesan transaksi. Sistem akan mencoba untuk memaksakan kerahasian dengan mengenkripsikan nomor kartu selama transmisi, dengan membatasi tempat-tempat yang memungkinkan data nomor tersebut terlihat (seperti dalam basis data, berkas log, cadangan, tanda terima tercetak, dan sebagainya), dan membatasi akses dimana nomor tersebut tersimpan. Jika pihak yang tidak berwenang dengan berbagi cara dapat memperoleh nomor kartu kredit tersebut, kebocoran kerahasiaan telah melanda.

Kebocoran rahasia bisa terjadi dalam berbagai bentuk, mengijinkan seseorang untuk melihat layar komputer ketika kita sedang menampilkan data rahasia termasuk pelanggaran kerahasian. Pada komputer laptop yang terdapat informasi sensitif tentang

kepegawaian perusahaan dicuri ataupun dijual juga merupakan pelanggaran kerahasiaan. Memberikan informasi rahasia melalui pesawat telepon juga bentuk pelanggaran kerahasianan jika pihak penelpon tidak berwenang untuk mendapatkan informasi tersebut. Kerahasiaan diperlukan untuk mempertahankan hak privasi orang-orang yang informasi pribadinya berada pada sistem

Komponen kedua adalah keterpaduan (*integrity*), dalam keamanan informasi integriti (kepaduan) berarti data tidak bisa di modifikasi tanpa adanya kewenangan. Hal ini tidak sama dengan istilah refensial integriti dalam basis data. Integritas (keterpaduan) dilanggar jika, pekerja secara tidak sengaja atau dengan niat jahat menghapus berkas data yang penting, ketika virus komputer menginfeksi komputer, ketika pekerja mampu untuk memodifikasi upahnya sendiri dalam basis data pembayaran upah, ketika pengguna yang tidak berwewenang menghancurkan situs web, ketika seseorang mampu untuk melakukan hak memilih yang banyak pada suatu sistem pengumpulan suara secara tersambung, dan sebagainya.

Ada berbagai cara dimana keterpaduan dapat dilanggar tanpa niat jahat. Pada kasus yang sederhana, seorang pengguna dapat jadi salah mengetik alamat seseorang. Pada skala yang besar, jika proses yang terautomasi tidak ditulis ataupun di uji secara benar, bentuk pembaharuan basis data dapat merubah data dalam cara yang tidak benar, menyebabkan keterpaduan data telah di kompromikan. Pekerja profesional di bidang keamanan informasi memiliki tugas untuk menemukan cara-cara kendali implementasi yang mencegah kesalahan dalam keterpaduan tersebut.

Komponen ketiga adalah ketersediaan (*availability*), pada setiap sistem informasi keberadaan informasi harus tersedia setiap saat ketika dibutuhkan. Hal ini berarti sistem komputer dipergunakan untuk menyimpan dan memproses informasi, kendali keamanan digunakan untuk melindungi informasi, dan jalur komunikasi yang digunakan untuk mengaksesnya haruslah berfungsi secara benar. Ketersediaan sistem yang tinggi bertujuan agar informasi tersebut selalu tersedia setiap saat, mencegah kekacauan layanan selama terjadi kekurangan daya, kegagalan perangkat lunak, dan proses peningkatan sistem. Tindakan untuk memastikan ketersedian informasi termasuk pencegahan serangan penolakan layanan (*denial-of-service*).

2.1.5 Keamanan Jaringan

Manfaat dari adanya jaringan adalah adanya kemampuan untuk saling berbagi, tetapi dengan mengijinkan orang lain untuk mengakses komputer menciptakan kesempatan bagi siapapun yang berniat jahat. Jaringan pada awalnya relatif aman karena berada pada sistem tertutup, namun pihak yang berniat jahat akan berbuat apapun untuk melakukan pengrusakan terhadap akses fisik ke sistem yang terhubung pada area jaringan lokal. Akses jarak jauh dan konektifitas internet telah merubah hal itu. Ketersedian yang luas dan biaya jaringan satelit yang lebih murah (DSL and kabel) membuat komputer yang dirumah dapat tetap terkoneksi ke Internet selama 24 jam per hari, yang akan meningkatkan kesempatan bagi para penyusup untuk memperoleh akses. Kebijakan keamanan jaringan meliputi penggabungan usaha pencegahan yang dibuat untuk mengatasi kelemahan infrastruktur jaringan komputer, adopsi kebijakan-kebijakan

para administrator jaringan untuk melindungi jaringan dan sumber daya jaringan yang dapat diakses oleh individu yang tidak memiliki kewenangan untuk akses, selalu konsisten,memantau jaringan secara terus menerus dan mengukur ketidak efektifkan jaringan menjadi satu tindakan pengamanan (Jahchan, 2008:289).

Keamanan jaringan dimulai dari proses autentikasi setiap pengguna, seperti nama pengguna dan kata sandi. Setelah terautentikasi, aturan pada firewall akan memaksa kebijakan akses, seperti layanan apa yang diijinkan untuk di akses bagi pengguna jaringan. Walaupun terbukti efektif untuk mencegah akses yang tidak berwenang, komponen ini gagal untuk memeriksa konten yang berpotensi berbahaya seperti *worm* komputer (program komputer yang bisa menggandakan diri sendiri yang bertujuan untuk menghabiskan sumber daya lebar pita) di transmisikan melalui jaringan. Sistem pencegahan pengacauan (*Intrusion Prevention System*) membantu mendeteksi dan mencegah malware (perangkat lunak yang dirancang untuk menembus atau merusak sistem komputer tanpa pemilik bisa melakukan pencegahan). Sistem pencegah pengacauan termasuk memantau lalu lintas jaringan yang mencurigakan seperti konten, volume, dan anomali untuk melindungi jaringan dari serangan seperti penolakan layanan (*denial-of-service*). Komunikasi diantara dua host menggunakan jaringan bisa di enkripsi untuk menjaga kerahasian. Event (pesan perangkat lunak yang menunjukkan sesuatu sesuatu telah terjadi) individual yang melanda jaringan dapat di lacak untuk tujuan audit dan analisis tingkat lanjut.

Beberapa resiko keamanan yang terdapat pada jaringan adalah meliputi ancaman akses terhadap keamanan, ancaman keamanan internal, ancaman keamanan eksternal

dan ancaman akses jarak jauh. Pada ancaman akses terhadap keamanan, kemampuan untuk akses sumber daya jaringan berbeda pada administrator dan pengguna. Administrator menginginkan kondisi jaringan aman sementara pengguna menginginkan akses yang mudah ke sumber daya jaringan. Hal ini merupakan kondisi yang ganjil dikarenakan akses dan keamanan selalu bertolak belakang, semakin menitikberatkan ke satu sisi maka sisi yang lain yang berkurang. Bagi jaringan yang digunakan oleh perusahaan untuk kegiatan bisnis, kuncinya adalah untuk menyeimbangkan kedua hal tersebut sehingga karyawan tidak menjadi frustasi dan tidak nyaman dengan takaran keamanan, sementara tingkat keamanan harus tetap terjaga guna mencegah pihak yang tidak berwenang mendapatkan akses.

Ancaman keamanan internal merupakan bentuk ancaman yang berasal dari dalam area jaringan lokal perusahaan ataupun area jaringan luas pada cabang perusahaan. Ancaman internal termasuk tindakan pegawai yang dengan sengaja berusaha mencuri data atau memperkenalkan virus baru atau melakukan serangan terhadap jaringan. Ancaman internal lainnya juga bisa berasal dari pekerja diluar perusahaan (pekerja kontrak, pekerja jasa pembersih kantor, dan sebagainya) yang memiliki akses fisik ke area jaringan lokal komputer. Walaupun demikian, banyak ancaman internal terjadi karena unsur ketidak sengajaan. Pekerja bisa saja menginstal, menggunakan perangkat lunak ataupun perangkat keras demi kenyamanan mereka, tidak sadar bahwa hal tersebut dapat menjadi resiko keamanan pada komputer mereka dan keseluruhan jaringan perusahaan. Beberapa contoh ancaman keamanan internal adalah instalasi perangkat lunak yang tidak sah seperti program permainan maupun perangkat

lunak yang gratis diunduh dari Internet, instalasi perangkat keras yang tidak sah (contohnya Wireless Access Point pribadi, modem pribadi, media penyimpan portabel pribadi serta pencetak) merupakan tindakan yang beresiko dalam keamanan jaringan karena dapat membuka celah kepada pihak pengganggu atau pihak berniat jahat untuk mengakses informasi perusahaan.ataupun untuk menyerang ketersedian sumber daya jaringan.

Ancaman keamanan eksternal merupakan bentuk ancaman yang berada diluar area jaringan lokal, biasanya melalui Internet (tetapi terkadang melalui koneksi dial-up ke server akses jarak jauh yang berada pada area jaringan lokal. Ancaman tersebut biasanya dilakukan oleh peretas, perengah dan penyerang jaringan. Mereka memiliki kemampuan untuk mengekploitasi cacat pada aplikasi perangkat lunak dan sistem operasi dan memahami karakteristik sistem operasi dan perangkat lunak tersebut. Mereka melakukan ekploitasi cara kerja protokol komunikasi jaringan untuk melakukan empat hal seperti pertama masuk dan akses ke dalam sistem (baca, duplikasi, merubah atau hapus) data. Kedua, membuat sistem menjadi tidak merespon, merusak dan menghancurkan sistem operasi dan berkas aplikasi sehingga tidak bisa digunakan. Ketiga, menanam virus dan worm yang dapat menyebar ke sistem lainnya melalui jaringan lokal. Keempat penggunakan sistem untuk melancarkan serangan terhadap sistem yang lain atau jaringan lain. Ancaman lainya bisa juga berasal dari ekploitasi aplikasi dan sistem operasi , ekploitasi surat elektronik (e-mail), aplikasi berita cepat (contohnya Yahoo Messenger), berbagi berkas dan unduh dan halaman web yang jahat juga dikategorikan sebagai ancaman.

2.2 Sistem Operasi

Menurut pendapat Tanenbaum (2001:3) sistem operasi dapat dilihat dari dua sudut pandang yaitu pengaturan sumber daya dan mesin meluas. Dalam sudut pandang pengaturan sumber daya, tugas sistem operasi adalah untuk mengatur bagian-bagian yang berbeda dari sistem secara efisien. Dalam sudut pandang mesin meluas, tugas dari sistem operasi adalah menyediakan pengguna dengan suatu mesin virtual yang lebih nyaman digunakan daripada mesin yang sebenarnya.

Secara umum, sistem operasi adalah perangkat lunak pada lapisan pertama yang ditaruh pada memori komputer pada saat komputer dinyalakan. Sedangkan perangkat lunak lainnya dijalankan setelah sistem operasi berjalan, dan sistem operasi akan melakukan layanan inti umum untuk perangkat-perangkat lunak itu. Layanan inti umum tersebut seperti akses ke cakram, manajemen memori, skeduling task, dan antar-muka user. Sehingga masing-masing perangkat lunak tidak perlu lagi melakukan tugas-tugas inti umum tersebut, karena dapat dilayani dan dilakukan oleh sistem operasi. Bagian kode yang melakukan tugas-tugas inti dan umum tersebut dinamakan dengan kernel (komponen pusat pengatur sumber daya dan komunikasi antara komponen perangkat keras dengan perangkat lunak) suatu sistem operasi.

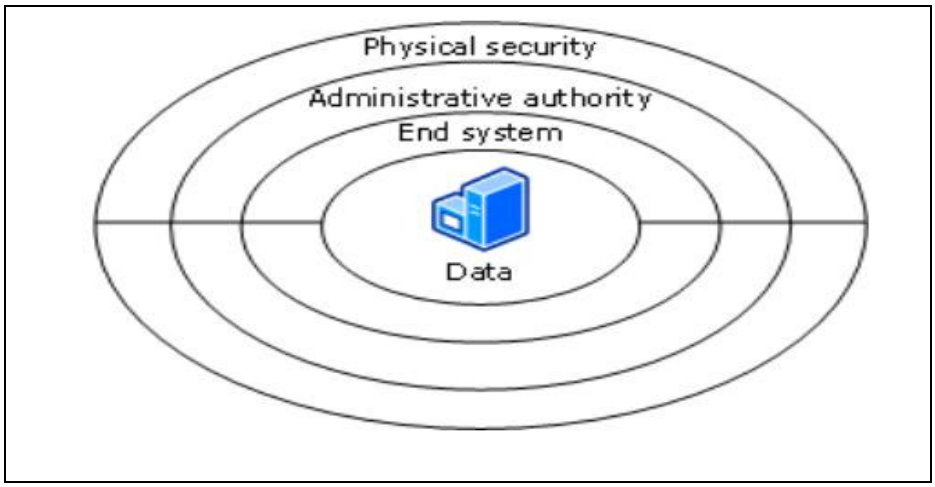
2.3 Direktori aktif

Direktori aktif merupakan basis data dengan menggunakan sistem operasi Windows Server 2003. Direktori aktif berisikan informasi tentang objek seperti pencetak, akun jaringan, grup, server seperti informasi lainnya tentang ranah. Direktori

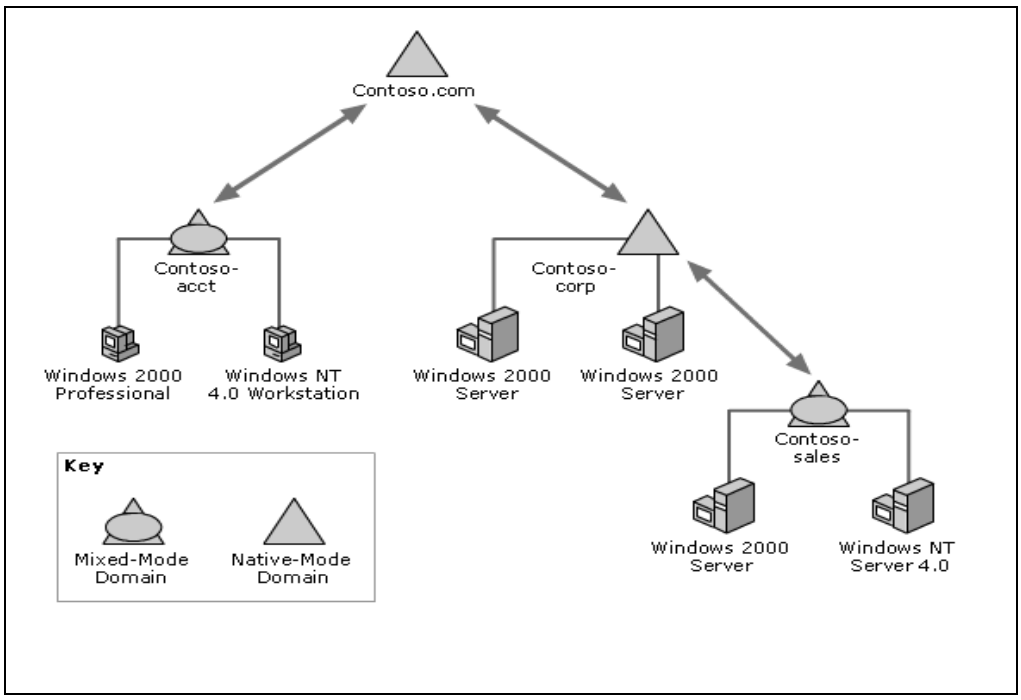
aktif di dukung dalam Windows Server 2003, Enterprise Edition dan Datacenter Edition. Direktori aktif tidak bisa di instal pada server Windows 2003 Web Edition. Direktori aktif menyediakan hirarki yang terstruktur bagi administrator untuk mengatur objek-objek di dalam ranah. Perencanaan yang layak pada struktur direktori aktif dapat mengijinkan para administrator untuk menyederhanakan delegasi administratsi dan memudahkan pengaturan sistem desktop.

Keamanan kebijakan direktori aktif dapat dipisahkan menjadi lapisan-lapisan (lihat Gambar 2.3):

a. Keamanan fisik, untuk keamanan pengatur ranah dan jaringan (akses fisik pengatur ranah, duplikasi data, dan komponen jaringan)
b. Kewenangan administratif, meliputi manajemen keamanan dan praktek administrasi yang aman.
c. Sistem tujuan, meliputi keamanan pengaturan pengatur ranah, pengaturan kebijakan, dan praktek penyebaran.



Gambar 2.3 Lapisan keamanan direktori aktif



Gambar 2.4 Contoh direktori aktif

Keuntungan dari direktori aktif, pada setiap perusahaan pastilah membuat struktur organisasi sebagai usaha untuk memudahkan pengaturan di lingkungan perusahaan. Sebagai contoh, perusahaan-perusahaan sering membagi struktur operasionalnya kedalam bentuk departemen (seperti sales, marketing dan engineering), dan individu yang mengisi peran dalam departemen tersebut (sebagai manajer dan staf). Tujuan pembagian tersebut adalah untuk membangun dan mengkoordinasi berbagai fungsi pekerjaan yang diperlukan untuk keberhasilan suatu organisasi. Contoh direktori aktif dapat dilihat pada gambar 2.4.

Departemen teknologi informasi didalam suatu perusahaan bertanggung jawab untuk memelihara keamanan informasi-informasi perusahaan. Pada kegiatan bisnis modern, hal ini meliputi perencanaan, penerapan dan mengatur berbagai macam sumber daya jaringan. Server, anjungan kerja dan perangkat router merupakan infrastruktur yang

umum yang digunakan untuk menghubungkan para pengguna dengan informasi yang dibutuhkan untuk melaksanakan pekerjaannya. Kecuali pada ruang lingkup organisasi yang kecil, usaha yang dibutuhkan untuk mengatur semua sumber daya yang berhubungan dengan teknologi sangatlah besar.

Untuk itulah Windows Server 2003 dan direktori aktif Microsoft dibuat untuk mengatasi hal-hal tersebut. Pada definisi yang dasar, direktori merupakan suatu tempat penyimpanan yang merekam informasi dan membuatnya tersedia untuk para pengguna. Tujuan keseluruhan perancangan direktori aktif adalah untuk membuat satu sentralisasi (atau desentralisasi dengan banyak pengatur ranah) penyimpanan informasi yang diatur secara aman terhadap sumber daya perusahaan. Manajemen akun pengguna, keamanan, dan aplikasi hanyalah beberapa wilayah dari direktori aktif.

Direktori aktif merupakan penyimpan data yang mengijinkan para administor untuk mengatur berbagai jenis informasi dalam satu distribusi basis data. Hal ini bukan merupakan tugas yang ringan, tapi banyak fitur-fitur teknologi direktori aktif yang membuatnya dapat memenuhi kebutuhan berbagai ukuran skala perusahaan. Secara spesifik fitur-fitur direktori aktif adalah:

1. Hirarki organisasi**,** perbedaan yang mencolok pada struktur datar dari ranah Windows NT 4, direktori aktif dirancang dengan menggunakan rancangan hirarki. Melalui berbagai variasi komponen organisasi (atau objek), suatu perusahaan dapat membuat pengaturan jaringan, infrastuktur dan struktur organisasi yang mencerminkan suatu organisasi bisnis. Hal ini berarti jika satu perusahaan memiliki sepuluh divisi besar, dan setiap divisi memiliki beberapa departemen (seperti sales

atau personalia), model layanan direktori dapat mencerminkan struktur ini melalui berbagai variasi objek dalam suatu direktori. Struktur ini secara efisien mengakomodir aspek fisik dan lojik sumber daya informasi seperti, basis data yang berbeda, para pengguna dan komputer. Direktori aktif juga terintegrasi dengan layanan penamaan jaringan, *Domain Name System* (DNS). DNS menyediakan penamaan secara hirarki dan lokasi sumber daya di keseluruhan perusahaan dan di publik Internet.

2. Skema yang dapat diperluas, salah satu hal yang selalu menjadi fokus perhatian dalam setiap jenis basis data adalah kesulitan yang akan dijumpan ketika mencoba untuk mengakomodir semua jenis informasi kedalam suatu tempat penyimpanan informasi. Untuk itulah direktori aktif dirancang untuk dapat diperluas. Dalam hal ini perkataan diperluas berarti kemampuan untuk memperluas skema direktori. Skema merupakan struktur yang aktual dalam suatu basis data seperti tipe data dan lokasi dari atribut. Skema merupakan hal penting karena mengijinkan aplikasi untuk mengetahui dimana kepingan informasi berada. Kita tidak bisa menghapus bagian dari skema tapi kita dapat merubah, memodifikasi atau pun mengubahnya. Informasi yang tersimpan dalam stuktur direktori aktif dapat diperluas dan dan di dapat diubah-ubah melalui berbagai jenis peralatan. Salah satu peralatan yang dapat digunakan adalah *Active Directory Services Interface* (ADSI) yang tersedia di situs Microsoft. ADSI menyediakan objek dan antar muka yang dapat diakses dengan bahasa pemrograman yang umum seperti Visual Basic, Visual C#, dan Active Server Pages (ASP) . Fitur-fitur ini memungkinkan direktori aktif beradaptasi ke suatu aplikasi

khusus dan menyimpan tambahan informasi yang diinginkan dan juga memperbolehkan kesemua area yang bervariasi dalam suatu organisasi (ataupun keduanya) untuk berbagi data dengan mudah dalam suatu struktur direktori aktif.

3. Penyimpanan data yang tersentralisasi, seperti yang disebutkan sebelmnya, semua informasi dalam direktori aktif berada dalam suatu penyimpanan data terdistribusi yang mengijinkan para pengguna dan sistem administrator untuk dengan mudah mengakses informasti yang diinginkan dimanapun mereka berada selama dalam lingkungan perusahaan. Hal ini merupakan tujuan perancangan yang terbesar dari direktori aktif untuk mampu mnyediakan lokasi data secara keseluruhan yang aman dan tersentralisasi. Keuntungan dari penyimpanan data yang tersentralisasi termasuk mengurangi kebutuhan administrasi, mengurangi duplikasi, ketersediaan yang tinggi, dan memudahkan untuk melihat dan mengatur data.
4. Replikasi, jika performa dan keandalan server tidak menjadi bahan perhatian, mungkin lebih masuk akal untuk menyimpan keseluruhan direktori aktif di satu server. Dalam kenyataan, keinginan untuk dapat tetap mengakses cabang yang terpencil namun memiliki keterbatasan biaya, cara replikasi basis data dapat dilakukan melalui jaringan. Direktori aktif menyediakan fungsi replikasi melalui jaringan dengan menggunakan teknologi replikasi. Basis data direktori aktif dapat didistribusikan ke banyak server dalam lingkup jaringan perusahaan. Kemampuan untuk mendefinikasi lokasi membuat para administrator sistem dan jaringan membatasi jumlah lalu lintas jaringan antar lokasi jauh dan memastikan jaringan tetap memiliki performa dan kemampuan untuk digunakan yang memadai.

