RIWAYAT HIDUP

Nama	:	Prio Hartono, S.Kom
Tempat / Tanggal Lahir	:	Jakarta, 28 Oktober 1982
Alamat Rumah	:	Komplek Reni Jaya Blok D 20 / 7 Kecamatan Sawangan
Nomor Telepon	:	021-7434746; 085781886217
Email	:	rioh24@gmail.co.id
Riwayat Pendidikan	:	1. TK Islam Nurul Hidayah (1987-1988)
		2. SD Islam Nurul Hidayah (1988-1994)
		3. SMPN I Pamulang (1994-1997)
		4. SMUN I Serpong (1997-2000)
		5. Universitas Gunadarma (2000-2006)
Riwayat Pekerjaan	:	IT Consultant (2006-sekarang)

ABSTRAK

Prio Hartono S.Kom (92310023)

Analisis Dampak Dan Pengendalian Serangan *Malware* Pada Keamanan Sistem Jaringan Komputer PT XYZ

Tesis, Jurusan Perangkat Lunak Sistem Informasi, Fakultas Sistem Informasi, Universitas Gunadarma, 2012

(xiii + 83 halaman + Lampiran)

PT XYZ merupakan perusahaan manufaktur otomotif terbesar di Indonesia dan memiliki beberapa anak cabang di Indonesia sehingga membutuhkan sistem jaringan komputer untuk melakukan pertukaran data dan informasi.

Namun, untuk pertukaran informasi dengan ukuran data yang besar, dibutuhkan bukan hanya sekedar sistem jaringan komputer, namun juga media penyimpanan yang bersifat *mobile* dan *user friendly* dan digunakanlah *USB Storage*, namun penggunaan *USB Storage* tanpa adanya kontrol yang baik, mempunyai dampak yang kurang baik bagi sistem jaringan komputer, dikarenakan *USB Storage* merupakan media perantara bagi *malware* untuk melakukan penyerangan dan penyebarannya di dalam sistem jaringan komputer.

Penelitian ini bertujuan untuk melihat dampak dari serangan *malware* bagi sistem jaringan komputer dan bagaimana mengurangi jumlah serangan *malware* dengan menganalisis sumber serangan *malware* dan mengatasi jumlah serangan *malware* langsung pada sumbernya. Hasil penelitian ini menunjukkan bahwa serangan *malware* berdampak negatif terhadap sistem jaringan komputer dan mengatasi serangan *malware* langsung kepada sumbernya berhasil menurunkan jumlah serangan *malware*.

Kata Kunci: Analisis Dampak, Keamanan Sistem Jaringan Komputer, *Malware*

DAFTAR PUSTAKA (1994-2012)

KATA PENGANTAR

Puji dan syukur penulis sampaikan kepada ALLAH SWT yang telah memberikan rahmat dan hidayah-Nya serta nikmat yang selalu dicurahkan terutama nikmat sehat kepada penulis, sehingga penulis dapat menyelesaikan Tesis yang berjudul "**Analisis Dampak Dan Pengendalian Serangan *Malware* Pada Keamanan Sistem Jaringan Komputer PT XYZ**" ini dengan baik.

Tujuan dari penulisan Tesis ini adalah dalam rangka memenuhi persyaratanyang diperlukan dalam memperoleh gelar Magister Manajemen Sistem Informasi pada Universitas Gunadarma. Hasil dari tesis ini, penulis persembahkan untuk bangsa dan negara Indonesia tercinta.

Penulis menyadari sepenuhnya bahwa tulisan yang telah tersusun ini bukanlah hasil kerja penulis semata, namun terdapat bantuan dari berbagai pihak yang turut membantu dalam penyelesaian Tesis ini baik berupa materil maupun moril. Oleh karena itu pada kesempatan ini penulis bermaksud mengucapkan terima kasih dan penghargaan sebesar-besarnya kepada:

1. Ibu Prof. Dr. E. S. Margianti, SE., MM., selaku Rektor Universitas Gunadarma.
2. Bapak Prof. Dr. Yuhara Sukra, MSc., selaku Koordinator Program Pascasarjana Universitas Gunadarma.
3. Bapak Prof Dr. Ir. Bambang Suryawan, MT, selaku Direktur Program Pascasarjana Universitas Gunadarma.
4. Ibu Dr. Renny Nurainy, SE., MM selaku pembimbing materi dan penulisan Tesis atas segala arahan, masukan serta motivasi terhadap penulis.
5. Bapak, Ibu dan adik dirumah yang selalu senantiasa membimbing dan mendukung penulis dalam menyelesaikan studi Pasca Sarjana ini.
6. Direktur dan General Manager perusahaan tempat penulis bekerja yang mengizinkan dan memberi dukungan kepada penulis dalam melanjutkan kuliah Pasca Sarjana di Universitas Gunadarma.