Sinkronisasi data yang dapat diandalkan mengizinkan untuk replikasi secara banyak, hal inilah yang membuat pengatur ranah dapat selalu memperbaharui informasi yang tersimpan dalam direktori aktif dan memastikan konsistensi informasi dalam waktu yang sama.

5. Kemudahan pengaturan, untuk mengakomodasi berbagai model bisnis, direktori aktif dapat di konfigurasi untuk administrasi terpusat ataupun tidak terpusat. Hal ini membuat para administrator sistem dan jaringan kemampuan untuk mendelegasikan kewenangan dan tanggung jawab keseluruhan organisasi namun tetap dapat memelihara keamanannya. Peralatan-peralatan dan utiliti yang digunakan untuk tambah, pindah dan merubah objek direktori aktif tersedia di seluruh pengatur ranah Windows Server 2003. Peralatan dan utility tersebut dapat mempermudah membuat perubahan yang meluas dengan hanya beberapa klik saja pada tetikus.
6. Keamanan jaringan, melalui penggunaan log on masuk tunggal dan berbagai jenis autentikasi dan mekanisme enkripsi, direktori aktif dapat memfasilitasi keamanan dikeseluruhan perusahaan. Melalui proses delegasi, kewenangan keamanan tingkat tinggi yang lebih tinggi dapat memberikan izin ke administrator lainnya. Untuk memudahkan administratsi, objek dalam struktur pohon direktori aktif dapat menurunkan izin dari objek induk mereka. Para pengembang aplikasi dapat mengambil keuntungan dari berbagai jenis fitur ini untuk memastikan para penguna teridentifikasi secara unik dan aman. Administrator jaringan dapat membuat dan memperbaharui izin yang diperlukan dalam suatu penyimpangan tunggal, yang tentukan akan mencegah perubahan yang tidak akurat atau konfigurasi yang usang.

7. Manajemen konfigurasi klien, salah satu tantangan terbesar bagi para administrator sistem berasal dari pemeliharaan jaringan yang memiliki beraneka ragam sistem dan aplikasi. Salah satu bentuk kegagalan yang sederhana seperti kerusakan cakram keras dapat menyebabkan berjam-jam waktu kerja untuk mengkonfigurasi kembali dan simpan ulang anjungan kerja, terutama pada server kelas-perusahaan. Waktu kerja yang lama juga dapat disebabkan ketika para pengguna dipaksa pindah antar komputer dan mereka menginginkan semua aplikasi mereka di instalasi kembali dan seting sistem mereka di perbaharui. Banyak organisasi teknologi informasi menemukan bahwa jenis-jenis tindakan seperti itu dapat menghabiskan sumber daya dan waktu para staf teknologi informasi. Teknologi baru yang terintegrasi dengan direktori aktif mengizinkan kendali dan administrasi yang telah disempurnakan untuk mengatasi berbagai jenis persoalan jaringan. Keseluruhan keuntungan ini adalah mengurangi waktu sistem tidak tersedia, kepuasan dari pengguna dan mengurasi proses pengaturan.
8. Kemampuan sistem untuk dikembangkan, organisasi yang besar selalu memiliki pengguna yang banyak dan kuantiti informasi yang besar untuk diatur. Direktori aktif telah dirancang dengan kemampuan untuk bisa diperluas. Tidak hanya mengizinkan untuk menyimpan jutaan objek diantara server-server dan lokasi-lokasi. Fitur ini sangat meringankan beban dalam perancangan infrastruktur aktif direktori dari segi teknikal terlepas dari faktor bisnis.
9. Fungsional pencarian, salah satu keuntungan yang paling penting dari memiliki keseluruhan sumber daya jaringan tersimpan dalan satu penyimpanan tunggal adalah

adanya kemampuan untuk melakukan pencarian yang akurat. Para pengguna sering melihat sistem operasi jaringan sebagai sesuatu yang rumit. Sebagai contoh, ketika kita ingin mencari pencetak, kita harus tahu nama ranah atau nama server cetak untuk objek tersebut. Menggunakan direktori aktif, para pengguna dapat dengan cepat menemukan informasi mengenai pengguna atau sumber daya lainnya seperti pencetak-pencetak dan server-server melalui antar muka pencarian intuitif.

2.4 Kriteria Perlindungan Aset Informasi

Kriteria perlindungan aset informasi berdasarkan CISA terbagi atas tiga bahagian besar yaitu:

1. Perlindungan proses administratif/personalia seperti:
    a. Manajemen keamanan informasi.
    b. Peran kewenangan terhadap data.
2. Implementasi perlindungan fisik
    a. Kontrol lingkungan.
    b. Penyimpanan yang aman.
3. Perlindungan secara teknikal
    a. Metode autentikasi.
    b. Proteksi akses jaringan.
    c. Metode enkripsi.
    d. Infrastruktur kunci-publik.
    e. Protokol keamanan jaringan.

f. Rancangan untuk duplikasi.

2.4.1 Manajemen Keamanan Informasi

Beberapa jenis tanggung jawab dalam manajemen keamanan informasi adalah:

a. Kepala keamanan informasi, memiliki kewenangan untuk menjelaskan dan memaksakan kebijakan keamanan dalam organisasi.
b. Kepala privasi informasi, bertanggung jawab untuk melindungi keamanan informasi para pelanggan dan karyawan.
c. Manajer keamanan sistem informasi, bertanggung jawab dalam proses harian untuk memastikan pelaksanaan keamanan sistem.

2.4.2 Peran Kewenangan Terhadap Data

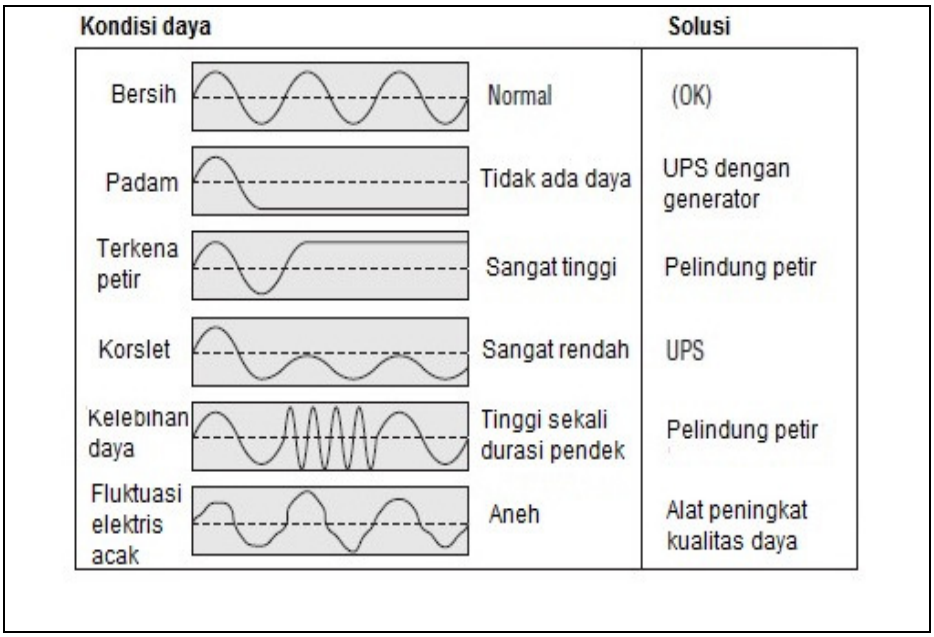
Untuk implementasi kebijakan, standar, dan prosedur diperlukan untuk identifikasi orang berdasarkan kewenangan. Tiga tingkat kewenangan adalah:

a. Pemilik data, merujuk ke pihak eksekutif atau manajer yang bertanggung jawab terhadap kandungan data, menetapkan tingkat klasifikasi informasi, menetapkan kontrol yang sesuai, menetapkan penggunaan data yang dapat diterima, identifikasi pengguna, dan menunjuk pemelihara data.
b. Pengguna data, merupakan pengguna bisnis yang mendapatkan manfaat dari data yang terkomputerisasi. Peran pengguna data termasuk mengikuti standar penggunaan yang dapat diterima, menuruti kontrol pemilik data, menjaga kerahasiaan data, dan melaporkan aktifitas yang tidak berwenang.

c. Petugas data, bertanggung jawab untuk implementasi usaha penjagaan penyimpanan data dan memastikan ketersedian data. Kewajiban dari petugas data meliputi implementasi kontrol yang sesuai dengan klasifikasi informasi, monitor pelanggaran keamanan data, mengatur kontrol akses pengguna, memastikan integritas data melalui kontrol proses, membuat salinan data untuk melindungi kehilangan data, selalu tersedia untuk memecahkan setiap permasalahan.

2.4.3 Kontrol Lingkungan

Kepentingan utama pada pusat data adalah daya elektrikal. Daya elektrikal merupakan aliran darah pada sistem komputer. Daya yang tidak stabil adalah salah satu ancaman terhadap operasi yang bersifat konsisten. Beberapa tipe kondisi daya listrik dapat dilihat pada Gambar 2.5.



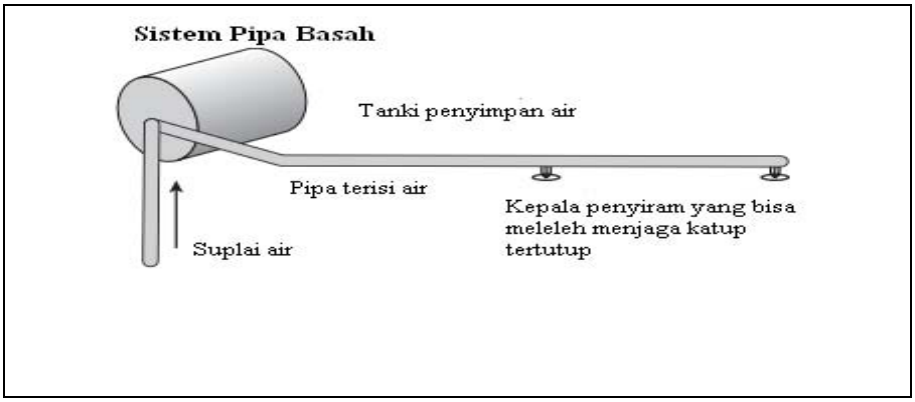
Gambar 2.5 Kondisi daya listrik

Setiap pusat data minimal harus memiliki pendingin daya dan catu data tanpa interupsi. Kontrol lingkungan meliputi:

1. Pemadaman darurat, kelistrikan memiliki keuntungan dan bahaya. Pengamanan kebakaran memerlukan saklar pemadaman darurat di lokasi dekat pintu keluar. Saklar bertujuan mematikan daya untuk mencegah individu tersengat arus listrik.
2. Catu daya tanpa interupsi merupakan monitor daya pintar yang dirangkai dengan baterai elektrik. Selama terjadi terputusnya daya, catu daya tersebut dapat menyediakan daya baterai terbatas untuk menjaga sistem tetap berjalan. Lama daya baterai tergantung pada konsumsi elektrikal dari perangkat yang disupport.
3. Generator cadangan menyediakan daya tambahan ketika pasokan daya PLN ter ganggu. Generator cadangan dapat di koneksikan ke catu daya tanpa interupsi untuk mulai secara automatis. Generator cadangan sanggup bekerja terus menerus selama memiliki persediaan oli mesin, dan bahan bakar (solar atau gas alam).
4. Sistem transfer daya menyediakan koneksi antara PLN dan baterai catu daya tanpa interupsi didalam generator. Saklar transfer daya bisa manual ataupun terkomputerisasi. Ketika terjadi pemadaman generator akan hidup untuk menyediakan arus elektrikal. Setelah daya utama hidup (PLN) maka transfer daya akan mentransferkan daya dari generator kembali ke daya PLN.
5. Pemanas, ventilasi, dan pendingin udara diperlukan pada instalasi ruangan komputer. Perangkat elektronik berjalan dengan baik pada kondisi dingin namun media magnetis tidak boleh dibiarkan membeku. Ventilasi diperlukan untuk mendinginkan perangkat komputer. Kerusakan fisik terjadi jika sirkuit komputer

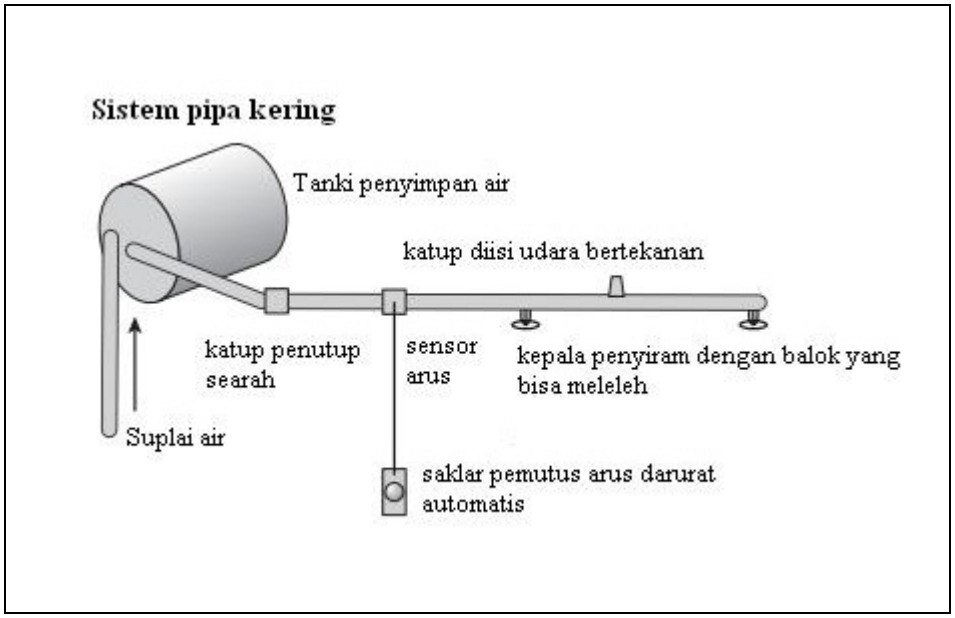
mencapai suhu 40 derajat celsius dan kerusakan sirkuit elektronik internal pada suhu 46 derajat celsius selama proses operasi. Pendingin udara digunakan untuk menjaga kelembaban yang bertujuan untuk mengatur elektrikal statis yang bisa merusak sirkuit elektrikal.

6. Deteksi panas, asap dan api harus tersedia di setiap pusat data dan penyimpanan catatan. Deteksi asap menggunakan detektor asap optik atau deteksi asap radioaktif. Deteksi panas menggunakan termostat temperatur tetap yang aktif pada suhu 93 derajat celsius atau menggunakan deteksi kenaikan-cepat (mengaktifkan alarm jika temparatur naik secara drastis dalam hitungan menit). Deteksi api bergantung pada radiasi ultraviolet dari nyala api atau tingkat getaran dari nyala api.
7. Pemadam api merupakan langkah lanjutan setelah deteksi api, dan dapat berupa sistem automatis maupun mekanikal. Sistem pemadaman api pertama berupa sistem pipa basah dimana air berada pada pipa dan pada setiap kepala penyiram terdapat penjepit yang dapat meleleh. Api yang berada dekat kepala penyiram akan melelehkan penjepit dan katup akan terbuka untuk melepaskan air didalam pipa. Hal ini ditunjukkan pada Gambar 2.6.



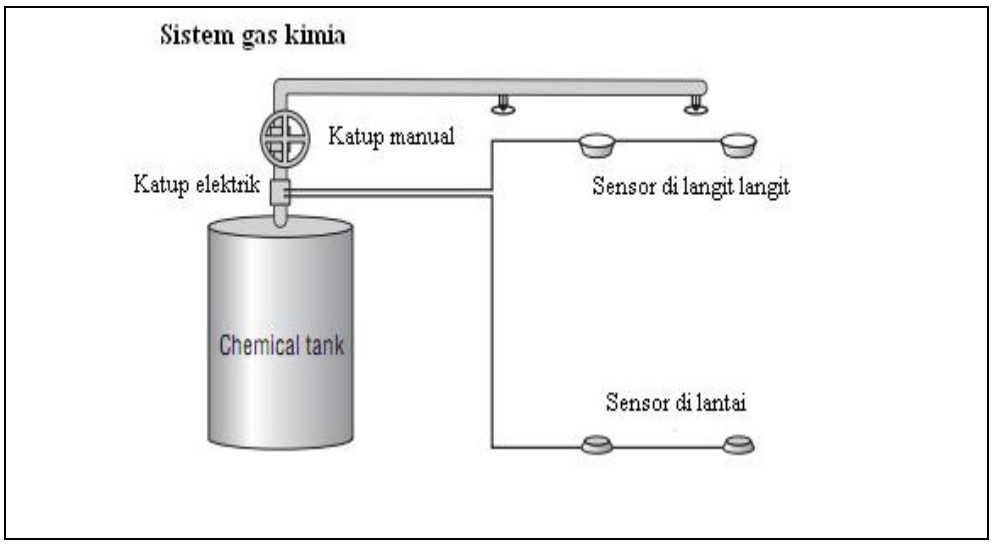
Gambar 2.6 Sistem pemadam pipa basah

Sistem yang kedua berupa sistem pipa kering dimana pipa dikompres penuh dengan udara untuk dilepaskan. Ketika katup terbuka udara keluar terlebih dahulu dan air akan dilepaskan melalui pipa seperti yang ditunjukkan oleh Gambar 2.7.



Gambar 2.7 Sistem pemadam pipa kering

Sistem yang ketiga berupa sistem kimiawi kering yang sering digunakan pada instalasi perangkat komputer karena kimiawi kering mencegah bahaya air terhadap perangkat listrik pada komputer seperti yang ditunjukkan oleh Gambar 2.8. Sistem kimiawi kering menggunakan jenis gas seperti FM-200 atau NAF-S-3 untuk memadamkan api. Manusia tidak boleh menghirup gas yang digunakan pada sistem kimiawi kering karena bisa mematikan.



Gambar 2.8 Sistem pemadam kimia kering

8. Deteksi air, air yang mengalir dari perangkat pendingin udara biasanya turun kebawah lantai yang dapat diangkat (*raised floor*). Sistem deteksi air dapat berada di bawah lantai untuk memperingatkan personil atas pipa saluran air yang macet. Sistem deteksi air juga bisa diletakkan di langit-langit untuk deteksi kebocoran pipa di langit-langit.

2.4.4 Penyimpan Aman

Catatan bisnis penting dan media komputer memerlukan perlindungan terhadap ancaman lingkungan (daya magnet, debu), kebakaran, pencurian, dan kerusakan lainnya. Tempat penyimpanan yang aman di perlukan. Tindakan terbaik adalah menggunakan kabinet berkas tahan api. Catatan bisnis standar di simpan dalam penyimpan kabinet berkas tahan api. Tape penyimpan digital komputer dan media cakram di simpan pada penyimpanan tahan api. Penyimpanan tahan api menyediakan proteksi fisik dan

menjamin temperatur dalam lemari tidak mencapai 54 derajat celsius. Salinan berkas digital dan arsip berkas digital di transfer ke penyimpanan lemari besi.

Fasilitas penyimpanan di luar area kantor (*offsite storage*) menyediakan duplikasi catatan penting dan berkas data cadangan. Fasilitas penyimpanan harus digunakan secara aman dalam pemeliharaan berkas jangka panjang. Praktek standarnya adalah mengirim tape cadangan ke lokasi penyimpanan luar setiap hari atau setiap dua hari. Lokasi penyimpan harus dirancang dengan baik, aman dan dijaga oleh keamanan selama 24 jam. Lokasi harus aman dari api, banjir, dan pencuri. Penyedia jasa penyimpan harus tidak terlalu memperlihatkan fasilitas penyimpanan ini ke orang yang lalu lalang. Kebanyakan fasilitas jasa penyimpan di luar area menyediakan media transportasi yang aman.

Dalam hal media transportasi setiap catatan bisnis dan media magnetic harus dimasukkan dalam kotak dengan baik ketika perjalanan. Isi dalam kotak harus di label dengan baik. Inventori harus di catat terlebih dahulu sebelum dikirim ke penyimpan di luar tanpa terkecuali. Tape cadangan berisi hampir seluruhnya rahasia dari setiap organisasi. Setiap media yang meninggalkan fasilitas utama harus di jaga dalam penyimpanan yang aman setiap saat dan terpantau selama transit. Penggunaan enkripsi diperlukan pada tape cadangan dan penanggung jawab tape cadangan harus mengecek ulang kedatangan media ke fasilitas penyimpanan. Pihak berwenang atas data juga harus bisa melacak lokasi dan status semua berkas data di luar fasilitas utama.

Penyimpanan aman ini diperlukan untuk menyimpan cadangan isi dari direktori aktif. Informasi tersebut meliputi informasi pengguna, informasi group dimana penguna

dikelompokkan, dan hak akses pengguna tersebut untuk mengakses sumber daya terhadap satu atau beberapa pelipat pada server berbagi berkas (*file sharing server*).

2.4.5 Metode Autentikasi

Langkah pertama mendapatkan ijin akses adalah identitas pengguna. Langkah kedua autentikasi akses pengguna. Autentikasi bertujuan untuk menjamin akses diberikan kepada orang yang tepat.

Autentikasi bertujuan untuk mencegah pengaksesan informasi oleh pihak yang tidak berwenang. Autentikasi sendiri terbagi atas tiga tipe, yaitu:

1. Sesuatu yang orang ketahui, contohnya ID log masuk dan kata sandi. Log masuk dan ID masuk haruslah berbeda bagi setiap pengguna. Kata sandi merupakan autentikasi yang lemah karena dapat dilupakan, dibagi, ditemukan dengan pengamatan, dan rusak dalam arti teknikal.
2. Sesuatu yang orang miliki, perbaikan dari tipe pertama dengan mengautentikasi pengguna berdasarkan sesuatu kepemilikan yang unik. Pengguna harus memiliki log masuk ID dengan kata sandi dan sesuatu yang unik pada setiap log masuk. Contoh autentikasi tipe 2 adalah kartu ATM dan PIN, smart card, USB token, token perangkat lunak (*digital certificates*).
3. Perangkat biometrik yang menyimpan karakter fisik, merupakan tipe autentikasi yang berdasarkan ciri fisik yang unik. Perekaman karakteristik dan pencocokan proses dikenal sebagai biometrik. Tipe data biometrik yang digunakan untuk autentikasi meliputi sidik jari tangan, sidik telapak tangan, pindai iris mata, pindai

retina mata, pindai wajah, tanda tangan dinamik, dan pola suara. Penjelasan karakteristik sebagai berikut:

a. Sidik jari tangan, telah dipergunakan sebelumnya sebagai metode untuk identifikasi orang, terutama pelaku kriminai. Dalam biometrik sidik jari tangan dipergunakan untuk autentikasi (bukan identifikasi) pengguna. Informasi mengenai sidik jari tangan direkam dalam basis data biometrik. Basis data hanya merekam karakteristik unik dari sidik jari seperti alur berliku, posisi, pola punggung, jarak alur, persilangan punggung, bentuk pulau, dan gabungan punggung sidik jari. Ketika pengguna akan masuk, detail kecil di identifikasi oleh perangkat keras tambahan dan dibandingkan dengan basis data.
b. Sidik telapak tangan, memiliki ciri yang unik seperti sidik jari tangan. Sidik telapak tangan mengandung sejumlah detail kecil ditambah garis-garis keriput, pola aliran darah, dan bekas luka.
c. Geometri tangan, memilki konsep untuk mengukur detil tangan seseorang dalam gambar tiga dimensi. Teknik yang biasa digunakan adalah meletakkan tangan dalam mesin dengan jari-jari diregangkan diantara pasal metal. Metode lainnya adalah meraih tombol/balok metal ketika sensor mengukur pola aliran darah. Geometri tangan termasuk efektif dan murah.
d. Pindai iris mata, teknologi pemindaian iris mata berdasarkan fitur yang bisa terlihat seperti kerutan, cincin, dan alur dalam cincin warna yang mengelilingi pupil mata. Iris mata bertahan dalam setahun usia sampai seumur hidup. Fitur yang terlihat dan lokasi digabungkan untuk membentuk pola kode digital.

e. Pindai retina mata, retina mata mengandung pola unik dari pembuluh darah halus dan pembuluh arteri yang memancarkan cahaya. Perubahan pada retina dapat terjadi selama kehidupan seseorang. Beberapa perubahan tersebut dapat menunjukkan serangan penyakit pada kondisi terakhir seseorangan, seperti penyakit strok atau kencing manis (*diabetes*). Pengguna harus memperhatikan kondisi kesehatannya atau terjadi kemungkinan pelanggaran hak akses.

f. Pindai wajah, teknologi pindai wajah menggunakan urutan gambar diam direkam dengan kamera video. Teknologi ini menggunakan pengukuran tiga dimensi dari fitur wajah, termasuk posisi kelopak mata, hidung, bukaan mulut, dan pengukur pola panas. Fitur data kemudian di ekstrak dari bentuk gambar menjadi bentuk pola wajah digital.

g. Tanda tangan dinamik, merupakan pola kebiasaan dari data biometrik. Tanda tangan pengguna di monitor untuk durasi waktu, tekanan, dan teknik. Keuntungannya biayanya adalah implementasinya murah. Kekurangannya adalah banyak individu yang tidak menuliskan tanda tangannya secara konsisten.

h. Pola suara, penggunakan pengenal pola suara (*voice pattern*) merupakan metode yang murah untuk identifikasi seseorang dari caranya berbicara. Pengenal pola suara berbeda dengan pengenal bicara (*speech recognition*). Pengenal bicara merangkai bunyi suara kedalam kata. Analisis pola suara memeriksa karakter tekanan suara, nada, dan durasi suara. Suara seseorang di analisis untuk karakter suara unik, nada, perubahan nada suara, dan kecepatan pengucapan. Metode tipikal yang digunakan adalah memerintahkan pengguna untuk mengulang frasa

khusus yang tertentu. Karakteristik dari frasa tersebut di konversi menjadi pola digital. Pengenal pola suara lebih mudah dan kurang akurat dibandingkan jenis biometrik lain. Autentikasi suara bisa di bohongi dengan rekaman suara orang tersebut melalui pemutar audio.

Manajemen sistem biometrik harus mengikuti tujuh fase siklus yaitu fase kemungkinan digunakannya biometrik, kebutuhan biometrik, pemilihan sistem, konfigurasi sistem, implementasi biometrik, setelah implementasi, pembuangan sistem biometrik. Permasalahan dengan sistem biometrik adalah bagaimana hasil biometrik digunakan. Apakah sistem biometrik diharapkan untuk menyediakan identifikasi atau autentikasi. Pengguna juga memiliki kekhawatiran terhadap isu kebersihan terhadap kontak fisik individu yang bergantian pada perangkat biometrik. Tingkat kesalahan juga terdapat di setiap sistem yang automatis. Beberapa jenis kesalahan yang bisa terjadi pada sistem biometrik adalah :

1. Pendaftaran, setiap pengguna harus memiliki contoh untuk sistem biometrik selama proses pendaftaran. Contoh tersebut bisa gagal di terima oleh sistem. Proses pendaftaran harusnya membutuhkan waktu 2 sampai 5 menit, selebihnya dapat menjengkelkan pengguna.
2. Kegagalan pendaftaran (*failure to enroll*), walaupun jarang data pengguna dapat tidak diterima oleh sistem. Hal ini bisa terjadi akibat kualitas gambar, kalibrasi, masalah sistem, atau pemindai tidak meng interpretasikan ketidak normalan fisik seseorang.

3. Penolakan yang salah (*false rejection*), pengguna yang sah dapat di tolak dan gagal untuk di autentikasi. Kegagalan untuk menerima pengguna yang sah di kenal dengan tingkat penolakan salah (*false rejection rate* atau FRR) kekeliruan tipe 1. Hal ini dianggap kekeliruan tipe pertama karena merupakan tipe kekeliruan yang umum terjadi.
4. Penerimaan yang salah (*false acceptance*), hal ini mungkin terjadi dimana sistem mengijinkan akses kepada individu yang seharusnya di tolak, orang yang salah di autentikasi. Hal ini dirujuk sebagai tingkat penerimaan salah (*false acceptance rate* atau FAR) tipe ke dua.
5. Kekeliruan seimbang/simpangan, setiap sistem memiliki tahap keseimbangan yang sulit antara kecepatan alat melampaui efisiensi. Pada biometrik keseimbangan ini dirujuk sebagai tingkat kekeliruan sama (*equal error rate*) atau tingkat kekeliruan persimpangan (*crossover error rate*).
6. Tingkat keluaran (*throughput rate*), salah satu tantangan adalah berapa banyak sampel orang yang bisa diproses oleh sistem, dan tetap memiliki akurasi yang masuk akal. Keluaran proses yang rendah (lambat) mungkin bisa di terima dalam situasi resiko tinggi. Keluaran proses tinggi (cepat) lebih baik digunakan dalam situasi yang beresiko kecil seperti kumpulan sidik jari pengunjung memasuki taman hiburan.

2.4.6 Proteksi Akses Jaringan

Setiap komputer jaringan cenderung mengalami masalah kontrol akses. Tantangannya adalah menyediakan akses pengguna yang sah dan menghalangi akses dari yang lainnya. Ada dua teknologi umum untuk proteksi akses jaringan yaitu:

1. Kerberos yang merupakan protokol yang menyediakan autentikasi timbal balik antara klien dengan server dan antar server. Direktori aktif menggunakan kerberos sebagai sistem autentikasi jaringan yang di pilih. Ketika pengguna log masuk ke ranah dengan menggunakan kata sandi log masuk, komputer mencari lokasi server direktori aktif dan layanan autentikasi kerberos. Kerberos kemudian menerbitkan tiket untuk mengizinkan akses ke layanan jaringan. Tiket tersebut mengandung data yang terenkripsi, termasuk kata sandi yang terenkripsi, yang mengkonfirmasi identitas pengguna terhadap layanan. Proses Kerberos dapat dijelaskan sebagai berikut :
   a. Pengguna di autentikasi ke perangkat lunak anjungan kerja Kerberos. Autentikasi bisa melalui kata sandi atau metode biometrik
   b. Perangkat lunak anjungan kerja di autentikasi ke server Kerberos
   c. Tiket akses Kerberos di kirim ke anjungan kerja, di tandai kunci enkripsi berbasis pada anjungan kerja. Kesemua server-server dalam jaringan menerima tiket yang sama untuk menjamin anjungan kerja akses ke server sumber daya
   d. Pengguna secara automaris ditandai untuk boleh akses ke semua server
2. *Firewall* jaringan, merupakan tindakan pengamanan terhadap serangan yang bisa masuk melalui berbagai layanan port pada jaringan. *Firewall* sendiri adalah sebuah

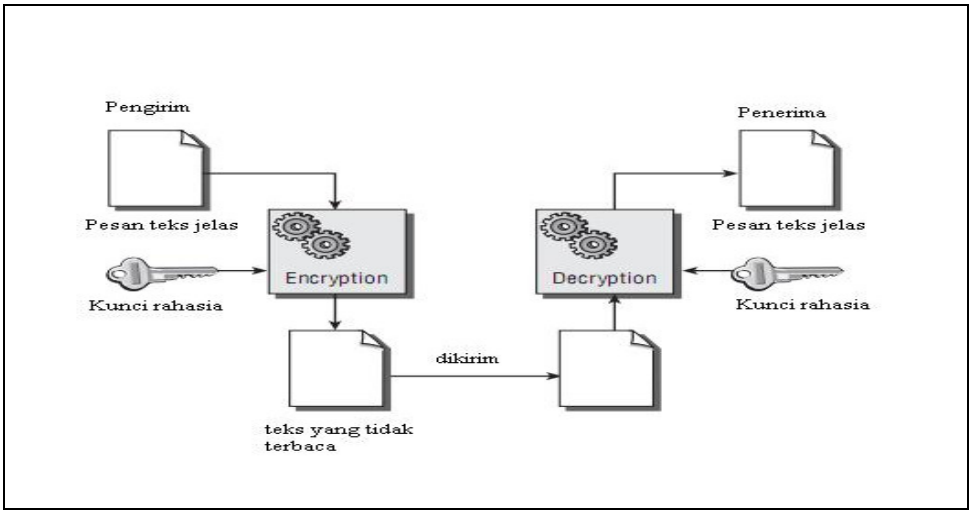
sistem atau perangkat yang mengizinkan lalu lintas jaringan yang dianggap aman untuk melaluinya dan mencegah lalu lintas jaringan yang tidak aman. *Firewall* sendiri memiliki kelebihan dan kekurangan. Kelebihannya adalah mengurangi akses dari luar ke dalam jaringan internal. Kekurangannya adalah selalu ada celah untuk lalu lintas jaringan diizinkan melaluinya. *Firewall* juga tidak melindungi modem atau akses poin lainnya. *Firewall* sendiri dapat di konfigurasi secara tidak tepat atau diakali secara teknikal. *Firewall* tidak menjamin keamanan. Konsep *firewall* sendiri menciptakan kesadaran yang salah terhadap keamanan. *Firewall* jaringan telah mengalami beberapa generasi perbaikan. Generasi pertama hanya sebuah perangkat router dengan akses list kuno yang menspesifikasikan menuju tujuan dan asal alamat jaringan. Pihak penyerang menjadi lebih canggih, dan begitu juga kebutuhan untuk perangkat *firewall* yang lebih baik.

2.4.7 Metode Enkripsi

Sistem enkripsi menyediakan metode untuk konversi teks jelas dan terbaca ke kalimat yang tak bermakna. Sistem dekripsi menkonversi balik kalimat tak bermakna tersebut menjadi pesan yang bisa dibaca. Ada tiga tipe dasar sistem enkripsi, sistem enkripsi kunci rahasia, sistem enkripsi kunci umum yang keduanya berbentuk digital (berkas) serta tanda tangan digital (*digital signature*).

Sistem enkripsi kunci rahasia menggunakan kunci rahasia, yang di bagikan antara pengirim yang berwenang dan pengirim yang tertuju. Sistem kunci rahasia memiliki dua komponen dasar. Komponen pertama adalah algoritma matematis untuk mengacak dan

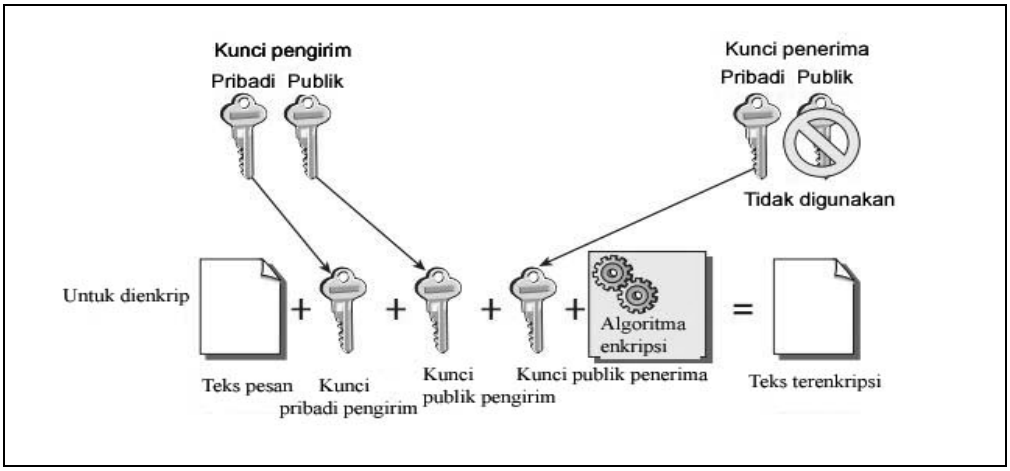
menguraikan pesan (enkripsi dan dekripsi). Komponen kedua adalah kunci matematika digunakan sebagai pengacak dalam algoritma enkripsi. Kunci rahasia tunggal di bagi antara pengirim dan penerima di sebut sebagai kriptografi kunci simetrik. Hal ini terlihat pada Gambar 2.9.



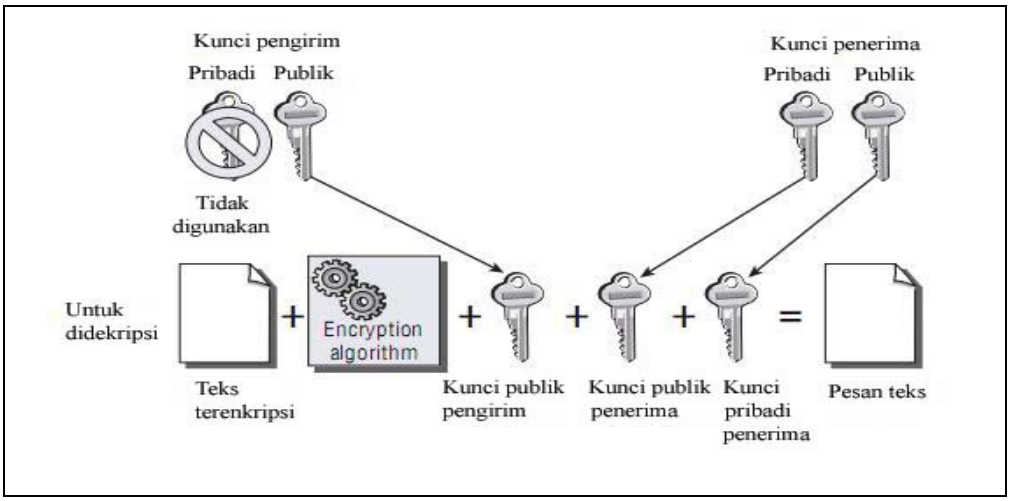
Gambar 2.9 Alur emkripsi dan dekripsi kunci rahasia

Kunci publik disebut juga kriptografi asimetrik. Rancangan ini menggunakan pasangan kunci terpisah untuk enkripsi dan dekripsi. Pasangan kunci tersebut dibentuk dari kunci rahasia yang dijaga oleh pemilik dan kunci public kedua di distribusikan secara bebas. Kedua kunci tersebut berhubungan satu dengan yang lainnya secara matematis. Kunci rahasia dan kunci umum dihasilkan angka prima yang di perluas. Kekuatan kriptografi kunci umum bergantung pada algoritma yang dipergunakan dan besarnya kunci enkrips. Untuk mengenkripsi pesan, pengirim harus menggunakan kunci rahasia, kunci publik mereka, dan ditambah kunci publik dari pengirim yang dituju. Hal ini terlihat pada Gambar 2.10. Dalam proses dekripsi, pengirim menggunakan kunci rahasia dan kunci umum mereka, ditambah kunci umum si pengirim. Konsep dasar yang

diperlukan hanyalah tiga kunci untuk membuka data (dekripsi). Jika kedua nilai tersebut hilang maka dekripsi berkas menjadi tidak mungkin (lihat Gambar 2.11)



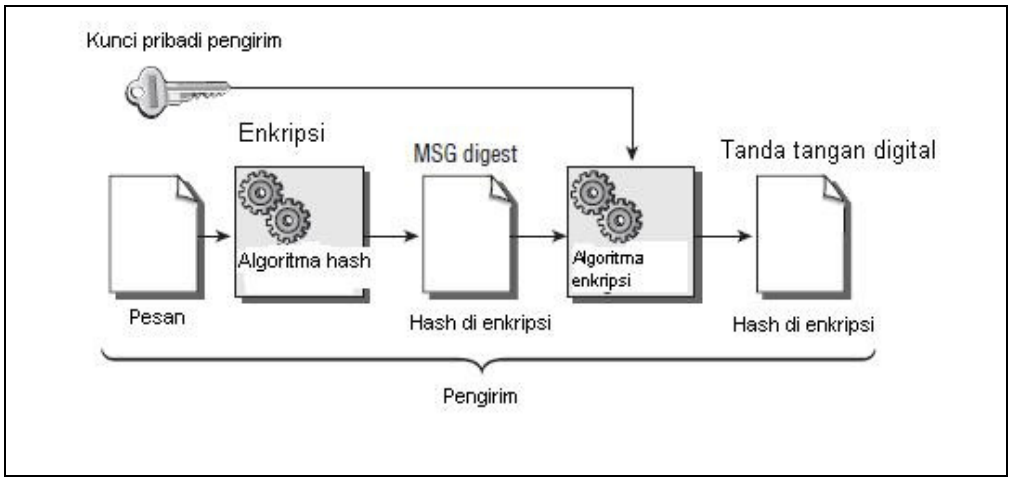
Gambar 2.10 Enkripsi menggunakan sistem kunci public



Gambar 2.11 Dekripsi menggunakan sistem kunci public

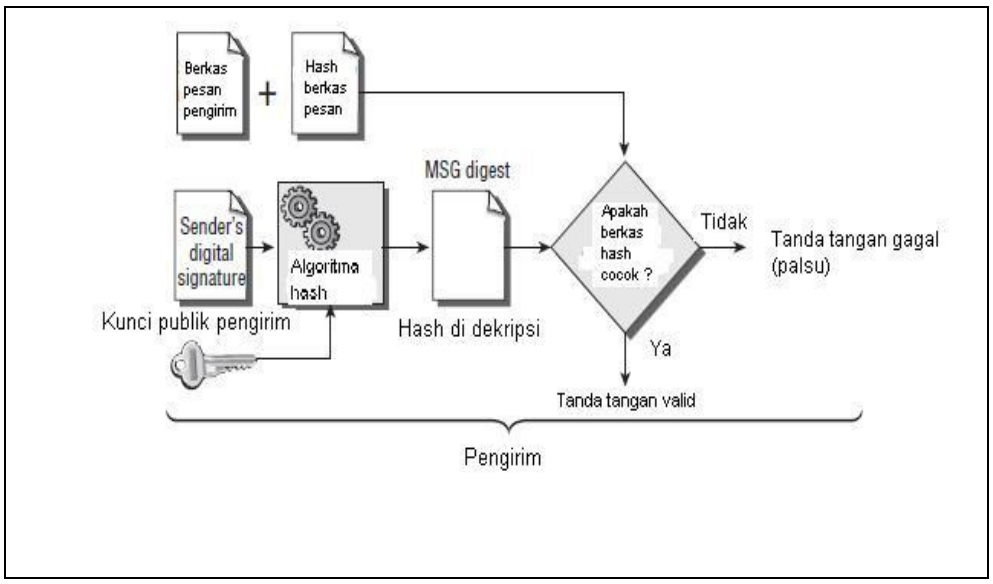
Tanda tangan digital dibuat sebagai versi eletronik tanda tangan seseorang. Tujuannya adalah untuk mengindikasikan bahawa pesan telah dikirim dengan identitas individu yang unik. Tanda tangan digital biasa digunakan untuk penanda dokumen e-

mail maupun dokumen pengolah kata (misalnya Microsoft office). Tanda tangan digital di jalankan dengan utilitas *hash* terhadap berapapun jumlah berkas akan menghasilkan keluaran 120-bit atau 160-bit enkripsi. *Hash* merupakan prosedur proses deterministik yang mengambil sembarang blok dari data dan mengembalikan jumlah nilai *string* bit yang pasti (*fixed-size bit string*). Proses membangun berkas *hash* dan tanda tangan digital seperti yang ditunjukkan oleh Gambar 2.12.



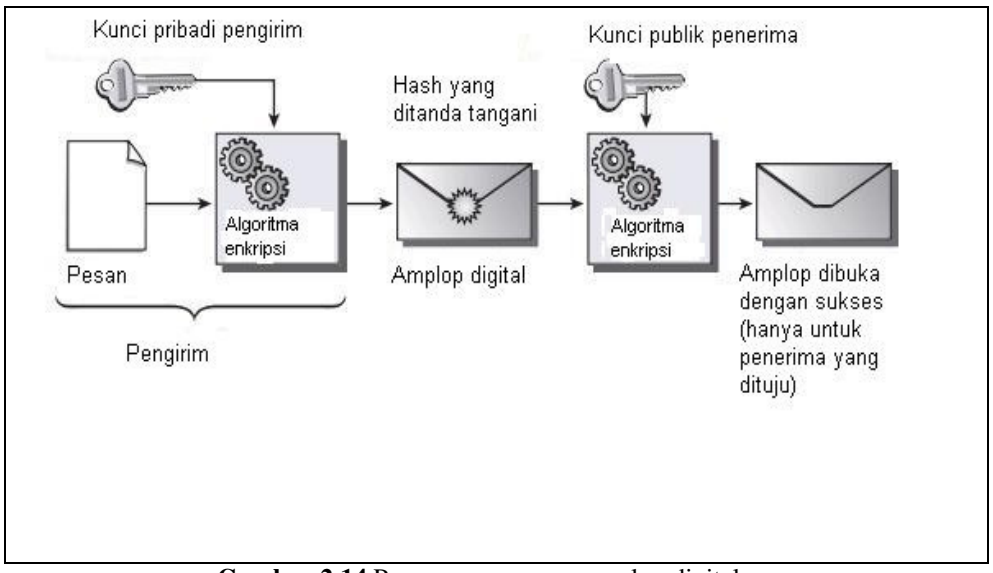
Gambar 2.12 Proses membangun tanda tangan digital

Tanda tangan digital dilampirkan ke berkas pesan, dan keduanya di kirim ke penerima. Penerima harus menggunakan berkas pesan, berkas tanda tangan digital, dan kunci publik pengirim untuk menguji keabsahan tanda tangan tersebut. Tanpa pengujian tanda tangan digital, tidak akan ada indikasi kewenangan telah sesuai. Gambar 2.13 memperlihatkan proses verifikasi tanda tangan digital.