7. Rekan-rekan kerja khususnya Asih Setianingsih yang senantiasa membantu penulis dalam proses penyelesaian Tesis ini.
8. Seluruh pihak yang tidak bisa penulis sebut satu-persatu yang telah memberikan dukungan baik langsung maupun tidak langsung

Penulis menyadari bahwa penulisan Tesis ini masih jauh dari sempurna, baik dari penyajian materi maupun dari penyajian secara redaksional. Oleh karena itu dengan tangan terbuka penulis menerima segala kritikan dan saran yang membangun untuk nantinya dijadikan sebagai bahan perbaikan bagi penulisan selanjutnya di masa yang akan datang.

Semoga Tesis yang penulis buat ini dapat bermanfaat adanya,

Jakarta, 28 Maret 2013

Prio Hartono, S.Kom

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I
PENDAHULUAN

1.1 Latar Belakang

Perkembangan *Malware* akhir-akhir ini sangat berdampak buruk bagi kinerja perusahaan, hampir semua perusahaan menggunakan sistem komputer yang saling terhubung menggunakan jaringan komputer, dan mayoritas menggunakan *USB Storage* sebagai media dalam penyimpanan dan pertukaran data. Hal inilah yang dimanfaatkan *malware* atau yang lebih kita kenal sebagai *virus*, untuk menyebar dan merusak data-data ataupun sistem operasi komputer dan lebih parah lagi, dapat merusak perangkat keras komputer seperti *motherboard, prosesor, memory dan harddisk*. Jika hal ini terjadi bagi seorang pengguna komputer atau *notebook* dan bersifat pemakaian pribadi atau perorangan, mungkin dampaknya hanya dirasakan oleh satu atau dua orang, namun jika hal ini dialami oleh perusahaan, dampaknya akan sangat luas dan bahkan akan berdampak kepada produktifitas perusahaan, dan juga berdampak kepada keuangan perusahaan.

Malware komputer atau yang lebih dikenal dengan sebutan *Virus*, adalah sebuah perangkat lunak atau program yang merusak sistem komputer atau melakukan proses yang tidak diinginkan pada sistem operasi komputer. Secara teknis, *malware* memiliki istilah yang lebih luas karena mencakup *virus, worms, backdoors, trojan*.

Namun, *malware* yang biasa kita dengar dalam kehidupan sehari – hari adalah *virus* komputer. *Malware* komputer telah menjadi ancaman utama pada sistem komputer dan jaringan sejak tahun 1990. Namun,belakangan ini *malware* mengalami perkembangan yang cukup pesat. *Malware* mengalami peningkatan dalam fungsionalitas dan karakteristik (Sadia Noreen, 2009).

Pada Tahun 2011 – 2012, terjadi serangan *malware* yang menyerang hampir seluruh pengguna komputer di seluruh dunia. Dimana banyak *file* dan dokumen *office* yang disembunyikan , dirusak dan bahkan terhapus oleh *malware* ini dan tentunya hal ini sangatlah mengganggu kinerja perusahaan di karenakan banyaknya laporan-laporan yang disimpan dalam *format office*.

Pada PT XYZ, serangan *malware* yang sering terjadi justru bukan dari luar jaringan *WAN / LAN*, melainkan dari dalam jaringan. Serangan tersebut bersumber dari *USB Storage* yang terinfeksi *malware* dari luar area jaringan, dimana *malware* berasal dari komputer pribadi milik pegawai / komputer warnet yang menyebabkan sistem sekuriti perusahaan tersebut terganggu. *malware* tersebut akan menyebar melalui jaringan, sehingga kinerja komputer dan jaringan akan menurun, khususnya *File Server Storage*. Oleh sebab itu, masalah *malware* pada PT XYZ tersebut haruslah diperhatikan karena akan mengganggu produktivitas dan kinerja perusahaan. Serangan *malware* juga terjadi pada *server thin client* yang mengakibatkan sebanyak 500 pengguna *thin client* tidak dapat mengoperasikan *thin client*. Perlu dicatat bahwa semua *PC, Notebook* maupun *server Thin Client* yang terserang menggunakan *anti Malware* ternama dan selalu terbaharui.

1.2 Tujuan

Adanya fasilitas penggunaan *USB Storage* oleh perusahaan tanpa adanya pengawasan dari pihak perusahaan akan semakin memudahkan *malware* untuk menyebar pada jaringan dan melakukan aksinya. Fasilitas yang diberikan perusahaan ini sebenarnya bertujuan untuk memudahkan karyawannya untuk saling bertukar informasi dari berbagai negara demi produktifitas dan kinerja perusahaan. Namun kebijakan ini berbanding terbalik dengan pendapat pakar TI bahwa : Kemudahan (Kenyamanan) mengakses informasi berbanding terbalik dengan tingkat keamanan sistem informasi itu sendiri, dengan kata lain semakin mudah orang mengakses dan bertukar informasi, maka akan semakin rendah pula

tingkat keamanan yang diberlakukan oleh kebijakan perusahaan. Semakin tinggi tingkat keamanan yang diberlakukan oleh perusahaan maka akan semakin sulit dan rumit untuk mengakses informasi. Berbagai macam gangguan keamanan jaringan komputer dapat menggangu kinerja perusahaan dan dalam kasus ini dapat mengganggu produksi dan mengakibatkan kerugian materi perusahaan.