Gambar 2.13 Verifikasi tanda tangan digital

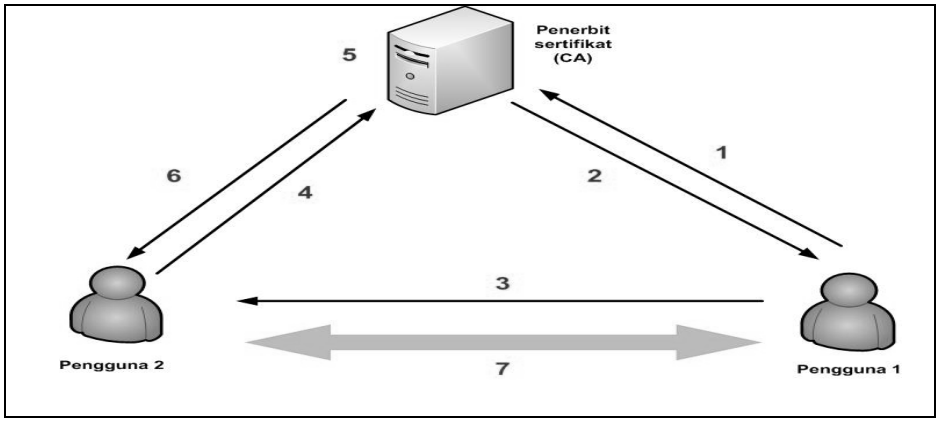
Ada metode baru untuk mengirim pesan yang di enkripsi berikut kunci untuk membukanya. Proses ini menggunakan amplop digital. Pesan yang di sandikan (*encrypted*) bersamaaan dengan kunci sesi. Kunci sesi adalah waktu kedua sandii menggunakan kunci publik si penerima pesan. Setelah proses transmisi, penerima dapat membuka (*decrypt*) dengan menggunakan kunci pribadi si penerima, dan membuka kembali dengan menggunakan kunci publik penerima. Dua langkah penyandian memastikan tidak ada seorangpun yang bisa membuka kunci ketika dalam perjalanan transmisi pesan. Gambar 2.14 memperlihatkan proses penggunaan amplop digital.



Gambar 2.14 Proses penggunaan amplop digital

2.4.8 Infrastruktur Kunci Publik

Infrastruktur kunci publik merupakan implementasi dari berbagai teknik kriptografi yang bertujuan untuk mengamankan data, memastikan keaslian data maupun pengirimnya dan mencegah penyangkalan. Proses membagi file terenkripsi diantara beragam pihak dirancang untuk menyediakan tingkat ketepercayaan dan keaslian identifikasi antara pengguna. Ada 4 komponen dasar infrastruktur kunci umum pertama penerbit sertifikat, kewenangan registrasi, daftar penolakan, dan pernyataan pelaksanaan. Salah satu contoh proses infrastruktur kunci publik seperti yang ditunjukkan oleh Gambar 2.15.



Gambar 2.15 Proses infrastruktur kunci publik

Penjelasan proses infrastuktur pada Gambar 2.15 dapat diuraikan sebagai berikut:

1. Pengguna 1 meminta penerbit sertifikat untuk menerbitkan sertifikat atas nama pengguna 1.
2. Penerbit sertifikat memvalidasi identitas pengguna 1 dan menerbitkan sertifikat untuk pengguna 1.
3. Pengguna 1 memberikan sertifikat yang berisi identitas pengguna 1 kepada pengguna 2.
4. Pengguna 2 tidak mengenal pengguna 1 sehingga pengguna 2 menanyakan ke penerbit sertifikat untuk memeriksa identitas pengguna 1.
5. Penerbit sertifikat memeriksa keabsahan sertifikat pengguna 1 (tidak pernah berubah, kadaluarsa dan pemeriksaan lainnya).
6. Penerbit sertifikat memberitahukan kepada pengguna 2 bahwa sertifikat pengguna 1 adalah sah.
7. Pengguna 2 kemudian mempercayai identitas pengguna 1 adalah memang benar terpercaya.

2.4.9 Protokol Keamanan Jaringan

Dalam dunia perdagangan/transaksi secara on-line (*e-commerce*) harus di bangun dalam suatu protokol keamanan jaringan untuk keamanan. Protokol keamanan jaringan untuk bertransaksi terbagi tiga :

a. PGP (*Pretty Good Privacy*) bekerja pada tingkat ketujuh pada lapisan OSI menggabungkan kelebihan kunci umum dan kriptografi simetris. Distribusi kunci dan performa juga semakin meningkat tanpa mengorbankan keamanan. Menyediakan solusi untuk distribusi kunci dan isu transmisi data ketika menggunakan enkripsi simetris. PGP memiliki kelemahan sebagai proses kompleks dan konsepnya terkadang susah dimengerti. Kedua pihak (pengirim dan penerima) harus bisa menggunakan PGP.

b. SSL (*Secure Socket Layer*) banyak digunakan pada situs web untuk sesi HTTP dan memiliki beberapa keuntungan. Pada sisi enkripsi isi pesan dari pengirim dan penerima terlindungi dari pembongkaran. Di sisi kewenangan pelayan, komputer klien yang menyimpan catatan sertifikat digital SSL dapat memastikan autentikasi tidak berubah sewaktu-waktu. Di sisi seting untuk SSL juga tidak merepotkan. Kelemahannya menaikkan beban komputer karena proses komunikasi enkripsi dan dekripsi menaikkan intensif proses unit pemrosesan pusat (CPU) dibandingkan komunikasi tanpa enkripsi. Identifikasi klien juga tidak tersedia dan memerlukan beberapa tambahan ektensi di instal di sisi klien.

c. HTTPS (*Hypertext Transfer Protocol Secure*) merupakan kombinasi HTTP dengan protokol SSL. Hal ini untuk menyediakan proses enkripsi dan mengamankan

identifikasi yang aman pada server. Koneksi HTTPS umum digunakan untuk transaksi pembayaran secara on-line dari web dan transaksi sensitif pada sistem informasi perusahaan.

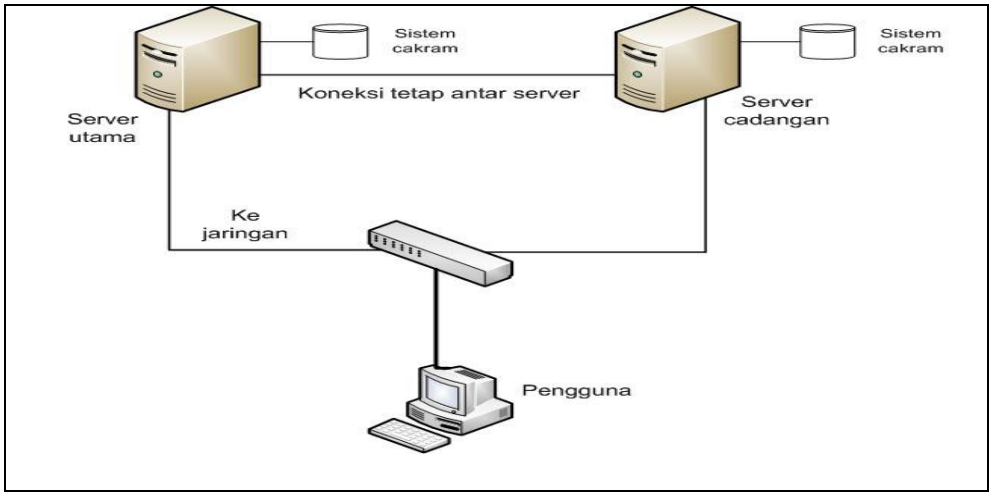
d. IPSec (*IP Security*) merupakan protokol menggunakan AH (*authentication header*) dan ESP (*encapsulated security payload*) dan bekerja di tingkatan ketiga (jaringan) pada model lapisan OSI (*Open System Interconnection*). Secara teknis, IPSec terdiri atas dua bagian utama. Bagian pertama mendeskripsikan dua protokol untuk penambahan depan (*header*) pada paket yang membawa pengenal keamanan (*security identifier*), data mengenai kontrol integritas (*integrity control*), dan informasi keamanan lain. Bagian kedua berkaitan dengan protokol pembangkitan dan distribusi kunci. Dua protokol untuk penambahan depan (*header*) adalah yang pertama AH yang menyediakan integritas data, autentikasi awal data dan perlindungan terhadap serangan berulang. Kedua ESP menyediakan layanan yang disediakan oleh AH ditambah layanan data kerahasiaan dan kerahasiaan aliran data. Karena IPSec bekerja pada tingkat jaringan maka sesuai untuk mengamankan lalu lintas pada waktu nyata seperti VoIP (*Voice over IP*). Kelemahannya akan menimbulkan kesulitan jika bekerja dari luar lokasi kantor dan ingin akses ke jaringan kantor, karena batasan dari firewall perusahaan.

2.4.10 Rancangan Untuk Duplikasi

Ada banyak cara melindungi aset informasi dari sekadar enkripsi. Jaringan komunikasi harus di rancang dengan menggunakan rute cadangan seperti rute alternatif

komunikasi. Rute alternatif ini akan digunakan jika rute utama mengalami kegagalan dari pihak penyedia jaringan komunikasi *broadband* (ISP). Hal ini bisa di gunakan pada jaringan area lokal atau jaringan area luas untuk menjaga ketersediaan informasi tetap bisa diakses oleh pengguna..

Teknik lain untuk menjamin ketersediaan dan integritas aset informasi adalah penggunaan server cadangan yang menduplikasi semua proses dan transaksi dari server utama. Server cadangan ini dikenal sebagai server dengan ketersediaan tinggi (*high-availability servers*). Salah satu server bertindak sebagai server utama dan yang kedua sebagai cadangan. Server cadangan (*failover server*) berjalan pada di belakang layar sampai server utama mengalami kegagalan untuk beroperasi atau sistem tidak tersedia untuk diakses *(downtime)*. Server cadangan akan mengambil alih tanggung jawab keseluruhan proses jika server utama gagal dengan apapun penyebabnya. Perkembangan teknologi virtualisi juga memungkinkan untuk memindahkan kinerja server utama ke server cadangan secara automatis begitu server utama tidak bisa diakses. Rancangan tersebut seperti yang di tunjukkan pada Gambar 2.16.



Gambar 2.16 Topologi server ketersedian tinggi

Sistem cadangan tape dapat membantu memulihkan data dalam kondisi kegagalan sistem cakram yang menyebabkan hilangnya data berharga. Untuk memulihkan data memerlukan adanya penambahan periode waktu dimana sistem tidak tersedia. Salah satu solusi masalah ini adalah implementasi redundansi cakram keras. RAID (*Redundant Array of Independent/Inexpensive Disk*) menyediakan metode yang bagus untuk melindungi aset informasi.

2.5 Peralatan Analisis Keamanan

Peralatan analisis keamanan yang digunakan adalah *Certified Information System Auditor* (CISA) dan metode matriks keputusan Stuart Pugh. CISA merupakan sertifikasi audit profesional yang di sponsori oleh ISACA (*Information System Audit and Control Association*). CISA sendiri bertujuan untuk:

a. Mengembangkan dan memelihara suatu alat yang bisa digunakan untuk evaluasi kompetensi dalam melakukan audit sistem informasi.

b. Menyediakan mekanisme untuk mengawasi audit sistem, kontrol, dan keamanan informasi.
c. Menyediakan kriteria untuk memberikan bantuan ke pihak manajemen dalan seleksi personil dan pengembangan.

Pada CISA terdapat berbagai *best practice* untuk melakukan audit sistem informasi dan pembahasan mengenai aspek-aspek yang akan mendukung untuk melakukan audit sistem informasi. Aspek-aspek tersebut antara pembahasan mengenai proses audit sistem, struktur pengendali teknologi informasi, teknologi jaringan, manajemen siklus hidup perangkat lunak, membawakan layanan teknologi informasi, proteksi aset informasi, pemulihan bencana, dan kelangsungan bisnis.

Metode matrik keputusan Stuart Pugh merupakan suatu teknik kuantitatif yang digunakan sebagai urutan peringkat pilihan multi dimensi dari sekumpulan pilihan. Matriks keputusan tersebut merupakan kumpulan kriteria dimana pilihan yang potensial dapat di pisahkan, di hitung, dan dijumlah total yang kemudian menjadi urutan prioritas. Keunggulan pendekatan matrik ini terhadap pengambil keputusan adalah pendapat yang subjektif tentang suatu alternatif pilihan terhadap pilihan lain dapat dijadikan lebih objektif.

Metode matriks keputusan dalam tugas akhir ini dirancang untuk melakukan penilaian terhadap 3 komponen keamanan yaitu kerahasiaan, integritas, dan ketersediaan. Masing-masing komponen memiliki bobot maksimal bernilai 5. Setiap parameter dinilai berdasarkan 5 skala penilaian seperti yang ditunjukkan pada Tabel 2.1.

Tabel 2.1 Skala penilaian

Nilai	Arti
1	Jelek sekali
2	Jelek
3	Cukup
4	Bagus
5	Bagus sekali

BAB III

ANALISIS

3.1 Manajemen Keamanan Informasi

Manajemen keamanan informasi bertujuan untuk memastikan kerahasiaan, integritas, dan ketersediaan sumber daya komputer untuk akses informasi. Informasi sendiri terbagi atas informasi publik (informasi yang disetujui untuk konsumsi publik), informasi sensitif (informasi yang hanya untuk pihak tertentu tetapi tidak semua), informasi internal (informasi prosedur operasi dan catatan kepegawaian), informasi rahasia (informasi yang tidak boleh di bagi diluar organisasi). Penilaian mengenai manajemen keamanan informasi terlihat pada Tabel 3.1.

Tabel 3.1 Matriks keputusan manajemen keamanan informasi

Nomor	Kriteria	Kerahasiaan		Integritas		Ketersediaan		Total Skor
	Bobot	5		5		5		
		Skor	Jumlah	Skor	Jumlah	Skor	Jumlah	
	Parameter							
1.	Kepala keamanan informasi	3	15	2	10	3	15	40
2.	Kepala privasi informasi	4	20	1	5	1	5	30
3.	Manajer keamanan informasi	5	25	5	25	5	25	75

Penjelasan matriks keputusan manajemen keamanan informasi pada Tabel 3.1 dapat diuraikan sebagai berikut:

1. Kepala keamanan informasi mendapatkan total nilai 40. Dalam komponen kerahasiaan kepala keamanan informasi mendapatkan nilai 3 dikarenakan bertugas untuk memaksakan kebijakan keamanan dalam lingkungan. Untuk komponen integritas mendapatkan nilai 2 karena tidak bertugas untuk menjaga integritas data. Komponen ketersediaan mendapatkan nilai 3 karena memiliki tugas menjamin tingkat autorisasi kepada petugas keamana sistem informasi namun tidak dapat menjamin ketersediaan informasi.
2. Kepala privasi informasi mendapatkan total nilai 30. Pada komponen kerahasiaan mendapatkan nilai 4 dikarenakan memiliki tugas utama menjaga kerahasiaan informasi para pelanggan dan karyawan. Komponen integritas mendapatkan nilai 1 dikarenakan posisi ini tidak berwenang terhadap integritas informasi. Komponen ketersedian juga mendapat nilai 1 dikarenakan posisi ini tidak bertanggung jawab atas ketersediaan informasi.

3. Manajer keamanan sistem informasi mendapatkan total nilai 75. Pada komponen kerahasiaan mendapatkan nilai 5 karena bertugas utama sebagai penyelia analisa sistem keamanan informasi harian yang bertanggung jawab penuh terhadap kerahasiaan informasi perusahaan. Pada komponen integritas mendapatkan nilai 5 karena posisi ini bertanggung jawab penuh terhadap integritas data dan memastikan tingkat autorisasi atas data berjalan normal. Pada komponen ketersediaan mendapatkan nilai 5 dikarenakan posisi ini bertanggung jawab atas ketersediaan informasi dengan menyusun strategi teknis seperti strategi teknis cadangan data dan sistem ketika terjadi kehilangan/kerusakan sistem atau data.

Manajer keamanan informasi mendapatkan total skor tertinggi dengan nilai 75. Pada perusahaan yang diteliti tidak ditemukan adanya kepala keamanan informasi, dan kepala privasi informasi yang bertanggung jawab terhadap keamanan informasi data karyawan dan pelanggan.

3.2 Peran Kewenangan Terhadap Data

Peran kewenangan data terbagi atas tiga yaitu pemilik data, pengguna data, dan petugas data yang fungsinya telah dijelaskan pada sub bab 2.4.2. Penilaian mengenai manajemen keamanan informasi terlihat pada Tabel 3.2.

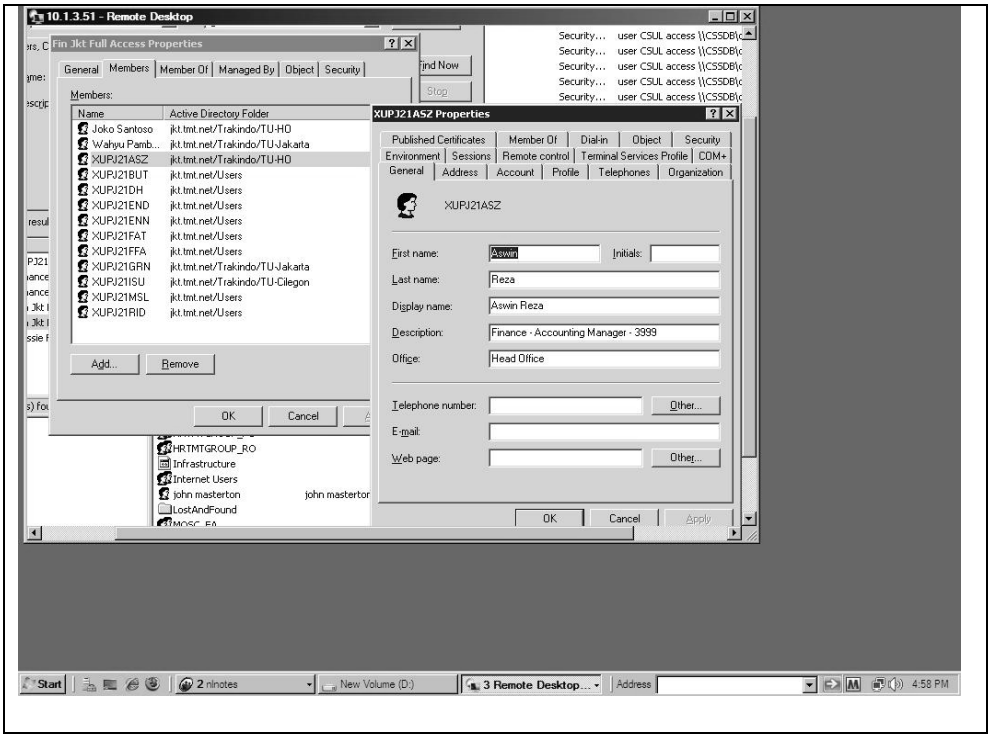
Tabel 3.2 Matriks keputusan peran kewenangan terhadap data

Nomor	Kriteria	Kerahasiaan		Integritas		Ketersediaan		Total Skor
	Bobot	5		5		5		
		Skor	Jumlah	Skor	Jumlah	Skor	Jumlah	
	Parameter							
1.	Pemilik data	4	20	5	25	1	5	50
2.	Pengguna data	3	15	3	15	1	5	35
3.	Petugas data	5	25	5	25	5	25	75

Penjelasan matriks keputusan peran kewenangan terhadap data pada Tabel 3.2 dapat diuraikan sebagai berikut:

1. Pemilik data pada komponen kerahasiaan mendapatkan nilai 4 dikarenakan memiliki kewenangan untuk menetapkan klasifikasi dan penetapan kontrol atas informasi yang sesuai. Pada komponen integritas mendapat nilai 5 karena pemilik data bertanggung jawab atas isi data dan menentukan penggunaan data tersebut. Komponen ketersediaan mendapat nilai 1 karena tidak memiliki kewenangan atas ketersediaan data. Contoh pemilik data dapat dilihat pada Gambar 3.1.
2. Pengguna data mendapatkan nilai 3 pada komponen kerahasiaan karena pengguna data harus menjaga kerahasiaan data dan melaporkan aktifitas yang tidak berwenang terhadap data. Pada komponen integritas mendapatkan nilai 3 karena pengguna harus mengikuti standar penggunaan data dan sesuai dengan kontrol dan hak akses yang diberikan pemilik data. Pada komponen ketersediaan data mendapatkan nilai 1 karena tidak memiliki wewenang untuk ketersediaan. Contoh pengguna data dapat dilihat pada Gambar 3.2.