Adanya data yang rusak, *file* yang hilang, rusaknya *file server*, matinya jaringan akibat serangan *malware* baik dari dalam maupun luar jaringan itu sendiri merupakan salah satu gangguan keamanan yang dapat terjadi dan merugikan perusahaan. Hal tersebut bisa saja terjadi baik ketidaksengajaan *user* ataupun ada yang dengan sengaja melakukannya demi kepentingan pribadi atau pihak lain. Oleh karena itu, seharusnya masalah keamanan sistem jaringan komputer khususnya *malware* menjadi salah satu aspek penting dari sebuah sistem informasi di perusahaan. Namun pada kenyataannya hal ini sering kali kurang mendapat perhatian serius dari perusahaan khususnya divisi *infra* dan *security*. Berdasarkan uraian diatas, maka permasalahan yang akan dikaji dalam penelitian ini antara lain mengenai :

(1) Bagaimanakah dampak serangan *malware* pada keamanan sistem jaringan komputer pada PT XYZ ?

(2) Bagaimanakah pengendalian serangan *Malware* pada sistem jaringan komputer pada PT XYZ ?

1.3 Batasan Masalah

Sebagai pedoman dalam menulis tugas akhir ini maka diperlukan batasan masalah sehingga pembahasan menjadi terarah. Batasan yang dimaksud tersebut adalah :

(1) Pembahasan sistem keamanan jaringan komputer di lingkungan PT XYZ pada tahun 2012.

(2) Pengendalian serangan *malware* pada sistem jaringan komputer menggunakan *USB Storage Controlling* di PT XYZ.

1.4 Tujuan Penelitian

Berdasarkan perumusan masalah yang telah di ceritakan diatas, maka penelitian yang dilakukan di perusahaan ini bertujuan untuk :

(1) Menggambarkan dampak serangan *malware* pada sistem jaringan komputer di PT XYZ.

(2) Menganalisis pengendalian keamanan sistem jaringan komputer PT XYZ.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat bermanfaat bagi perusahaan dan pembaca, antara lain yaitu :

(1) Bagi perusahaan dapat meningkatkan sistem keamanan jaringan komputer.

(2) Bagi pembaca, hasil penelitian ini diharapkan sebagai referensi untuk penelitian selanjutnya ataupun pihak lain yang memerlukan informasi mengenai kemanan sistem informasi khususnya *Malware*.