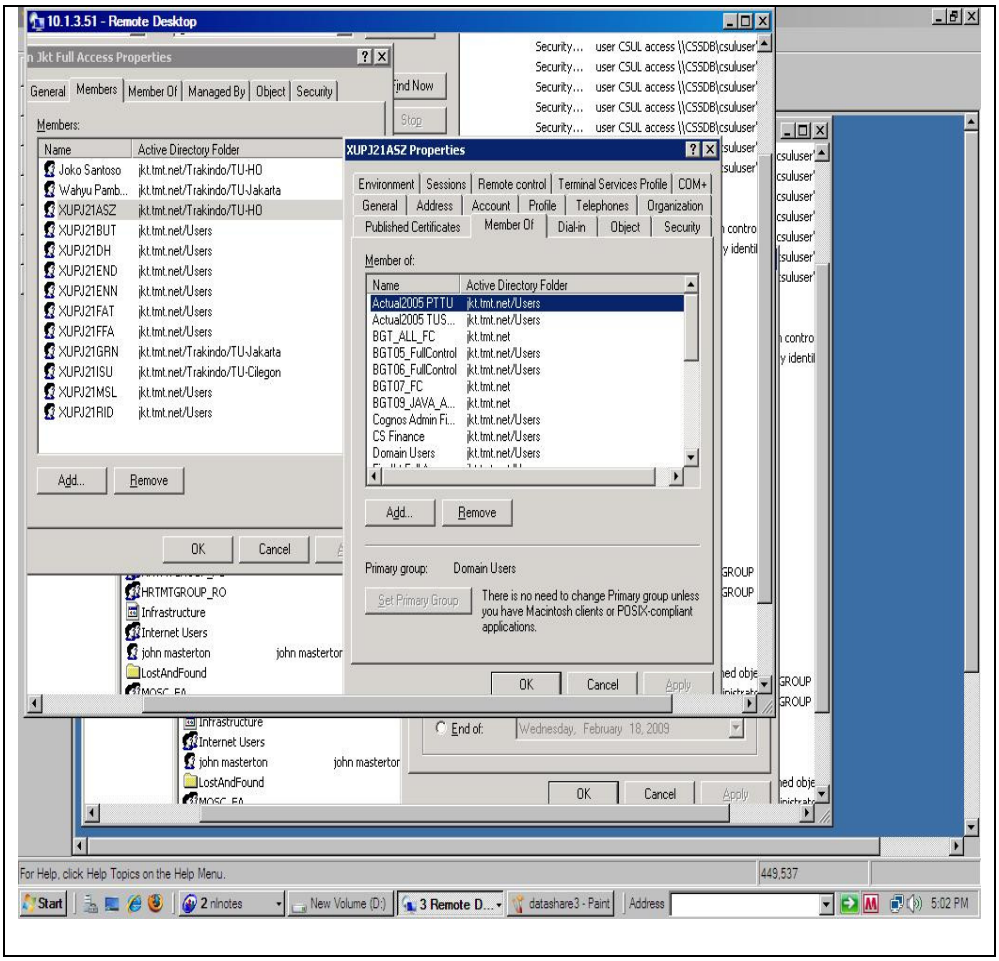
3. Petugas data mendapatkan nilai 5 untuk kerahasiaan karena berwenang untuk memonitor keamanan data atas penyalah gunaan, implementasi kontrol atas klasifikasi informasi, dan administrasi kontrol akses pengguna. Pada komponen integritas mendapat nilai 5 karena bertanggung jawab atas integritas data melalui kontrol proses. Pada komponen ketersediaan mendapat nilai 5 karena bertugas untuk mengamankan data dari terjadinya kehilangan, dan selalu ada jika terjadi permasalahan teknis terhadap data. Petugas data dalam direktori aktif adalah administrator yang bertanggung jawab secara teknis terhadap kerahasiaan, integritas, dan ketersediaan informasi. Secara administratif petugas data adalah atasan langsung/manajer masing-masing pengguna. Contoh petugas data dapat dilihat pada Gambar 3.3.



Gambar 3.1 Contoh pemilik data

Penjelasan contoh pemilik data pada Gambar 3.1 dapat diuraikan sebagai berikut:

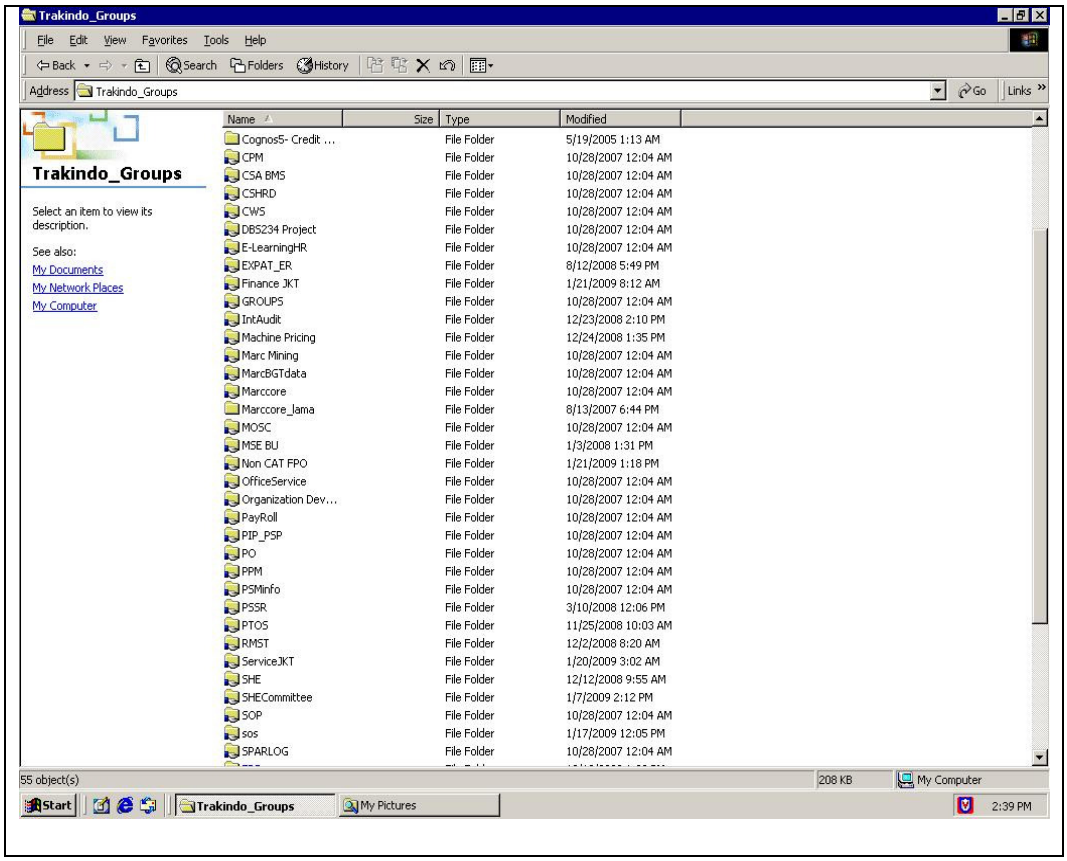
- Pengguna Aswin Reza merupakan pemilik data pada berkas pelipat (folder) dengan nama Fin Jkt (Finance Jakarta). Pengguna Aswin Reza merupakan seorang manajer finance yang bertanggung jawab untuk cabang Jakarta. Pengguna tersebut memiliki akses penuh yang berarti memiliki hak untuk menambah, menghapus, dan memberikan akses hanya terhadap pelipat Fin Jkt saja.



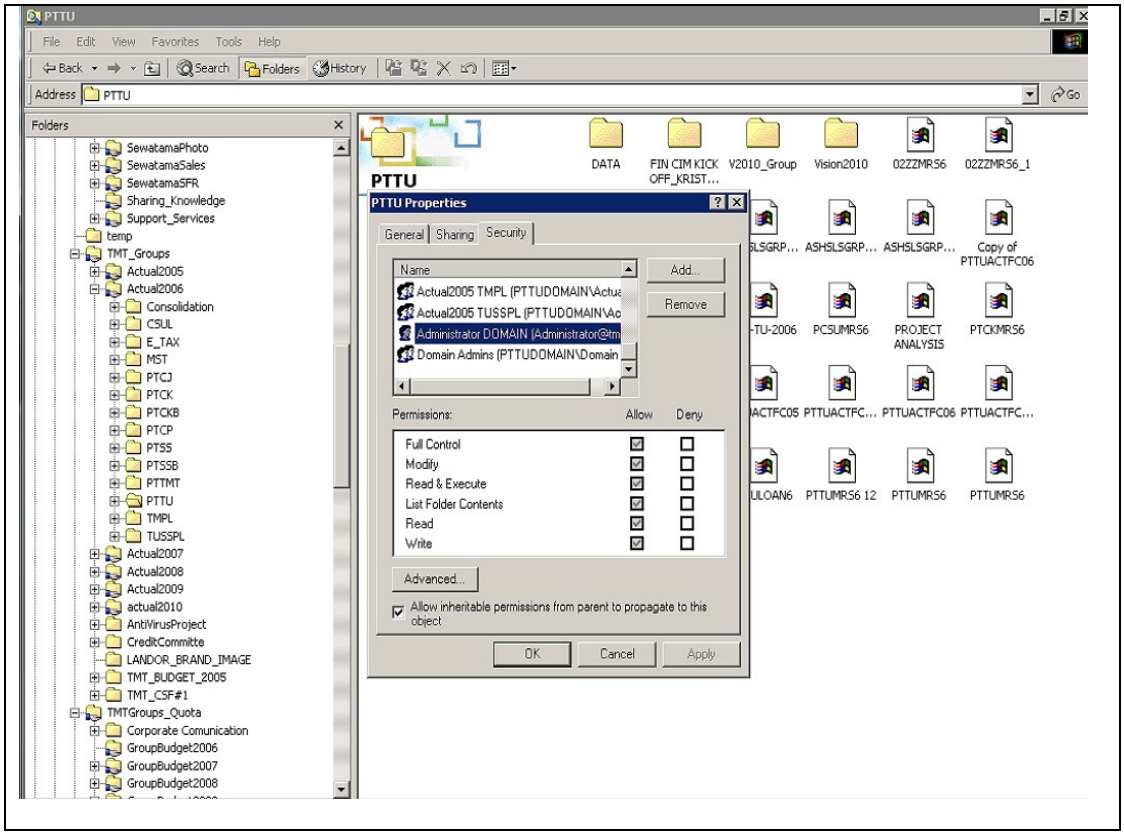
Gambar 3.2 Contoh pengguna data

Penjelasan contoh pengguna data pada Gambar 3.2 dapat diuraikan sebagai berikut:

1. Pengguna Aswin Reza juga merupakan pengguna data untuk meng akses pelipat lain namun bukan pemilik data. Pengguna Aswin Reza juga merupakan pengguna data untuk pelipat dengan nama Actual2005 PTTU, Actual2005 TUSRA, BGT_ALL_FC (budget all finance controller), BGT07_FC (budget tahun 2007 finance controller) namun bukan pemilik data dari pelipat tersebut.
2. Pelipat tersebut berisikan data-data yang diperlukan bagi para manajemen keuangan (finance manager). Semua pelipat tersebut berada pada satu server berbagi (*file sharing server*) yang setiap pelipat di berikan hak akses melalui direktori aktif seperti yang ditunjukkan oleh Gambar 3.3.



Gambar 3.3 Pelipat pada server berbagi



Gambar 3.4 Petugas data pada pelipat berbagi

Petugas data mendapatkan skor tertinggi dengan nilai 75. Pemilik, pengguna dan petugas data merupakan komponen pada direktori aktif.

3.3 Kontrol Lingkungan

Kontrol lingkungan diperlukan untuk menjaga tetap beroperasinya server pengatur ranah utama (PDC) serta pengatur ranah cadangan (BDC). Kontrol lingkungan yang buruk dapat mempengaruhi kinerja server pengatur ranah. Hal tersebut dapat menimbulkan permasalahan di komputer-komputer pengguna yang memerlukan akses

terhadap sumber daya untuk mendapatkan informasi. Tabel 3.3 memperlihatkan penilaian mengenai kontrol lingkungan.

Tabel 3.3 Matriks keputusan kontrol lingkungan

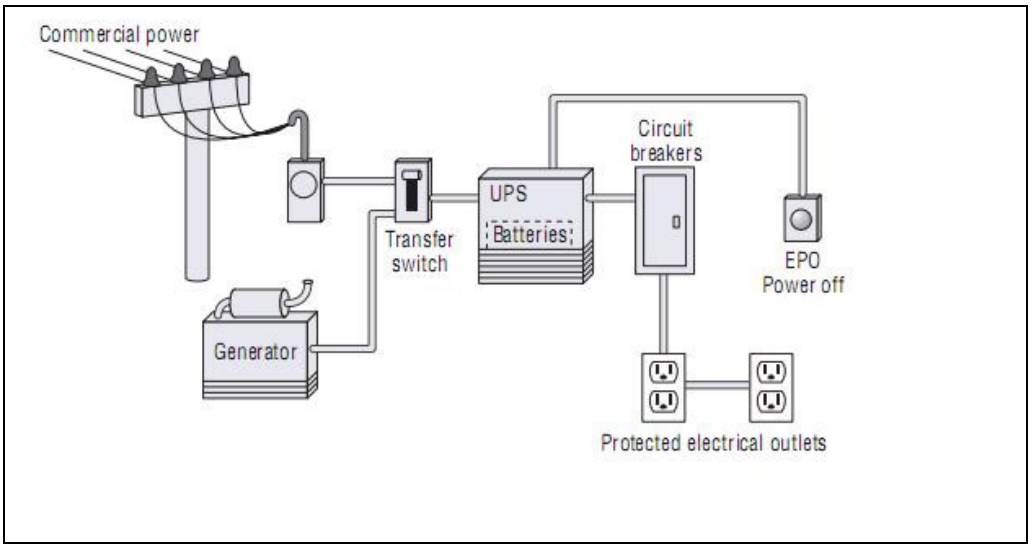
Nomor	Kriteria	Kerahasiaan		Integritas		Ketersediaan		Total Skor
	Bobot	5		5		5		
		Skor	Jumlah	Skor	Jumlah	Skor	Jumlah	
	Parameter							
1.	Pemadaman darurat	1	5	1	5	1	5	15
2.	Suplai daya tanpa interupsi	3	15	3	15	3	15	45
3.	Generator cadangan	5	25	5	25	5	25	75
4.	Sistem transfer daya	5	25	5	25	5	25	75
5.	Pemanas, ventilasi dan pendingin udara	1	5	1	5	5	25	35
6.	Deteksi panas, asap dan api	1	5	1	5	3	15	25
7.	Pemadam api	1	5	1	5	3	15	25
8.	Deteksi air	1	5	1	5	3	15	25

Penjelasan matrik keputusan kontrol lingkungan pada Tabel 3.3 dapat diuraikan sebagai berikut:

1. Pemadaman darurat mendapatkan nilai 1 untuk kerahasiaan karena tidak mempengaruhi kerahasiaan informasi. Nilai 1 untuk integritas karena tidak mempengaruhi unsur integritas data. Nilai 1 untuk ketersediaan karena data tidak tersedia ketika terjadi pemadaman. Letak saklar pemadam darurat pada perusahaan dapat dilihat pada Gambar 3.5.
2. Suplai daya tanpa interupsi mendapat nilai 3 untuk kerahasiaan karena dapat mendukung daya sementara untuk menjaga keamanan daftar kontrol akun. Nilai 3 untuk integritas karena dapat mempertahankan integritas data walaupun sesaat.

Nilai 3 untuk ketersediaan karena dapat menyediakan data walaupun untuk sesaat. Sistem suplai daya tanpa interupsi (UPS) pada perusahaan seperti yang ditunjukkan oleh Gambar 3.5.

3. Generator cadangan mendapat nilai 5 untuk kerahasiaan karena daya tersedia untuk menjaga proses akses informasi pada sistem. Nilai 5 untuk integritas karena daya selalu tersedia untuk perangkat sehingga autentikasi kewenangan atas data berjalan pada sistem. Nilai 5 untuk ketersediaan karena sistem mendapatkan daya untuk memastikan data tersedia. Gambar 3.5 memperlihatkan diagram sistem generator cadangan pada pusat data perusahaan. Perangkat generator cadangan yang di gunakan adalah CAT ® 3460C *Diesel Engine* 350 kVA



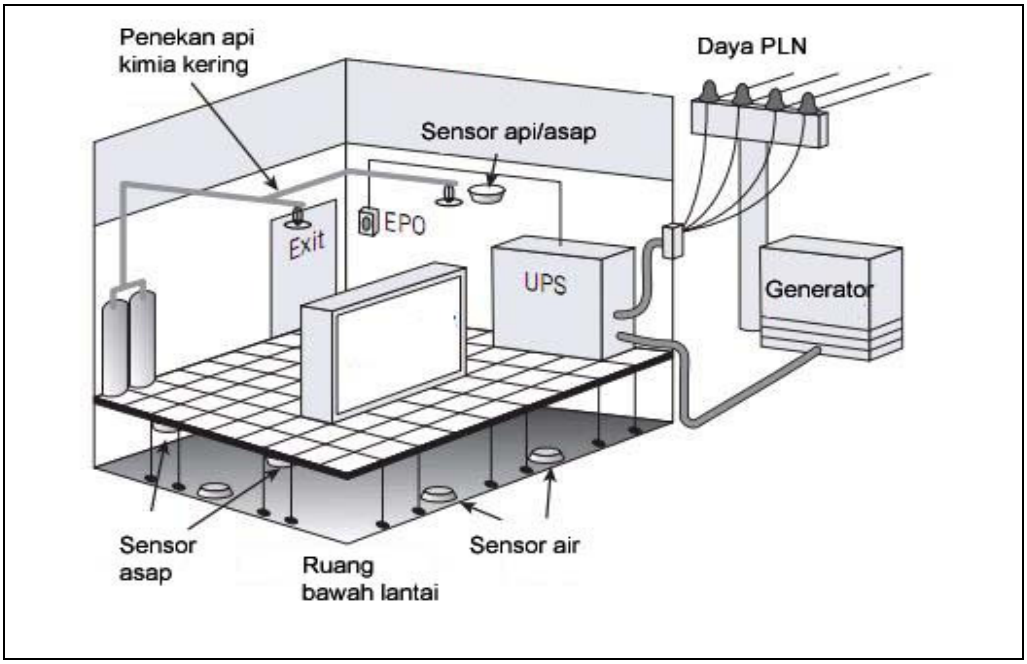
Gambar 3.5 Diagram sistem generator cadangan

4. Sistem tranfer daya mendapat nilai 5 untuk kerahasiaan karena daya tersedia untuk menjaga proses akses informasi pada sistem informasi. Nilai 5 untuk integritas karena daya selalu tersedia untuk perangkat sehingga autentikasi kewenangan atas data tetap berjalan pada sistem. Nilai 5 untuk ketersediaan karena sistem

mendapatkan daya untuk memastikan data tersedia. Diagram sistem transfer daya terdapat pada pusat data perusahaan dapat dilihat pada Gambar 3.5.

5. Pemanas, ventilasi dan pendingin udara mendapatkan nilai 1 untuk keamanan karena tidak berpengaruh terhadap keamanan sistem informasi. Nilai 1 untuk integritas karena tidak ada pengaruh terhadap pelanggaran perubahan berkas. Nilai 5 untuk ketersedian karena ventilasi dan pendingin udara menjaga komponen elektrikal pada perangkat komputer bekerja dengan baik (tidak mengalami kondisi panas berlebihan). Ventilasi dan pendingin udara terdapat pada pusat data perusahaan.
6. Deteksi panas, asap dan api mendapat nilai 1 untuk keamanan karena tidak berpengaruh terhadap keamanan sistem informasi. Nilai 1 untuk integritas karena tidak ada pengaruh terhadap pelanggaran perubahan berkas. Nilai 3 untuk ketersediaan karena langkah pencegahan atas kerentanan hilangnya ketersediaan informasi. Deteksi panas, asap dan api terdapat pada pusat data perusahaan seperti yang ditunjukkan oleh Gambar 3.6.
7. Pemadam api mendapat nilai 1 untuk keamanan karena tidak berpengaruh untuk keamanan. Nilai 1 untuk integritas karena tidak ada pengaruh terhadap pelanggaran perubahan berkas. Nilai 3 untuk ketersediaan sebagai langkah pencegahan atas kerentanan kehilangan informasi atas bahaya api. Pemadam api terdapat pada pusat data perusahaan seperti yang ditunjukkan oleh Gambar 3.6.
8. Deteksi air mendapat nilai 1 untuk keamanan karena tidak berpengaruh untuk keamanan. Nilai 1 untuk integritas karena tidak ada pengaruh terhadap pelanggaran

perubahan berkas. Nilai 3 untuk ketersediaan sebagai langkah pencegahan atas kerentanan kehilangan informasi atas bahaya air terhadap komponen elektrikal. pemadam air terdapat pada pusat data perusahaan seperti yang ditunjukkan oleh Gambar 3.6.



Gambar 3.6 Diagram kontrol lingkungan pusat data

Sistem transfer daya dan generator mendapatkan total nilai tertinggi dengan total skor 75. Sistem transfer daya dan generator untuk pusat data ditemukan pada perusahaan yang diteliti. Kontrol lingkungan diperlukan untuk melindungi pengatur ranah utama atau cadangan direktori aktif untuk berjalan dengan normal.

3.4 Penyimpanan Aman

Penyimpanan aman diperlukan untuk mencegah kerusakan rekaman bisnis penting dan media komputer terhadap bahaya kebakaran, pencurian, dan bahaya lainnya. Tabel 3.4 memperlihatkan penilaian mengenai penyimpanan aman.

Tabel 3.4 Matrik keputusan penyimpan aman

Nomor	Kriteria	Kerahasiaan		Integritas		Ketersediaan		Total Skor
	Bobot	5		5		5		
		Skor	Jumlah	Skor	Jumlah	Skor	Jumlah	
	Parameter							
1.	Penyimpan yang aman	4	20	5	25	5	25	70
2.	Penyimpan di luar	4	20	5	25	5	25	70
3.	Media transportasi penyimpan	3	15	3	3	3	15	33

Penjelasan matriks keputusan penyimpan aman pada Tabel 3.4 dapat diuraikan sebagai berikut:

1. Penyimpan yang aman mendapatkan nilai 4 untuk kerahasiaan karena semua berkas data disimpan dalam kabinet berkas tahan api. Integritas mendapatkan nilai 5 karena data yang tersimpan tidak akan mengalami perubahan selama berada dalam kabinet berkas, dan tidak akan bisa di akses kecuali oleh petugas data. Pada ketersediaan mendapatkan nilai 5 karena berkas yang tersimpan di tempat yang aman dapat dipergunakan untuk cadangan data jika penyimpan data utama mengalami kerusakan.
2. Penyimpan di luar area mendapatkan nilai 4 untuk kerahasiaan. Penyedia jasa penyimpan di luar area utama menyediakan jasa keamanan 24 jam pada areanya. Pencurian tetap masih bisa terjadi dengan pengunaan identifikasi palsu petugas

keamanan. Integritas mendapatkan nilai 5 karena hanya petugas data yang berwenang yang bisa mengakses data. Ketersediaan mendapatkan nilai 5 karena jika data utama hilang atau rusak dapat di kembalikan melalui data cadangan di penyimpan luar area.