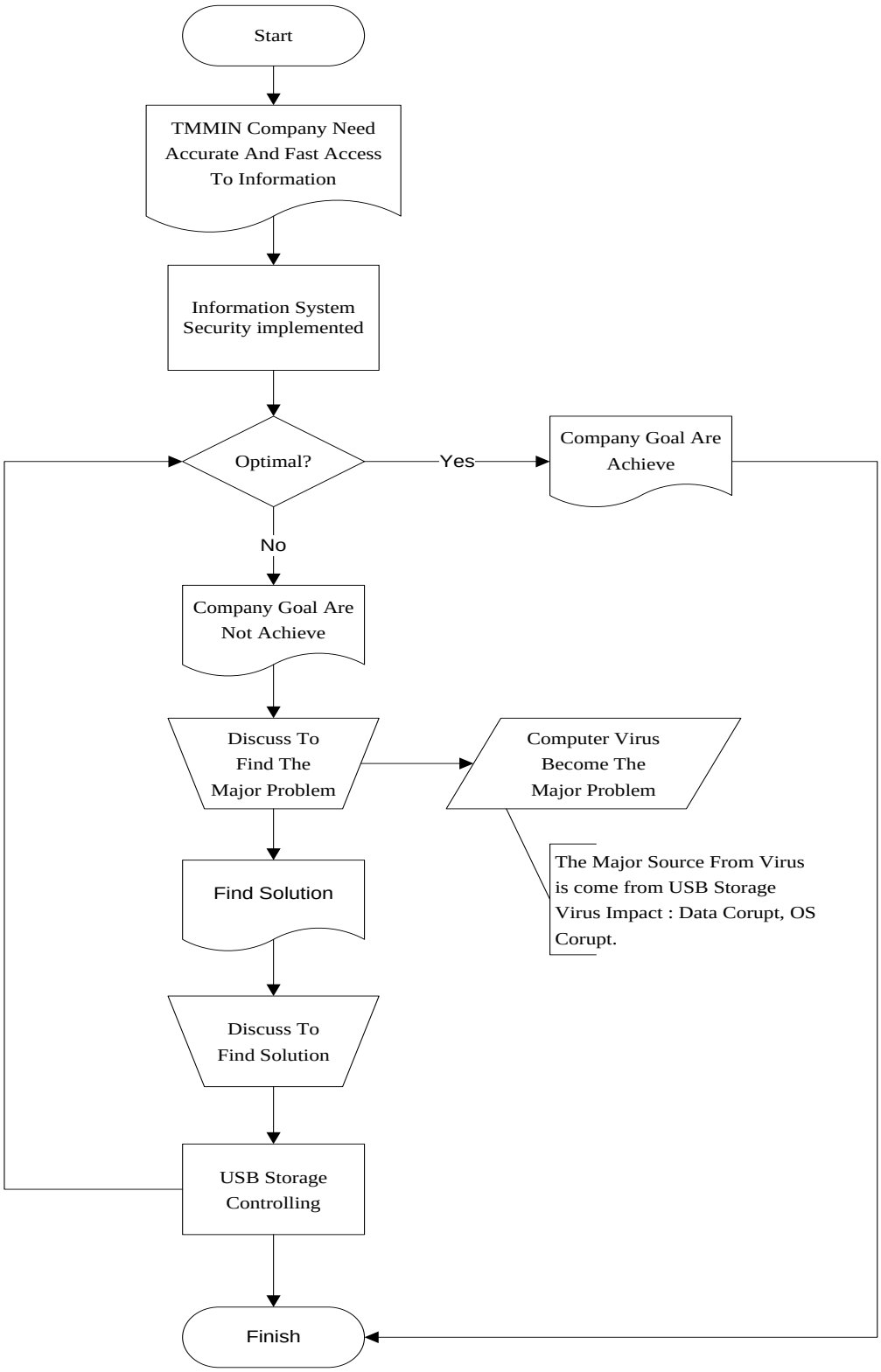
1.6 Kerangka Penelitian

PT XYZ ini merupakan perusahaan multinasional terkemuka yang berbasis di jepang yang memiliki banyak affiliasi dan anak perusahaan serta sering berhubungan dengan para *supplier*. Saat ini perusahaan telah mengimplementasikan teknologi jaringan komputer dalam mendukung kegiatan operasional bisnisnya yang semakin luas dan memerlukan pengambilan keputusan yang semakin kompleks. Tujuan dari implementasi teknologi tersebut adalah agar adanya kemudahan dalam mengakses informasi yang dibutuhkan secara cepat dan

akurat. Hal ini dikarenakan di dalam dunia bisnis yang berorientasi untuk mendapatkan keuntungan sebesar-besarnya dan pengeluaran yang sekecil-kecilnya seringkali membutuhkan pengambilan keputusan secara cepat melalui informasi yang akurat.

Jika keamanan sistem informasi yang dimiliki telah berjalan optimal, maka kinerja perusahaan akan berjalan dengan baik tanpa ada gangguan, namun jika kemanan sistem informasi tidak berjalan optimal yang terutama berasal dari internal perusahaan yaitu adanya jalur masuk serangan *Malware* melalui *USB Storage* yang boleh digunakan di area perusahaan maupun diluar area perusahaan sehingga jalan masuk *Malware* untuk menyebar dan beraksi akan semakin mudah dan terbuka lebar. Rusaknya data, hilangnya data, rusaknya sistem operasi, adanya pencurian *password*, sampai paling parah adalah rusaknya *hardware* akibat serangan *Malware* dapat mengganggu kinerja perusahaan untuk mencapai tujuan utamanya yaitu mencapai keuntungan optimal.

Dengan demikian dapat membantu perusahaan untuk mencapai tujuannya. Secara garis besar, penjelasan tersebut dapat dilihat pada gambar kerangka pemikiran berikut ini.



Gambar 1.1 Kerangka Pemikiran Pengendalian Malware

BAB II

TELAAH PUSTAKA

2.1 *Malware* Komputer

Berdasarkan *Sadia Noreen (2009). Malware* komputer atau yang lebih dikenal dengan sebutan *virus*, adalah sebuah perangkat lunak atau program yang merusak sistem komputer atau melakukan proses yang tidak diinginkan pada sistem operasi komputer. Secara teknis, *malware* memiliki istilah yang lebih luas karena mencakup v*irus, worms, backdoors, trojan*.

Namun, *malware* yang biasa kita dengar dalam kehidupan sehari – hari adalah *virus* komputer. *Malware* komputer telah menjadi ancaman utama pada sistem komputer dan jaringan sejak tahun 1990. Namun,belakangan ini *malware* mengalami perkembangan yang cukup pesat. *Malware* mengalami peningkatan dalam fungsionalitas dan karakteristik.