3. Media transportasi penyimpan mendapatkan nilai 3 untuk kerahasiaan karena selama perjalanan dari area penyimpan utama menuju tempat penyimpan di luar memiliki resiko. Resiko tersebut bisa berupa kecelakaan pada media sehingga pihak lain bisa mengambil media berkas yang tercecer. Nilai 3 untuk integritas karena pada kejadian kecelakaan maka data bisa dibuka oleh pihak yang tidak berwewenang. Nilai 3 untuk ketersediaan karena jika terjadi kecelakaan maka ketersediaan data tidak bisa terpenuhi.

Penyimpan aman dan penyimpan diluar area pusat data mendapatkan total nilai tertinggi dengan total skor 70. Penyimpan aman dan penyimpan di luar area pusat data tidak terdapat pada perusahaan yang diteliti

3.5 Metode Autentikasi

Beberapa metode autentikasi untuk mendapatkan akses informasi adalah kata sandi, kartu pintar, token perangkat keras, token perangkat lunak, sidik jari tangan, sidik telapak tangan, geometri tangan, pindai iris mata, pindai retina mata, pindai wajah, tanda tangan dinamik dan pola suara. Tabel 3.5 memperlihatkan penilaian mengenai metode autentikasi.

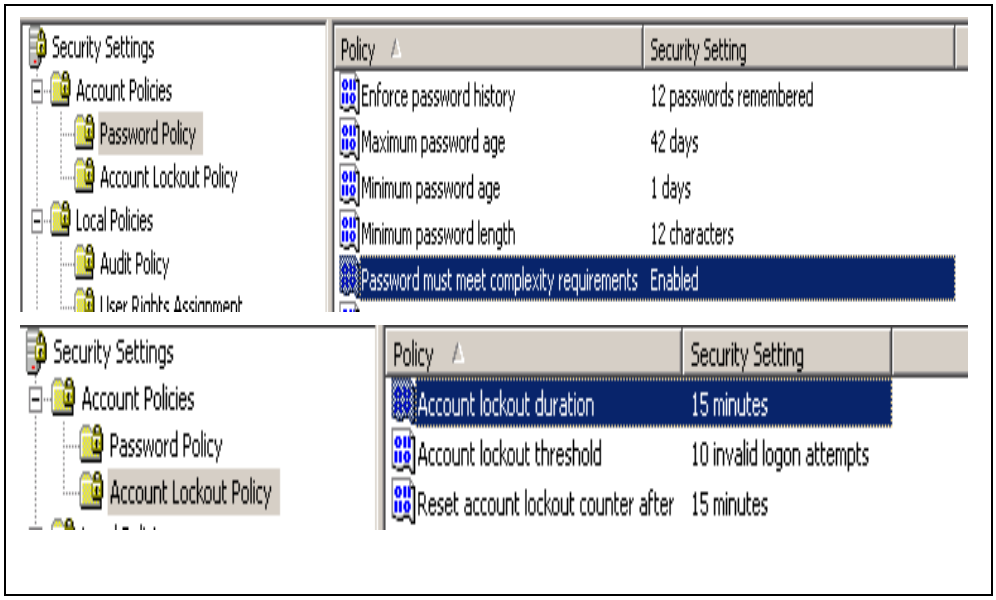
Tabel 3.5 Matriks keputusan metode autentikasi

Nomor	Kriteria	Kerahasiaan		Integritas		Ketersediaan		Total Skor
	Bobot	5		5		5		
		Skor	Jumlah	Skor	Jumlah	Skor	Jumlah	
	Parameter							
1.	Kata sandi	3	15	3	15	1	5	35
2.	Kartu pintar	3	15	3	15	1	5	35
3.	Token perangkat keras	3	15	3	15	1	5	35
4.	Token perangkat lunak	3	15	3	15	1	5	35
5.	Sidik jari tangan	5	25	5	25	3	15	65
6.	Sidik telapak tangan	5	25	5	25	3	15	65
7.	Geometri tangan	5	25	5	25	3	15	65
8.	Pindai iris mata	5	25	5	25	3	15	65
9.	Pindai retina mata	5	25	5	25	3	15	65
10.	Pindai wajah	5	25	5	25	3	15	65
11.	Tanda tangan dinamik	2	10	1	5	1	5	20
12.	Pola suara	1	5	1	5	1	5	15

Penjelasan matriks keputusan metode autentikasi pada Tabel 3.5 dapat diuraikan sebagai berikut :

1. Kata sandi merupakan autentikasi yang lemah karena dapat dilupakan, dibagi, ditemukan dengan pengamatan, dan rusak dalam arti teknikal. Kata sandi mendapatkan nilai 3 untuk kerahasiaan karena bisa terlupa, dibagi dengan tidak tidak sengaja dan diamati oleh pihak lain. Integritas mendapatkan nilai 3 karena kata sandi yang tertebak menyebabkan integritas data sudah di terobos sehingga data bisa di duplikasi oleh perengah . Ketersediaan data mendapat nilai 1 karena sandi yang

telah ditebak menyebabkan akses berkas bisa di hapus atau dirusak perengah. Gambar 3.7 memperlihatkan kebijakan kata sandi pada direktori aktif Windows Server 2003.



Gambar 3.7 Kebijakan kata kunci pada direktori aktif

2. Kartu pintar, berisikan chip mikro berisikan informasi unik yang hanya bisa dibaca oleh pemindai kartu. Kartu chip mendapatkan nilai 3 untuk kerahasiaan karena kartu chip punya resiko kelemahan seperti tertinggal, diduplikasi dan dimanfaatkan pihak lain. Nilai 3 untuk integritas karena kartu chip yang telah diduplikasi atau tertinggal bisa menyebabkan data diubah oleh pihak lain. Nilai 1 untuk ketersediaan karena data bisa dihapus pihak yang tidak berwenang jika kartu chip dicuri atau diduplikasi. Kartu pintar tidak ditemukan pada sistem direktori aktif perusahaan.
3. Token perangkat keras, merupakan kartu atau kunci yang dibaca pengguna pada saat log masuk. Pengguna mengetikkan nama dan kata sandi digabungkan dengan angka yang muncul pada layar token yang selalu berubah setiap 1-2 menit. Token

perangkat keras mendapatkan nilai 3 untuk kerahasiaan karena token punya kelemahan tertinggal, diduplikasi dan dimanfaatkan pihak lain. Nilai 3 untuk integritas karena token yang telah diduplikasi atau tertinggal bisa menyebabkan data diubah oleh pihak lain. Nilai 1 untuk ketersediaan karena data bisa dihapus pihak yang tidak berwenang jika token dicuri atau diduplikasi. Token perangkat keras tidak ditemukan pada sistem direktori aktif perusahaan.

4. Token perangkat lunak, dikenal sebagai sertifikat digital. Token perangkat lunak menangkap informasi unik termasuk nomor elektronik serial computer selama inisialisasi permintaan pengecekan sertifikat. Token perangkat lunak mendapatkan nilai 3 untuk kerahasiaan karena token punya kelemahan diduplikasi dan dimanfaatkan pihak lain. Nilai 3 untuk integritas karena token yang telah diduplikasi atau tertinggal bisa menyebabkan data diubah oleh pihak lain. Nilai 1 untuk ketersediaan karena data bisa dihapus pihak yang tidak berwenang jika token diduplikasi. Token perangkat lunak tidak ditemukan pada sistem direktori aktif perusahaan.
5. Sidik jari tangan merupakan metode identifikasi yang digunakan sejak lama untuk identifikasi orang, khususnya pelaku kriminal. Pada perangkat biometrik sidik jari tangan digunakan untuk autentikasi (bukan identifikasi) pengguna. Sidik jari mendapatkan nilai 5 untuk kerahasiaan karena bersifat unik pada setiap orang. Nilai 5 untuk integritas karena hanya yang memiliki pola sidik jari yang sesuai yang memiliki kewenangan atas data. Nilai 3 untuk ketersediaan data karena jika jari tangan terluka atau terpotong maka pola yang sudah di rekam pada biometrik akan

tidak sama. Hal tersebut menyebabkan autentikasi akan di tolak dan data yang dibutuhkan tidak dapat tersedia. Sidik jari tangan ditemukan pada direktori aktif dengan autentikasi sidik jari langsung ke kata sandi dengan menggunakan alat perangkat lunak Hewlet Packard pada laptop. Perangkat lunak tersebut hanya ada di beberapa tipe laptop tertentu yang memiliki fasilitas perangkat sidik jari (misalnya tipe HP Compaq 6530b) dan digunakan oleh sedikit pengguna. Tidak semua pengguna menggunakan tipe laptop, dan fasilitas sidik jari tersebut.

6. Sidik telapak tangan juga merupakan ciri khas yang unik seperti sidik jari. Seperti sidik jari telapak tangan memiliki jumlah detail kecil yang penting ditambah garis-garis keriput, pola pembuluh darah, dan bekas luka. Sidik telapak tangan mendapatkan nilai 5 untuk kerahasiaan karena bersifat unik pada setiap orang. Nilai 5 untuk integritas karena hanya yang memiliki pola sidik telapak tangan yang sesuai yang memiliki kewenangan atas data. Nilai 3 untuk ketersediaan data karena jika telapak tangan terluka atau terpotong maka pola yang sudah di rekam pada biometrik akan tidak sama. Hal tersebut menyebabkan autentikasi akan di tolak dan data yang dibutuhkan tidak dapat tersedia. Autentikasi sidik telapak tangan tidak ditemukan pada sistem direktori aktif perusahaan.
7. Geometri tangan memiliki konsep mengukur detil tangan seseorang dalam citra tiga dimensi. Sidik telapak tangan mendapatkan nilai 5 untuk kerahasiaan karena bersifat unik pada setiap orang. Nilai 5 untuk integritas karena hanya yang memiliki pola geometri tangan yang sesuai yang memiliki kewenangan atas data. Nilai 3 untuk ketersediaan data karena jika tangan terluka atau terpotong maka pola yang sudah di

rekam pada biometrik akan tidak sama. Hal tersebut menyebabkan autentikasi akan di tolak dan data yang dibutuhkan tidak dapat tersedia. Autentikasi geometri tangan tidak ditemukan pada sistem direktori aktif perusahaan.

8. Iris mata, teknologi pindai iris mata berdasarkan fitur yang terlihat seperti bintik, bulatan dan kerutan cincin warna di sekitar pupil mata. Pindai iris mata mendapatkan nilai 5 untuk kerahasiaan karena bersifat unik pada setiap orang. Nilai 5 untuk integritas karena hanya yang memiliki pola yang sesuai yang memiliki kewenangan atas data. Nilai 3 untuk ketersediaan data karena jika mata menggunakan lensa kontak maka pola yang sudah di rekam pada biometrik akan tidak sama. Hal tersebut menyebabkan autentikasi akan di tolak dan data yang dibutuhkan tidak dapat tersedia. Autentikasi iris mata tidak ditemukan pada sistem direktori aktif perusahaan.
9. Pindai retina mata, retina mata memiliki pola unik pembuluh halus darah dan pembuluh arteri yang memantulkan cahaya. Pindai retina mata mendapatkan nilai 5 untuk kerahasiaan karena bersifat unik pada setiap orang. Nilai 5 untuk integritas karena hanya yang memiliki pola yang sesuai yang memiliki kewenangan atas data. Nilai 3 untuk ketersediaan data karena jika retina mata terkena efek kondisi medis seperti penyakit stroke dan diabetes, maka pola yang sudah di rekam pada biometrik akan tidak sama. Hal tersebut menyebabkan autentikasi akan di tolak dan data yang dibutuhkan tidak dapat tersedia. Autentikasi retina mata tidak ditemukan pada sistem direktori aktif perusahaan.

10. Pindai wajah, teknologi pindai wajah terbaru menggunakan rangkaian citra diam yang ditangkap kamera video. Teknologi menggunakan pengukuran tiga dimensi dari fitur wajah, termasuk posisi rongga mata, hidung, bukaan mulut, dan termograph pola panas suhu. Pindai wajah mendapatkan nilai 5 untuk kerahasiaan karena bersifat unik pada setiap orang. Nilai 5 untuk integritas karena hanya yang memiliki pola yang sesuai yang memiliki kewenangan atas data. Nilai 3 untuk ketersediaan data karena jika wajah terkena efek kondisi medis seperti terluka atau bedah kosmetik, maka pola yang sudah di rekam pada biometrik akan tidak sama. Hal tersebut menyebabkan autentikasi akan di tolak dan data yang dibutuhkan tidak dapat tersedia. Autentikasi fitur wajah tidak ditemukan pada sistem direktori aktif perusahaan.
11. Tanda tangan dinamik merupakan bentuk perilaku dari data biometrik. Tanda tangan di monitor dengan durasi waktu, tekanan, dan teknik. Tanda tangan dinamik mendapatkan nilai 2 untuk keamanan karena bentuk tangan tangan dapat dipalsukan apalagi dalam bentuk tanda tangan digital. Nilai 1 untuk integritas karena sudah banyak metode untuk memalsukan tanda tangan. Nilai 1 untuk ketersediaan karena kerusakan perangkat mengakibatkan data tidak tersedia. Autentikasi tanda tangan dinamik tidak ditemukan pada sistem direktori aktif perusahaan.
12. Pola suara melakukan analisa atas karakter pitch, nada dan lama suara ketika mengucapkan satu frasa kata yang diulang. Karakter tersebut di konversi dalam template digital. mendapatkan nilai 1 untuk keamanan karena autentikasi suara dapat dibohongi dengan merekam ulang balik audio dari suara orang tersebut. Nilai

1 untuk integritas autentikasi suara dapat dibohongi dengan merekam ulang balik audio dari suara orang tersebut sehingga bisa akses data. Nilai 1 untuk ketersediaan karena kondisi kesehatan pengguna (radang tenggorokan, batuk dan pilek) serta kerusakan pada perangkat pengenal bisa mengakibatkan data tidak tersedia karena autentikasi akan ditolak. Autentikasi pola suara tidak ditemukan pada sistem direktori aktif perusahaan.

Sidik jari tangan, sidik telapak tangan, geometri tangan, pindai iris mata, dan pindai retina mata mendapatkan nilai tertinggi dengan total skor 53. Pada direktori aktif Windows Server 2003 perusahaan yang diteliti hanya metode autentikasi dengan menggunakan kata sandi yang ditemukan.

3.6 Proteksi Akses Jaringan

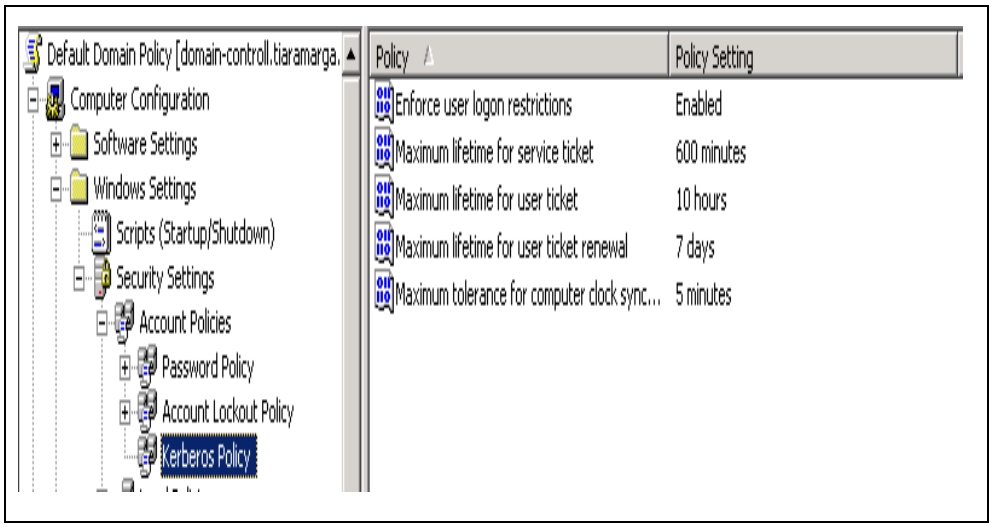
Setiap komputer di jaringan cenderung bermasalah dengan kontrol akses untuk menyediakan akses ke pihak yang sah dan memblokade akses dari pihak lain. Tabel 3.6 memperlihatkan penilaian mengenai proteksi akses jaringan.

Tabel 3.6 Matrik keputusan proteksi jaringan

Nomor	**Kriteria**	**Kerahasiaan**		**Integritas**		**Ketersediaan**		**Total Skor**
	Bobot	**5**		**5**		**5**		
		Skor	**Jumlah**	**Skor**	**Jumlah**	**Skor**	**Jumlah**	
	Parameter							
1.	Autentikasi Kerberos	3	15	3	15	3	15	45
2.	Firewall jaringan	3	15	3	15	3	15	45

Penjelasan matriks keputusan proteksi jaringan pada Tabel 3.6 dapat diuraikan sebagai berikut:

1. Autentikasi Kerberos mendapatkan nilai 3 untuk komponen keamanan karena kerberos hanya menyediakan keamanan pada titik akhir jaringan namun tidak pada jalur transmisi. Kerberos juga memiliki masalah kompatibilitas dengan versi implementasi yang berbeda. Komponen integritas mendapat nilai 3 karena kerberos hanya menyediakan keamanan pada titik akhir jaringan namun tidak pada jalur transmisi. Hal tersebut menyebabkan celah untuk peretas memanfaatkan jalur transmisi jaringan untuk mencegat data. Komponen ketersediaan mendapatkan nilai 3 karena peretas dapat memanfaatkan jalur transmisi jaringan untuk mengambil alih data dengan pola serangan *man in the middle*. Konfigurasi autentikasi Kerberos ditemukan pada sistem direktori aktif perusahaan seperti yang ditunjukkan oleh Gambar 3.8.



Gambar 3.8 Kebijakan Kerberos direktori aktif perusahaan

Penjelasan kebijakan Kerberos direktori aktif perusahaan pada Gambar 3.8 dapat diuraikan sebagai berikut:

a. *Enforce logon restriction,* menentukan apakah Kerberos *V5 Key Distribution Center* (KDC) akan memvalidasi setiap permintaan untuk akses terhadap kebijakan hak akses dari akun pengguna tersebut.

b. *Maximum lifetime for service ticket,* ,menentukan jumlah waktu dalam menit yang memperbolehkan akses terhadap beberapa layanan terhadap sumber daya server. Jangka waktu 600 menit

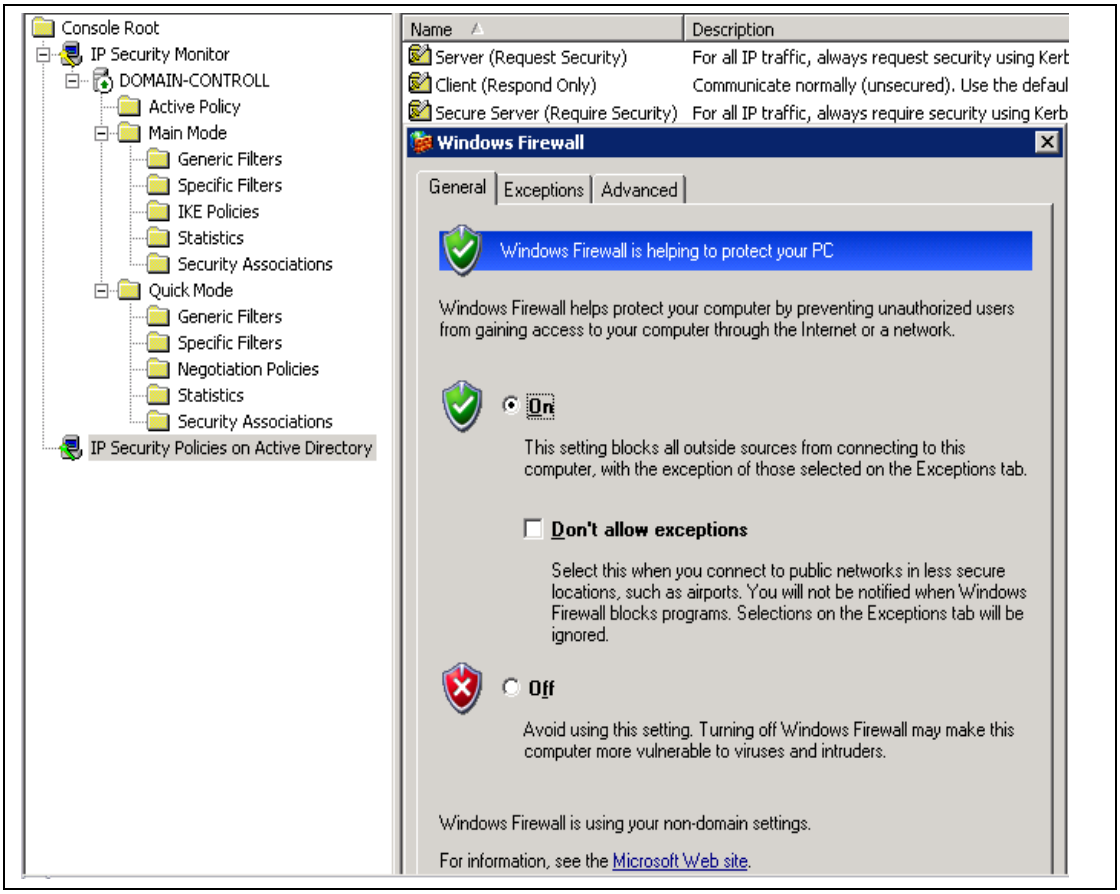
c. *Maximum lifetime for user ticket,* menentukan jumlah total waktu dalam hitungan jam terhadap penggunaaan TGT (*ticket-granted ticket*). Ketika TGT pengguna sudah kadaluarsa, pengguna harus melakukan permintaan TGT yang baru, atau yang kadaluarsa diperbaharui kembali. Jangka waktu 10 jam.

d. *Maximum lifetime for user ticket renewal,* menentukan jangka waktu dalam hitungan hari untuk masa TGT pengguna kapan harus diperbaharui. Jangka waktu 7 hari.