Menurut Penulis, *Malware* merupakan hasil pemikiran manusia yang di tuangkan melalui kumpulan kode-kode program komputer yang bersifat merugikan pemakai komputer dengan beberapa tujuan, yaitu:

- Mencuri informasi rahasia pribadi penguna komputer seperti kata sandi, nomor rekening, nomor kartu kredit berikut kata sandinya.
- Ajang pamer untuk membuktikan kemampuannya.
- Sarana untuk menyuarakan isi hati atau pemikiran si pembuat *malware*.
- Sabotase terhadap fasilitas yang menggunakan jaringan komputer.
- Aksi balas dendam terhadap seseorang atau instansi tertentu.

- Bentuk protes terhadap kebijakan suatu instansi atau organisasi tertentu yang dimana kebijakan tersebut merugikan banyak pihak dan terutama si pembuat *malware* itu sendiri.

2.2 Jenis-jenis *Malware*

Berdasarkan *Tahan, Rokach dan Shahar (2012).* ***Malware*** dapat dikategorikan menjadi beberapa bagian:

2.2.1 *Virus*

2.2.1.1 Definisi *Virus*

Berdasarkan *Eugene H.Spafford (1994).* Istilah *virus* komputer berasal dari istilah biologi yaitu *virus* secara biologis yang secara bahasa latin artinya adalah racun, secara sederhana infeksi *virus* secara biologis disebarkan oleh sel berbahaya (sebuah sel kecil yang terlindungi dan mengandung materi genetik yang berbahaya) menyuntik lebih dalam isi materi genetik yang ada kedalam sebuah sel–sel organisme yang lebih besar. Sel-sel tersebut kemudian akan terinfeksi dan terkonversi menjadi tempat untuk memproduksi tiruan-tiruan dari *virus* tersebut. Begitu juga dengan *virus* komputer, yang merupakan segmen dari kode mesin (biasanya 200-4000 *bytes*) yang akan mengkopi programnya sendiri (atau memodifikasi versinya sendiri) kedalam "*host*" program ketika telah aktif. Ketika program yang terinfeksi telah berjalan, kode *virus* tereksekusi dan *virus* menyebar ke area yang lebih jauh. Kadang kala, yang programnya lebih sederhana dari aplikasi : kode *boot*, *device drivers*, dan *command interpreter* juga dapat terinfeksi.

Pada umumnya *virus* komputer, dapat dibagi menjadi dua tipe, yaitu *virus* komputer yang dibuat untuk tujuan penelitian/studi (*virus* ini tidak dipublikasikan) dan *virus* komputer yang dibuat untuk merusak sistem komputer pada umumnya.

2.2.1.2 Sistem Kerja *Virus*

Secara umum, *virus* memiliki cara kerja yang relatif sama. Berbagai kemampuan yang dilakukan oleh *virus* diantaranya dapat mencuri sebuah informasi,memeriksa dan merusak suatu *file*,berkembang biak, menularkan diri, melakukan manipulasi, menyembunyikan diri, dan dapat bertahan hidup. Dalam mendapatkan sebuah informasi dari sebuah directory, *virus* tersebut memilih *file-file* yang bisa ditulari. Ketika pengguna membuka program atau *file* yang sudah terinfeksi oleh *virus*, itulah data yang dibutuhkan oleh *virus* tercipta.

Virus biasanya melakukan pengumpulan data dan menyimpannya di dalam *memory*. Ketika komputer dimatikan, data tersebut akan hilang. Data tersebut akan tercipta kembali ketika komputer dihidupkan. Biasanya data-data tersebut disimpan sebagai *hidden file* oleh *virus*. Sebelum melakukan penularan atau penyebaran, *virus* akan memeriksa *file* yang akan ditumpanginya. Hal ini tidak jauh berbeda dengan perilaku *virus* pada manusia. *Virus* akan memberikan suatu tanda pada *file* atau program yang telah terinfeksi, sehingga akan mudah dikenali oleh *virus* tersebut, seperti memberikan suatu *byte* atau tanggal pembuatan yang unik di setiap *file* yang telah terinfeksi.

Proses penggandaan diri yang dilakukan oleh *virus* terjadi setelah memberikan tanda, dilanjutkan dengan menuliskan kode objek *virus* pada *file* yang telah diperiksa. Proses penggandaan dilakukan dengan cara menghapus atau mengubah *file* induknya. Setelah itu, terciptalah suatu *file* yang berisi program *virus* dengan menggunakan nama asli atau dengan cara menumpang pada *file* yang sudah terinfeksi. Memanipulasi suatu *file* yang sudah terinfeksi dapat membahayakan dan dapat merusak suatu komputer. Kegiatan memanipulasi ini biasanya bertujuan untuk mempopulerkan nama pembuat *virus*.