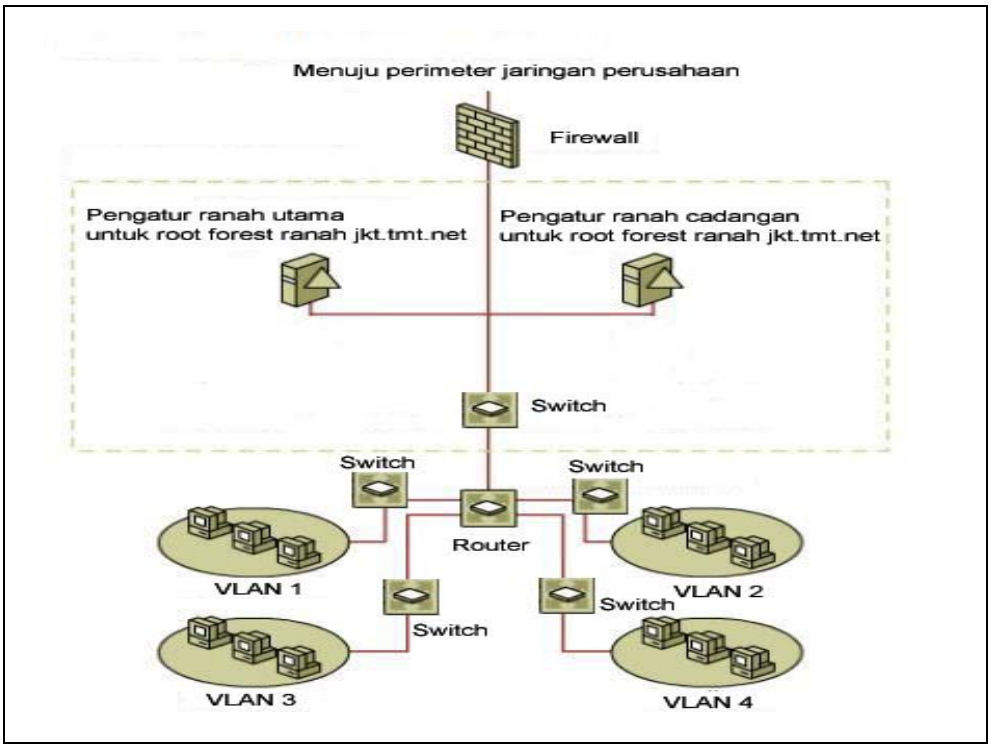
e. *Maximum tolerance for computer clock synchronize ,* menentukan maksimal selisih waktu dalam hitungan menit yang bisa ditolerasi oleh Kerberos V5 antara jam di komputer pengguna terhadap jam pada server pengatur ranah Windows Server 2003 yang menyediakan autentikasi Kerberos. Jangka waktu 5 menit.

2. Dinding pembatas jaringan (*network firewall*) memiliki nilai 3 untuk komponen keamanan karena dapat mengurangi akses dari luar menuju jaringan namun tidak

melindungi akses modem ataupun titik akses. Nilai 3 untuk integritas dan ketersediaan karena peretas masih bisa memanfaatkan akses modem atau titik akses yang tidak terlindungi *firewall* untuk menembus data. Pada sistem direktori aktif ditemukan firewall seperti yang ditunjukkan oleh Gambar 3.9 dan secara topologi seperti yang tunjukkan oleh Gambar 3.10.



Gambar 3.9 Pengaturan Windows firewall pada server direktory aktif



Gambar 3.10 Topologi firewall perusahaan

Penjelasan topologi firewall perusahaan pada Gambar 3.10 adalah sebagai berikut:

1. Perangkat *firewall* jaringan diletakkan sebelum area DMZ (*demilitarized zone*) yang merupakan batas perimeter dari area jaringan internal perusahaan dengan jaringan eksternal.
2. Pengatur ranah utama (*Primary Domain Controller*) dan pengatur ranah cadangan (*Backup Domain Controller*) diletakkan dibelakang *firewall* pada jaringan internal.
3. Komunikasi lalu lintas jaringan antara pengatur ranah utama dan komputer pengguna tetap berada di belakang *firewall*. Diatur melalui distribusi VLAN

(*Virtual Local Area Network*) untuk mengatur ranah pemancar komunikasi jaringan (*broadcast domain*) pada tingkat jaringan.

Autentikasi kerberos dan *firewall* mendapatkan nilai tertinggi dengan total skor 53. Kebijaksanaan autentikasi kerberos dan *firewall* terdapat pada direktori aktif Windows Server 2003 perusahaan.

3.7 Metode Enkripsi

. Ada dua tipe dasar sistem enkripsi, sistem enkripsi kunci rahasia dan sistem enkripsi kunci umum yang keduanya berbentuk digital (berkas). Tabel 3.7 memperlihatkan penilaian mengenai metode enkripsi.

Tabel 3.7 Matrik keputusan metode enkripsi

Nomor	**Kriteria**	**Kerahasiaan**		**Integritas**		**Ketersediaan**		**Total Skor**
	Bobot	**5**		**5**		**5**		
		Skor	**Jumlah**	**Skor**	**Jumlah**	**Skor**	**Jumlah**	
	Parameter							
1.	Enkripsi kunci rahasia	3	15	3	15	3	15	45
2.	Enkripsi kunci umum	3	15	3	15	3	15	45
3.	Tanda tangan digital	4	20	4	20	3	15	55

Penjelasan matriks keputusan metode enkripsi pada Tabel 3.7 dapat diuraikan sebagai berikut:

1. Enkripsi kunci rahasia memiliki nilai 3 untuk kerahasiaan. Kunci rahasia hanya dimiliki satu orang dan untuk dekripsi terhadap informasi harus memiliki kunci rahasia. Kelemahannya jika ada orang lain yang memiliki duplikat kunci rahasia

maka dia juga dapat melakukan dekripsi dan membaca informasi tersebut. Nilai 3 untuk integritas karena kewenangan atas data bisa jatuh ketangan orang yang tidak berwenang namun memiliki duplikat kunci rahasia. Nilai 3 untuk ketersediaan karena jika kunci rahasia hilang maka data tidak bisa diakses walaupun oleh pihak berwenang.

2. Enkripsi kunci umum berdasarkan kriptografi asimetrik. Di rancang untuk mendaya gunakan pasangan kunci terpisah untuk enkripsi dan dekripsi (kunci pribadi dan umum) untuk pengirim dan penerima. Nilai komponen keamanan adalah 3 untuk kerahasiaan karena pada sistem asimetrik pengirim dan penerima tidak perlu mengirimkan duplikasi kunci di antara mereka. Hal ini mencegah pihak ketiga untuk duplikasi kunci ketika transmisi. Kelemahannya adalah beberapa algoritma tidak menjamin keamanan terhadap serangan yang baru. Kemungkinan serangan mencegat transmisi kunci umum dari pihak ketiga juga bisa terjadi. Penggunaan kewenangan sertifikat digital, pihak ketiga yang terpercaya bisa meminimalkan pencegatan transmisi tersebut. Nilai integritas dan ketersediaan mendapatkan nilai 3 karena algoritma keamanan masih bisa ditembus walaupun menggunakan enkripsi RSA (Rivest, Shamir and Adleman) 512-bit.
3. Tanda tangan digital mendapatkan nilai 4 untuk keamanan karena tergantung pada keamanan komputer dan juga panjang kunci enkripsi dan jenis algoritma yang digunakan. Nilai 4 untuk integritas karena walaupun sudah didukung dengan algoritma yang baik namun teknologi ini belum bisa dijadikan standar keabsahan kepemilikan suatu dokumen karena masih memiliki kelemahan untuk bisa

dipalsukan. Nilai 3 untuk ketersediaan karena celah kelemahan dengan melakukan serangan *brute force* untuk menebak kunci pribadi pengirim, maka berkas memiliki kerentanan untuk bisa dihapus.

Enkripsi kunci rahasia, enkripsi kunci umum, dan tanda tangan digital mendapatkan nilai sama dengan total skor 45. Pada direktori aktif kebijakan sistem file enkripsi kunci publik dan kunci umum terdapat pada infrastruktur kunci publik seperti yang ditunjukkan oleh Gambar 3.11.

3.8 Infrastruktur Kunci Publik

Infrastruktur kunci publik merupakan sebuah cara untuk autentikasi, pengamanan data dan perangkat anti sangkal. Secara teknis, infrastruktur kunci publik adalah implementasi dari berbagai teknik kriptografi yang bertujuan untuk mengamankan data, memastikan keaslian data maupun pengirimnya dan mencegah penyangkalan. Table 3.9 memperlihatkan penilaian mengenai infrastruktur kunci publik.

Tabel 3.8 Matriks keputusan infrastuktur kunci publik

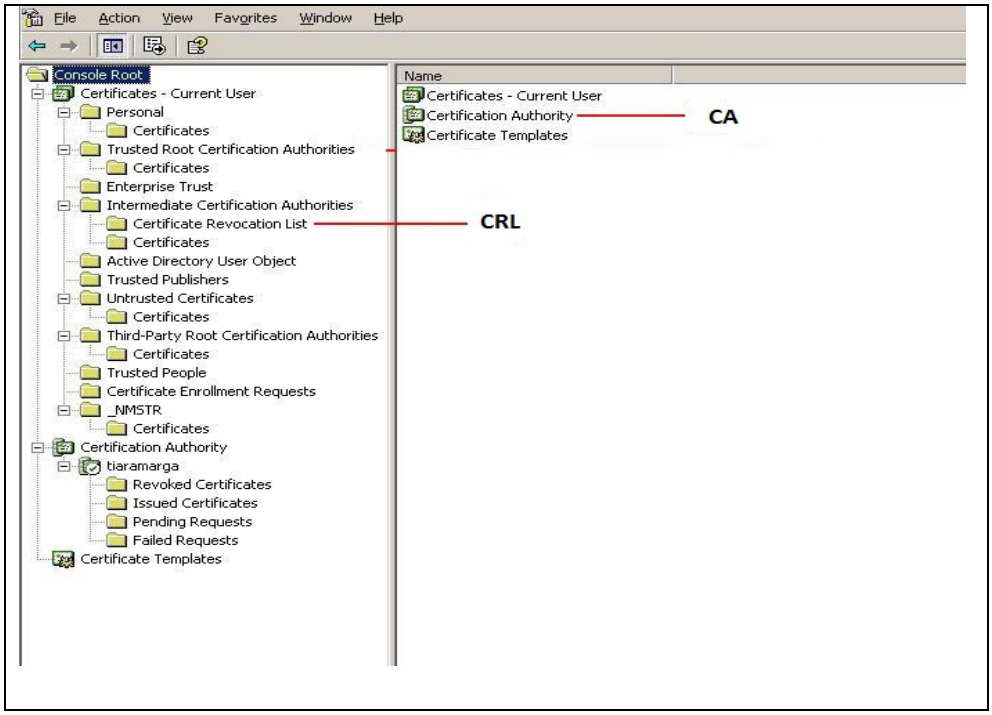
Nomor	**Kriteria**	**Kerahasiaan**		**Integritas**		**Ketersediaan**		**Total Skor**
	Bobot	**5**		**5**		**5**		
		Skor	**Jumlah**	**Skor**	**Jumlah**	**Skor**	**Jumlah**	
	Parameter							
1.	Penerbit sertifikat	4	20	4	20	4	20	60
2.	Kewenangan registrasi	4	20	4	20	4	20	60
3.	Sertifikat daftar penolakan	4	20	4	20	4	20	60
4.	Sertifikat pernyataan praktek	3	15	3	15	3	15	45

Penjelasan matriks keputusan infrastruktur kunci public pada Tabel 3.8 dapat diuraikan sebagai berikut:

1. Penerbit sertifikat (*certificate authority* (CA)) berfungsi untuk memelihara sertifikat digital yang telah diterbitkan dan memeriksa kewenangan. Penerbit sertifikat mendapatkan skor 4 untuk kerahasiaan, integritas dan ketersediaan. Hal ini dikarenakan untuk akses data pengguna data harus memiliki sertifikat pemilik data yang telah di validasi oleh penerbit sertifikat.
2. Kewenangan registrasi (*registration authority* (RA)) berfungsi untuk menjamin ikatan kewenangan antara pemilik dan pengguna data. Kewenangan registrasi mendapatkan skor 4 untuk kerahasiaan, integritas dan ketersediaan. Hal ini dikarenakan fungsi untuk menjamin kewenangan antara pemilik dan penguna data akan melindungi kerahasiaan, integritas dan ketersediaan data ataupun aplikasi.
3. Sertifikat daftar penolakan (*certification revocation list* (CRL)) digunakan untuk pemeriksaan sertifikat digital apakah sah atau tidak. Sertifikat daftar penolakan diterbitkan oleh penerbit sertifikat untuk indikasi sertifikat digital yang telah habis masa berlaku ataupun di cabut. Sertifikat daftar penolakan mendapatkan skor 4 untuk kerahasiaan, integritas dan ketersediaan. Hal ini dikarenakan sertifikat yang telah masuk daftar penolakan tidak akan bisa mengakses data ataupun aplikasi. Kekurangannya jika sertifikat daftar penolakan mengalami penolakan yang salah maka pengguna yang sah tidak bisa akses informasi.

4. Sertifikat pernyataan praktek (*certification practise statement* (CPS)) merupakan prosedur bagaimana infrastruktur kunci publik sertifikat digital akan diterbitkan, diatur, digunakan, diperbaharui, dan dicabut. Sertifikat pernyataan praktek mendapatkan nilai 3 untuk keamanan, integritas dan ketersediaan karena menyediakan prosedur untuk infrastruktur kunci publik. Kekurangannya tidak menyediakan proteksi secara teknikal hanya prosedural.

Penerbit sertifikat (CA), kewenangan registrasi (RA), dan sertifikat daftar penolakan (CRL) mendapatkan nilai tertinggi dengan total skor 20. Gambar 3.11 memperlihatkan penerbit sertifikat (*certificate authority* (CA)) dan sertifikat daftar penolakan (*certification revocation list* (CRL)) pada Sistem operasi Windows 2003 Server.



Gambar 3.11 Infrastuktur kunci publik Windows Server 2003

3.9 Protokol Keamanan Jaringan

Penggunaan transaksi *e-commerce* menjadi penting bagi perdagangan di era teknologi informasi. Kemudahaan akses Internet juga membuat transaksi *e-commerce* menjadi hal umum. Transaksi *e-commerce* dibangun atas protokol keamanan jaringan yang membantu kenyamanan pengguna. Penilaian mengenai protokol keamanan jaringan terlihat pada Tabel 3.9

Tabel 3.9 Matriks keputusan protokol keamanan jaringan

Nomor	Kriteria	Kerahasiaan		Integritas		Ketersediaan		Total Skor
	Bobot	5		5		5		
		Skor	Jumlah	Skor	Jumlah	Skor	Jumlah	
	Parameter							
1	PGP	4	20	5	25	4	20	65
2	SSL	3	15	4	20	3	15	50
3	HTTPS	3	15	3	15	3	15	45
4	IPSec	4	20	5	25	4	20	65

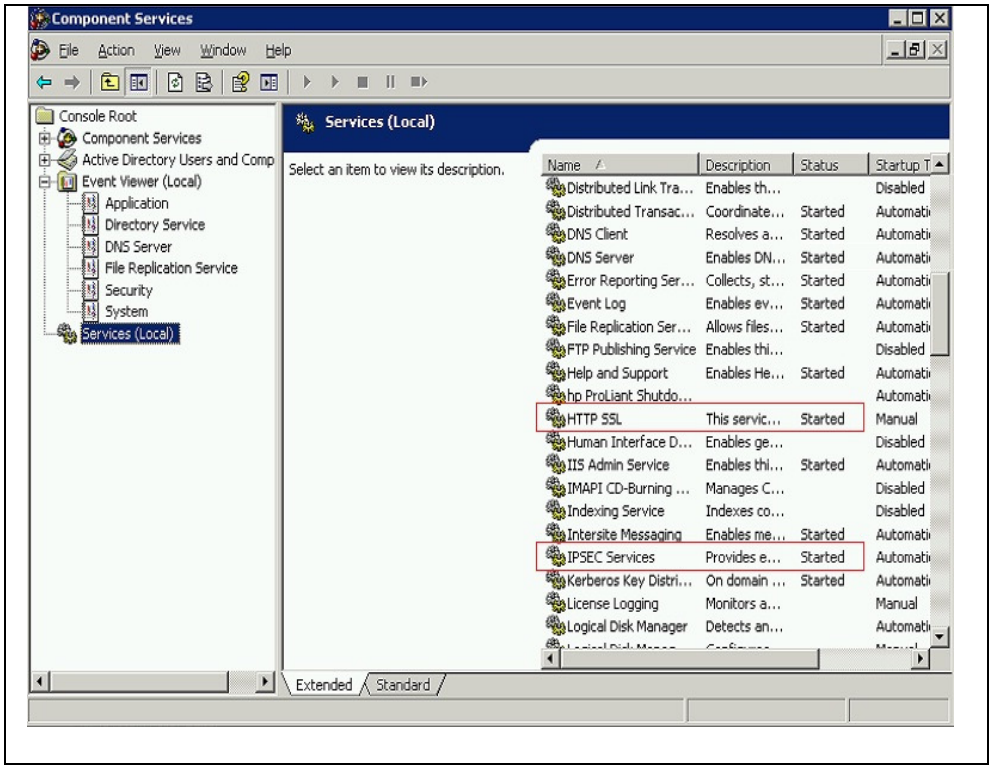
Penjelasan matriks keputusan protokol keamanan jaringan pada Tabel 3.9 dapat uraikan sebagai berikut :

1. PGP mendapatkan nilai 4 untuk menjaga kerahasiaan, dan ketersedian. Mendapatkan nilai 5 untuk integritas. PGP merupakan metode enkripsi yang baik walaupun proses dan konsepnya susah untuk dimengerti.
2. SSL mendapatkan nilai 3 untuk menjaga kerahasiaan, dan ketersediaan data Nilai 4 untuk integritas. SSL merupakan metode enkripsi yang banyak digunakan untuk keamanan transaksi dengan akses web. Komunikasi yang terjadi antara komputer

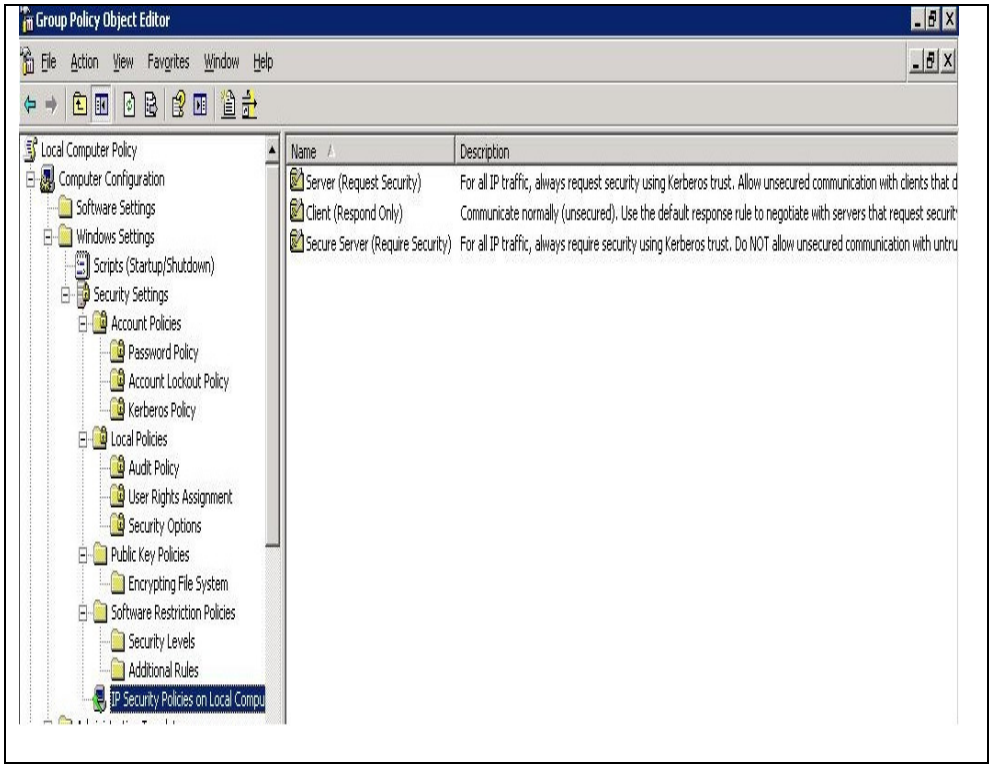
pengguna ke server melalui suatu jalur yang dienkripsi. Kelemahan SSL adalah tidak melindungi dari salah masuknya pengguna ke host yang berbahaya, ataupun tak melindungi apakah suatu kode yang didownload dari suatu situs bisa dipercaya, atau apakah suatu situs itu bisa dipercaya.

3. HTTPS mendapatkan nilai 3 untuk kerahasiaan, integritas, dan ketersediaan data. HTTPS merupakan metode untuk mengakses situs secara aman untuk melakukan transaksi on-line melalui web. Kelemahannya protokol HTTPS (port 443) ini sering di jadikan target oleh peretas.
4. IPSec mendapatkan nilai 4 untuk kerahasiaan, dan ketersediaan data. Nilai 5 untuk integritas. IPSec merupakan enkripsi yang bekerja pada layer 3 (jaringan) pada lapisan OSI. IPSec didesain untuk menyediakan keamanan berbasis kriptografi yang memiliki karakteristik dapat bertukar informasi dan berkualitas. Kelemahannya IPSec terlalu kompleks dan beberapa algoritma yang digunakan dalam IPSec telah dapat dipecahkan sehingga administrator harus menggunakan algoritma lain untuk mendapatkan keamanan yang lebih tinggi.

Protokol PGP dan IPSec mendapatkan nilai tertinggi dengan total skor 60. Pada Windows Server 2003 protokol keamanan jaringan HTTPS dan IPSec di aktifkan seperti yang ditunjukkan oleh Gambar 3.12 dan Gambar 3.13.



Gambar 3.12 Protokol keamanan jaringan Windows Server 2003



Gambar 3.13 Kebijakan IPSec pada Windows Server 2003

3.10 Rancangan Untuk Duplikasi

Perancangan duplikasi diperlukan sebagai cadangan jika peralatan utama mengalami kegagalan. Hal ini diperlukan untuk menjaga keamanan, integritas, dan ketersediaan data. Penilaian mengenai rancangan untuk duplikasi terlihat pada Tabel 3.10.