Kemampuan lain yang dimiliki oleh sebuah *virus* adalah menyembunyikan diri. Dengan cara ini, *virus* disimpan dalam bentuk kode mesin, digabung dengan program lain, dan menyimpannya di *boot* record atau track pada sebuah *disk*.

Program dibuat sependek mungkin, agar *file* yang telah terinfeksi tidak berubah ukurannya secara signifikan. Seperti *virus* dalam dunia kedokteran, *virus* komputer juga memiliki siklus hidup yang dapat dibagi menjadi empat tahap, sebagai berikut.

1. Waktu istirahat, umumnya *virus* menentukan tanggal atau waktu untuk menghentikan dan mengaktifkan *virus* pada komputer.
2. Waktu penyebaran, umumnya *virus* mereplikasi dirinya dengan menggandakan diri dalam suatu program ke sebuah tempat di media penyimpanan, seperti *harddisk*, *RAM*, dan *flashdisk*.
3. Waktu aktif, pada waktu tertentu *virus* akan mengaktifkan diri.
4. Waktu eksekusi, artinya *virus* yang telah aktif dan mulai kegiatannya.

2.2.1.3 Jenis-jenis *Virus*

2.2.1.3.1 *Virus* Yang Menyerang Sistem

2.2.1.3.1.1 Boot Sector Virus

Sebuah PC dapat terinfeksi oleh *boot* sector *virus* jika PC tersebut di-*boot* atau di *reboot* dari *floppy disk*, *flashdisk*, atau dari *portable harddrive* yang telah terinfeksi oleh jenis *virus* ini. *Boot* sector *virus* tidak menyebar melalui jaringan komputer, tetapi biasanya terjadi oleh pengunaan *Storage* yang telah terinfeksi.

Virus boot sector bekerja dengan cara memindahkan atau mengganti *boot* sector yang asli dengan program *booting virus*. Dengan cara ini, *virus* akan selalu aktif ketika komputer dijalankan. Setelah *operating system* aktif, *virus* tersimpan di dalam *memory* dan *virus* pun akan menginfeksi komputer dan menyebar ke seluruh media penyimpanan. Berikut contoh *virus* ini.

1. Varian *virus* wyx, wyx.C(B) yang menginfeksi *boot* record dan *floppy*. Panjangnya sekitar 520 *bytes* dan memiliki karakteristik tinggal di *memory* dan dalam kondisi terenkripsi.

2. Varian V-sign, *virus* ini menginfeksi *master boot* record dengan panjang 520 *bytes*.

2.2.1.3.1.2 Companion Virus

Companion virus adalah *virus* yang bekerja dengan berpura-pura menggantikan *file* yang akan diakses oleh pengguna, contohnya pada *system* operasi *DOS*. *FileA.EXE* dapat diinfeksi dengan membuat sebuah *file* dengan nama *A.COM*. *DOS* terlebih dahulu akan mencari *file* berekstensi *COM* sebelum *file* ekstensi EXE. Setelah *A.COM* dieksekusi, dilanjutkan dengan mengeksekusi *A.EXE*, sehingga *file* tersebut ikut terinfeksi. Cara lainnya adalah dengan menempatkan sebuah *file* dengan nama yang persis sama pada cabang lain dari *file tree*, sehingga bila *file* palsu ini ditempatkan secara tepat dan terjadi kesalahan menuliskan jalur yang lengkap, akan berakibat tereksekusinya *file* palsu tersebut.

2.2.1.3.1.3 Stealth Virus

Stealth virus menguasai perintah-perintah pada DOS yang sering dikenal dengan "*interrupt interceptor*". *Virus* ini mengendalikan instruksi level DOS. Berikut contoh *virus* ini:

1. Vmem(s), *virus* ini menginfeksi *file* *.EXE, *.SYS, dan *.COM, memiliki panjang 3275 *bytes* dengan karakteristik menetap di *memory* dengan ukuran tersembunyi dan di-enkripsi.

2. Yankee.XPEH.4928, menginfeksi *file* *.COM dan *.EXE dengan panjang 4298 *bytes*, memiliki karakteristik menetap di *memory*, ukurannya tersembunyi dan memiliki pemicu.

2.2.1.3.1.4 Polymorphic Virus

Virus ini mirip dengan *virus* influenza atau HIV. *Virus* ini mempunyai kemampuan mengecoh *anti virus* dengan mengubah strukturnya setiap kali menginfeksi suatu *file*. Contoh *virus* ini adalah Necropolis A/B, *virus* ini menginfeksi *file* *.*EXE*, *.*COM* dengan ukuran 1963 *bytes*. Memiliki karakteristik menetap di *memory*, ukurannya tersembunyi, ter-enkripsi, dan strukturnya dapat berubah.