Tabel 3.10 Matriks keputusan rancangan untuk duplikasi

Nomor	Kriteria	Kerahasiaan		Integritas		Ketersediaan		Total Skor
	Bobot	5		5		5		
		Skor	Jumlah	Skor	Jumlah	Skor	Jumlah	
	Parameter							
1.	Rute alternatif telekomunikasi	3	15	3	15	5	25	55
2.	Server cadangan	3	15	3	15	5	25	55
3.	Sistem RAID	3	15	4	3	4	20	38

Penjelasan matriks keputusan rancangan untuk duplikasi pada Tabel 3.10 dapat diuraikan sebagai berikut :

1. Rute alternatif telekomunikasi mendapatkan nilai 3 untuk kerahasiaan. Jalur komunikasi cadangan bisa disusupi dengan proses curi dengar (*eavesdropping*) jika memiliki proses kriptografi lemah pada komunikasi jaringan. Integritas mendapatkan nilai 3 karena bisa terjadi pola serangan orang tengah (*man-in-the middle*). Penyerang bersikap seperti orang yang memiliki kewenangan untuk mengakses data (dengan cara memantau, menangkap, dan mengatur komunikasi secara transparan) bisa membuat rute ulang pertukaran data. Untuk ketersediaan

mendapatkan nilai 5 karena jika jaringan utama putus proses komunikasi akan dialihkan ke jaringan cadangan.

2. Server cadangan mendapatkan nilai 3 untuk kerahasiaan karena setiap duplikasi akan membuka celah dalam keamanan. Untuk integritas mendapatkan nilai 3 karena celah menembus kewenangan menjadi terbuka jadi dua pada server utama dan cadangan. Ketersediaan mendapatkan nilai 5 karena jika server utama mengalami masalah/mati maka server cadangan akan mengambil alih fungsi utama, dan mempertahankan ketersediaan.
3. Sistem RAID mendapatkan nilai 3 untuk kerahasiaan, nilai 4 integritas dan nilai 4 untuk ketersediaan. Sistem RAID pada kerahasiaan memiliki kelemahan tidak bisa melindungi informasi dari pihak/sistem yang tidak berwenang. Sistem RAID bisa terpengaruh akibat serangan virus (memiliki kegiatan rusak/hapus data). Pada integritas bisa dilanggar pada pihak yang bisa meretas kedalam sistem bisa mengakses sistem RAID dan rentan akan penulisan ulang yang salah akibat kesalahan sistem. Sistem RAID menjamin ketersediaan data jika salah satu cakram keras mengalami kerusakan maka cakram keras pengganti bisa menggantikannya dengan cara diganti saat sistem nyala (*hot swap*). Hal ini dimungkinkan karena sistem RAID ada yang menggunakan sistem penyalinan data ke lebih dari satu buah cakram keras (*mirroring*), pemecahan data ke beberapa cakram keras (*striping*) dan juga deteksi dan koreksi masalah (*error correction code*). Kelemahannya beberapa sistem RAID seperti RAID 0 tidak memiliki metode untuk redundansi, hanya implementasi penyalinan data ke lebih dari satu buah cakram keras. Kerusakan pada

pengatur RAID dan kegagalan akibat kelebihan kapasitas untuk pemulihan data juga dapat berpengaruh atas ketersediaan data.

Rute alternatif komunikasi dan server cadangan mendapatkan nilai tertinggi dengan total skor 55. Rute alternatif komunikasi hanya ditemukan pada satu kantor cabang saja yaitu di daerah Sangatta Kalimantan Timur. Kantor cabang Trakindo Utama Sangatta menggunakan dua penyedia jasa komunikasi *broadband* yaitu Telkom dan Exelcom. Tidak semua cabang perusahaan menggunakan rute alternatif komunikasi. Server cadangan hanya terdapat untuk mesin produksi IBM AS/400 yang terletak di kantor pusat data utama, dan kantor pusat data cadangan di Cikarang, dan mesin BDC direktori aktif dari total sekitar 152 server yang tersebar di pusat data utama, dan di kantor-kantor cabang perusahaan.

BAB IV

REKOMENDASI

Berdasarkan dari sisi komersial bisnis perusahaan yang diteliti penulis menetapkan total standar persentase keamanan yang diharapkan untuk perusahaan adalah 75% sesuai dengan perspektif pengguna. Hal tersebut berdasarkan IBIMA *Publishing* (2010, tersedia di http://www.ibimapublishing.com/journals/CIBIMA/2010/486878/486878.pdf), yang membagi tingkat pengujian keamanan informasi menjadi tingkat rendah (0-49%), tingkat sedang (50-79%), dan tingkat tinggi (80-100%). Angka 75% ditetapkan karena sisi resiko komersial bisnis perusahaan berbeda dengan perusahaan lainnya yang membutuhkan standar keamanan/komitmen tingkat layanan pengguna yang lebih tinggi

seperti bank. Standar keamanan yang lebih tinggi ini sesuai dengan kepentingan/resiko komersial bisnis masing-masing perusahaan seperti misalnya jenis perusahaan jasa perbankan skala besar, perusahaan telekomunikasi, penyedia jasa pusat data, bursa saham dan lainnya.

Perhitungan total persentase didapat dengan rumus **total nilai didapat dibagi total nilai maksimal dikali seratus persen** untuk per parameter. Berdasarkan penilaian parameter-parameter keamanan pada bab 3 maka dapat dijabarkan beberapa rekomendasi bagi perusahaan.

4.1 Manajemen Keamanan Informasi

Persentase keamanan pada manajemen keamanan informasi dapat dilihat pada Tabel 4.1.

Tabel 4.1 Persentase manajemen keamanan informasi

Nomor	Parameter	Nilai	Persentase
1.	Kepala keamanan informasi	40	53.33%
2.	Kepala privasi informasi	30	40%
3.	Manajer keamanan informasi	75	100%
Total		**145**	**64.44%**

Pada Tabel 4.1 terlihat bahwa total nilai persentase yang didapatkan adalah 64.44% dari nilai 75% yang diharapkan. Rekomendasi peningkatan yang diperlukan adalah:

1. Perlu seorang kepala privasi informasi selaku pihak yang berada pada tingkat eksekutif senior, bertanggung jawab terhadap pengaturan resiko, dampak bisnis

terhadap undang-undang/kebijakan kerahasiaan, penggunaan dan menjaga keamanan transaksi bank perusahaan dan keuangan.

2. Perlu seorang kepala keamanan informasi yang bertanggung jawab untuk pengembangan, implementasi dan pengaturan visi, strategi, dan program keamanan korporat organisasi.

4.2 Peran Kewenangan Terhadap Data

Persentase keamanan pada peran kewenangan terhadap data dapat dilihat pada Tabel 4.2.

Tabel 4.2 Persentase peran kewenangan terhadap data

Nomor	Parameter	Nilai	Persentase
1.	Pemilik data	50	66.67%
2.	Pengguna data	35	47%
3.	Petugas data	75	100%
Total		**160**	**71.11%**

Pada Tabel 4.2 terlihat bahwa total nilai persentase yang didapatkan adalah 71.11% dari nilai 75% yang diharapkan. Rekomendasi peningkatan yang diperlukan adalah:

1. Pengguna data harus lebih bertanggung jawab terhadap keamanan data dengan cara selalu menjaga kata sandi mereka untuk akses sumber daya. Penggantian kata sandi secara berkala juga harus dilakukan. Hal ini bisa dilaksanakan dengan pengadaan pelatihan-pelatihan mengenai kesadaran keamanan informasi terhadap karyawan secara berkala.

2. Pemilik data juga harus berhati-hati untuk memberikan akses bagi pengguna data. Tindakan untuk selalu memperbaharui hak akses pengguna jika pengguna sudah pindah ataupun mengundurkan diri wajib dilaksanakan untuk menjaga keamanan informasi perusahaan.

4.3 Kontrol Lingkungan

Persentase keamanan pada control lingkungan dapat dilihat pada Tabel 4.3.

Tabel 4.3 Persentase kontrol lingkungan

Nomor	Parameter	Nilai	Persentase
1.	Pemadaman darurat	15	20%
2.	Suplai daya tanpa interupsi	45	60%
3.	Generator cadangan	75	100%
4.	Sistem transfer daya	75	100%
5.	Pemanas, ventilasi dan pendingin udara	35	47%
6.	Deteksi panas, asap dan api	25	33%
7.	Pemadam api	25	33.33%
8.	Deteksi air	25	33%
	Total	**320**	**53.33%**

Pada Tabel 4.3 terlihat bahwa total nilai persentase yang didapatkan adalah 53.33% dari nilai 75% yang diharapkan. Rekomendasi peningkatan yang diperlukan adalah:

1. Pemadaman darurat harus bisa diminimalisir dengan perawatan jalur elektrik dari penyedia daya menuju pusat data (tempat pengatur ranah utama direktori aktif berada). Penggunaan generator dan perangkat catu daya cadangan bisa membantu ketersediaan pasokan listrik pada pusat data untuk sementara waktu. Pelatihan

simulasi pemadaman darurat pada pusat data perlu dilakukan untuk penilaian seberapa cepat perangkat daya cadangan serta suplai daya tanpa interupsi dapat mengambil alih pasokan daya elektrik pada pusat data.

2. Perawatan pemanas, ventilasi, dan pendingin udara harus dilakukan secara berkala untuk menjaga temperatur pada pusat data tetap berada suhu 16-24º celcius, serta kelembaban sekitar 40-55%. Suhu yang melebihi 24º celcius atau di bawah 16º celcius secara terus menerus dapat menyebabkan kegagalan beroperasi pada server pengatur ranah utama direktori aktif di pusat data.
3. Perawatan secara berkala terhadap deteksi air, panas, api, asap harus dilakukan untuk menjaga sensor bekerja dengan baik pada saat terjadi kejadian di pusat data.
4. Pemadam api harus dirawat secara berkala untuk memastikan pemadam bisa bekerja dengan baik untuk memadamkan api. Masa kadaluarsa pemadam api juga harus diperhatikan, dan harus segera diganti jika memasuki waktu kadaluarsa.

4.4 Penyimpan Aman

Persentase keamanan pada penyimpan aman dapat dilihat pada Tabel 4.4.

Tabel 4.4 Persentase penyimpan aman

Nomor	Parameter	Nilai	Persentase
1.	Penyimpan yang aman	70	93%
2.	Penyimpan di luar	70	93%
3.	Media transportasi penyimpan	33	44%
Total		**173**	**77%**

Pada Tabel 4.4 terlihat bahwa total nilai persentase yang didapatkan adalah 77% melampaui nilai 75% yang diharapkan sehingga tidak ada rekomendasi yang akan diberikan.

4.5 Metode Autentikasi

Persentase keamanan pada penyimpan aman dapat dilihat pada Tabel 4.5.

Tabel 4.5 Persentase metode autentikasi

Nomor	Parameter	Nilai	Persentase
1.	Kata sandi	35	47%
2.	Kartu pintar	35	47%
3.	Token perangkat keras	35	47%
4.	Token perangkat lunak	35	47%
5.	Sidik jari tangan	65	87%
6.	Sidik telapak tangan	65	87%
7.	Geometri tangan	65	87%
8.	Pindai iris mata	65	87%
9.	Pindai retina mata	65	87%
10.	Pindai wajah	65	87%
11.	Tanda tangan dinamik	20	27%
12.	Pola suara	15	20%
Total		**565**	**63%**

Pada Tabel 4.5 terlihat bahwa total nilai persentase yang didapatkan adalah 63% dari nilai 75% yang diharapkan. Rekomendasi peningkatan yang diperlukan adalah:

1. Penggunaan kata sandi yang kompleks seperti gabungan karakter umum dengan karakter khusus dan panjang karakter lebih dari 8 untuk bisa akses informasi.

2. Menjaga kartu pintar, token perangkat keras dan token perangkat lunak agar tidak mudah untuk dicuri atau dipinjam orang lain.
3. Penggunaan perangkat biometrik yang berlapis (misalnya kartu pintar dan geometri tangan) untuk memasuki pusat data atau tempat penyimpan dokumen transaksi keuangan/perbankan perusahaan.

4.6 Proteksi Akses Jaringan

Persentase keamanan pada proteksi akses jaringan dapat dilihat pada Tabel 4.6.

Tabel 4.6 Persentase proteksi akses jaringan

Nomor	Parameter	Nilai	Persentase
1.	Autentikasi Kerberos	45	60%
2.	Firewall jaringan	45	60%
Total		**90**	**60%**

Pada Tabel 4.6 terlihat bahwa total nilai persentase yang didapatkan adalah 60% dari nilai 75% yang diharapkan. Rekomendasi peningkatan yang diperlukan adalah:

1. Penggunaan proteksi akses jaringan (*Network Access Protection*) teknologi Microsoft pada lapisan ke 7 OSI (aplikasi) untuk mengatur komputer berdasarkan tingkat kesehatan dari komputer itu sendiri. Kesehatan disini berarti celah-celah keamanan yang beresiko pada sistem komputer sudah ditambal dengan menggunakan *patch, service pack* terbaru serta antivirus definisi terbaru. Sistem operasi Windows 2003 Server yang terpakai sekarang harus di naikkan ke Windows Server 2008. Semua

komputer klien di naikkan versi ke Windows XP SP3, Windows Vista, atau Windows 7 untuk mendukung proteksi akses jaringan ini.

2. Melakukan uji coba audit keamanan berkala terhadap penggunaan Microsoft Windows *firewall* pada masing-masing komputer pengguna, dan *firewall* pada tingkat jaringan.

4.7 Metode Enkripsi

Persentase keamanan pada metode enkripsi dapat dilihat pada Tabel 4.7.

Tabel 4.7 Persentase metode enkripsi

Nomor	Parameter	Nilai	Persentase
1.	Enkripsi kunci rahasia	45	60%
2.	Enkripsi kunci umum	45	60%
3.	Tanda tangan digital	55	73%
Total		**145**	**64%**

Pada Tabel 4.7 terlihat bahwa total nilai persentase yang didapatkan adalah 64% dari nilai 75% yang diharapkan. Rekomendasi peningkatan yang diperlukan adalah:

1. Menggunakan metode enkripsi simetrik *Advanced Encryption Standard* (AES), yang memiliki 128, 192, atau 256-bit kunci untuk memperlama waktu peretas untuk mendekrip pesan. AES merupakan perbaikan dari metode *Data Encryption Standard* (DES) yang hanya menggunakan kunci 40-bit, 56-bit dan 3×56-bit (Triple DES).
2. Implementasi perangkat keras enkripsi pada sisi gerbang keluar masuk surat elektronik (*email gateway*) untuk pengaman kiriman pesan, menyediakan fleksibilitas

yang mendukung semua enkripsi surat elektronik. penjagaan kerahasiaan transaksi dan komunikasi surat elektronik. Perangkat keras tersebut salah satunya adalah produk Cisco IronPort Email and Web Security.

4.8 Infrastruktur Kunci Publik

Persentase keamanan pada proteksi akses jaringan dapat dilihat pada Tabel 4.8.

Tabel 4.8 Persentase infrastruktur kunci publik

Nomor	Parameter	Nilai	Persentase
1.	Penerbit sertifikat	60	80%
2.	Kewenangan registrasi	60	80%
3.	Sertifikat daftar penolakan	60	80%
4.	Sertifikat pernyataan praktek	45	60%
	Total	225	75%

Pada Tabel 4.7 terlihat bahwa total nilai persentase yang didapatkan adalah 75% sesuai dengan nilai 75% yang diharapkan sehingga tidak ada rekomendasi yang akan diberikan.

4.9. Protokol Keamanan Jaringan

Persentase keamanan pada proteksi akses jaringan dapat dilihat pada Tabel 4.9.

Tabel 4.9 Persentase protokol keamanan jaringan

Nomor	Parameter	Nilai	Persentase
1	PGP	65	87%
2	SSL	50	67%
3	HTTPS	45	60%
4	IPSec	65	87%
	Total	225	75%

Pada Tabel 4.9 terlihat bahwa total nilai persentase yang didapatkan adalah 75% dari nilai 75% yang diharapkan yang diharapkan, sehingga tidak ada rekomendasi yang akan diberikan.

4.10. Rancangan Untuk Duplikasi

Persentase keamanan pada proteksi akses jaringan dapat dilihat pada Tabel 4.10.

Tabel 4.10 Persentase rancangan untuk duplikasi

Nomor	Parameter	Nilai	Persentase
1	Rute alternatif telekomunikasi	55	73%
2	Server cadangan	55	73%
3	Sistem RAID	38	51%
	Total	148	66%

Pada Tabel 4.10 terlihat bahwa total nilai persentase yang didapatkan adalah 66% dari nilai 75% yang diharapkan. Rekomendasi peningkatan yang diperlukan adalah:

1. Pengadaan rute alternatif telekomunikasi di cabang-cabang perusahaan yang bergerak di bidang pertambangan, dan kegiatan komersial yang bersifat kritikal. Hal ini dikarenakan kegiatan operasi di tambang berlangsung selama 24 jam setiap hari yang membutuhkan ketersediaan komunikasi yang tinggi.
2. Pengadaan server direktori aktif cadangan (BDC) di cabang-cabang perusahaan untuk menjaga ketersediaan direktori aktif pda kantor cabang jika terjadi kegagalan server direktori aktif utama (PDC).

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan studi kasus yang telah dilakukan, mulai dari tahap studi pustaka, studi observasi, perancancangan dan implementasi sistem, maka dari hasil yang didapatkan bisa ditarik kesimpulan sebagai berikut:

1. Dari kesepuluh kriteria perlindungan aset informasi yang di analisa, tujuh kriteria diantaranya ditemukan pada direktori aktif Windows Server 2003 yang di implementasikan pada perusahaan.
2. Skor nilai tertinggi ditemukan pada parameter petugas data pada kriteria peran kewenangan terhadap data dengan total nilai 75. Kriteria petugas data ditemukan pada perusahaan. Skor nilai terendah ditemukan di parameter pemadaman darurat di

kriteria kontrol lingkungan dan pada parameter autentikasi pola suara di metode autentikasi. Keduanya mendapatkan nilai 15.

3. Implementasi peningkatan teknologi metode autentikasi, kontrol lingkungan, dan proteksi akses jaringan harus disesuaikan dengan kesepakatan tingkatan layanan (*service level agreement*) perusahaan.
4. CISA bisa digunakan untuk menganalisa keamanan direktori aktif pada perusahaan yang memiliki skala komersial bisnis seperti PT. Tiara Marga Trakindo group serta perusahaan lainnya yang memiliki skala komersial bisnis yang sama.

5.2 Saran-saran

Penulis memahami ada banyak metode untuk melakukan analisa/audit keamanan informasi perusaahaan yang lebih detil. Untuk itu penulis menyarankan antara lain:

1. Adanya kesadaran akan resiko keamanan informasi bagi semua pihak agar dapat berhati-hati dalam memanfaatkan dan menyebarkan informasi.
2. Tingkat keamanan informasi merupakan salah satu barometer bagi pelanggan untuk mempercayai integritas dan imej bisnis dari suatu perusahaan. Tingkat keamanan tersebut harus diukur secara berkala dengan menggunakan sistem audit keamanan.
3. Menggunakan audit keamanan informasi lain seperti ISO/TS 27790:2009 mengenai pengukuran manajemen keamanan informasi, dan ISO/IEC 29116-2008 untuk manajemen resiko keamanan informasi pada perusahaan.

DAFTAR PUSTAKA

Bragg, Roberta. 2005. *Security: A Technical Reference*. Columbus:Addison-Wesley.

Desmond, Brian. 2008. *Active Directory: Designing, Deploying, and Running Active Directory.* Massachusetts:O'Reilly Media.

Herjanto, Eddy. 2009. *Sains Manajemen: Analisis Kuantitatif Untuk Pengambilan Keputusan.* Jakarta: Grasindo.

Kouti, Sakari. 2004. *Inside Active Directory*. Columbus: Addison-Wesley.

Kurniawan, Yusuf. 2005. *Kriptografi: Keamanan Internet dan Jaringan Komunikasi.* Jakarta: Informatika.

L. Cannon, David. 2008 *CISA Certified Information Systems Auditor Study Guide Second Edition*. Indiana: Wiley Publishing Inc.

Muslich, Mohammad. 2009. *Metode Pengambilan Keputusan Kuantitatif*. Jakarta: Bumi Aksara.

Rosyid, D.M. 2009. *Optimasi: Teknik Pengambilan Keputusan Secara Kuantitatif*. Surabaya: ITS Press.

Sukamaaji, Anjik. 2008. *Jaringan Komputer : Konsep Dasar Pengembangan Jaringan dan Keamanan Jaringan.* Yogyakarta: Andi.

Supranto, J. 2005. *Teknik Pengambilan Keputusan*. Jakarta: Rineka Cipta

Syamsi, Ibnu. 2007. *Pengambilan Keputusan dan Sistem Informasi*. Jakarta: Bumi Aksara.

Tanenbaum, Andrew S. 2006 *Modern Operating System Second Edition*. New Jersey: Prentice Hall, Inc.

Wirija, Sudantha. 2003. *Microsoft Windows Server 2003*. Jakarta: Elex Media Komputindo.

Curriculum Vitae

Data Pribadi

Nama	: Bil Fauzi
Jenis kelamin	: Pria
Tempat/Tanggal lahir	: Medan, 02 Desember 1978
Kewarganegaraan	: Indonesia
Agama	: Islam
Alamat	: Jl.Lelie 262 Komp.Bukit Nusa Indah Sarua Ciputat 15414
Telepon/HP	: 021-7491773 / 081510272717
E-mail	: bil.fauzi@yahoo.co.id

Pendidikan

›› Formal

1985 – 1991	: SD Pertiwi, Medan
1991 – 1994	: SMP Pertiwi, Medan
1994 – 1997	: SMU Negeri 3, Medan
1997 – 2002	: Program Sarjana (S1) Sastra Inggris, Universitas Sumatera Utara, Medan
1998 – 2001	: Program Diploma (D3) Ilmu Komputer, Universitas Sumatera Utara, Medan
2005 – 2010	: Program Sarjana (S1) Teknik Informatika, Universitas Mercu Buana, Jakarta

›› Non Formal

2004	: Cisco Certified Network Associate training
2006	: HP Open View training
2007	: Cisco network admission control workshop
2008	: Ethical Hacker workshop

2009	: Configuring and troubleshooting Windows Server 2008 active directory domain services
2010	: VSphere 4.0 training
2010	: Brown Belt Lotus Domino 8.0 training

Sertifikasi

2009	: Microsoft Certified IT Professional Server Administrator
2009	: Microsoft Certified IT Professional Enterprise Administrator
2010	: VMWare Certified Professional 4.0

Pengalaman kerja

Bekerja di **PT. Mitra Solusi Telematika, TMT group,** Jakarta

Periode : 2003 – 2010

Status : Pegawai tetap

Posisi : System Administrator