2.2.1.3.1.5 File Virus

Virus file merupakan *virus* yang bekerja dengan cara menginfeksi secara langsung pada sistem operasi dan akan merusak *file* dengan ekstensi *.EXE atau *.COM, sehingga ukuran *file* yang diserang akan berubah dan merusak sistem. *Virus* jenis ini menginfeksi *file* lain ketika program yang telah terinfeksi dijalankan. Oleh sebab itu, jenis *virus* ini dapat menyebar melalui jaringan komputer dengan cepat.

2.2.1.3.1.6 Tunneling Virus

Tunneling Virus bekerja dengan cara mengambil alih *interrupt handlers* pada *DOS* dan *BIOS*. Kemudian meng-install dirinya**,** sehingga berada di bawah program-program lainnya. Akibatnya, *virus* ini dapat terhindar dari hadangan program anti*virus*.

2.2.1.3.1.7 Multipartition Virus

Virus ini merupakan gabungan dari *virus boot* sector dengan *virus file*.*Virus* ini bekerja menginfeksi *file* dengan ekstensi *.*EXE atau* *.*COM* dan menginfeksi *boot sector*.

2.2.1.3.2 *Virus* Yang Menyerang Data

2.2.1.3.2.1 Macro Virus

Virus makro merupakan *virus* yang dibuat dengan bahasa pemrograman yang terdapat pada suatu aplikasi dan akan berjalan dengan baik pada aplikasi pembentuknya. Sebagai contoh, *virus* makro yang dibuat pada aplikasi *word* akan berjalan pada aplikasi *microsoft word*. Pada umumnya, *virus* ini akan memodifikasi *file NORMAL.DOT* yang merupakan standar awal pengetikan jika menggunakan *Microsoft Word*. Berikut ini contoh dari *virus* makro.

1. *Melissa*, merupakan *virus* yang cukup ganas dan menyebar melalui internet.
2. Varian W97M, merupakan *virus* yang menginfeksi *NORMAL.DOT* dan dokumen jika *file* dibuka.

Macro adalah perintah yang isinya berupa program otomatis. Banyak aplikasi umum yang menggunakan *macro*. Jika seorang pengguna mengakses sebuah dokumen yang mengandung *macro* yang telah terinfeksi oleh *virus* ini dan secara tidak sengaja mengeksekusinya, *virus* ini dapat meng-*copy* ke dalam *file start up* dari aplikasi tersebut, sehingga komputer tersebut ikut terinfeksi dan sebuah salinan dari *macro virus* tersebut tinggal didalamnya.

Selain itu, dokumen lain di dalam komputer akan terinfeksi juga. Jika komputer berada di dalam suatu jaringan komputer, kemungkinan besar *virus* ini dapat menyebar dengan cepat ke komputer lain, misalnya melalui *flashdisk* ataupun *e-mail*, *virus* akan menjangkiti komputer penerima *file* tersebut. Proses ini akan berakhir jika *virus* ini telah diketahui dan seluruh *macro* yang terinfeksi dibasmi.

Macro virus merupakan salah satu jenis *virus* yang paling umum saat ini. Aplikasi seperti *Microsoft Word* dan *Microsoft Excel* tergolong sangat rentan

terhadap *virus* jenis ini. Satu hal yang membuat penyebaran *virus* ini cukup sukses adalah akibat maraknya penggunaan aplikasi *e-mail* dan *web*.

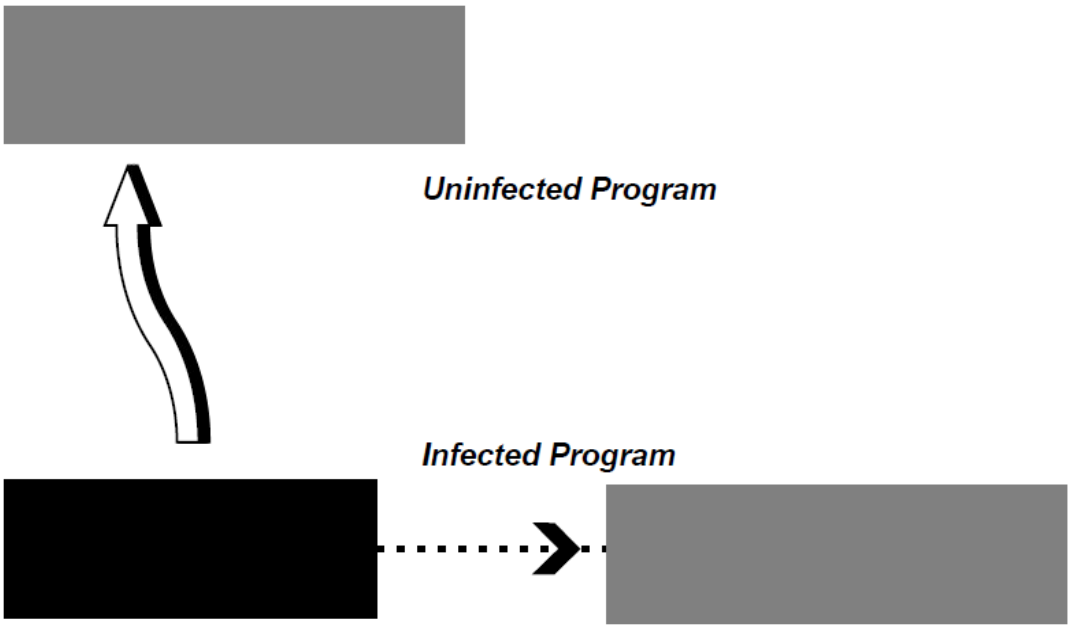
2.2.1.3.2.2 Email Worm

Penyebab utama berkembangnya *virus* saat ini adalah kemudahan pengguna men*download attachment e-mail* yang telah terinfeksi. Seringkali, isi *e-mail* yang bersangkutan mengandung *virus*, misalnya untuk kasus *worm* "*I LOVE YOU*" yang menyebar dengan nama *file* "*LOVE-LETTER-FOR-YOU.TXT.vb*"' disertai dengan pesan yang berbunyi "*kindly check the attached LOVELETTER coming from me*". Selain melalui *e-mail*, *worm* juga dapat menyebar melalui *newsgroup posting*.

2.2.1.4 Struktur Dan Operasi *Virus*

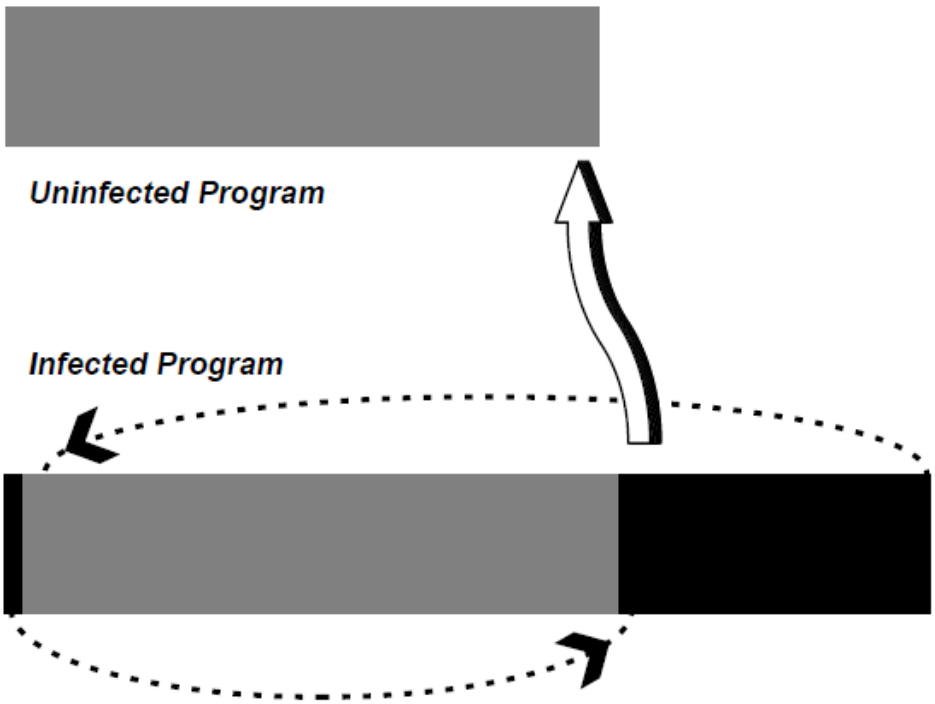
Virus mempunyai dua komponen utama: komponen yang berfungsi untuk menangani penyebaran , dan sebagai pembawa *virus* . Agar komputer *virus* dapat bekerja, haruslah menambahkan kode yang dapat mengeksekusi *virus* tersebut. Kode *virus* tersebut biasanya tereksekusi sebelum menginfeksi korbannya. Satu bentuk klasifikasi dari *virus* komputer adalah berdasarkan pada tiga cara *virus* menambahkan dirinya pada kode *host* : sebagai *shell*, *add on*, dan *Intrusive code* (kode perusak). Bentuk ke empat, yang disebut *companion virus*, bukanlah *virus*, melainkan sebuah *trojan horse* yang menggunakan mekanisme jalur eksekusi untuk mengeksekusinya ditempat program normal.

***Shell virus*es**, merupakan bagian yang melndungi *virus* (seperti pada lapisan luar yang melindungi telur) disekitar kode asli. Dan hasilnya, *virus* menjadi program, dan program asli dari *host* menjadi *internal subroutine* dari kode *virus*. Sebuah contoh ekstrim dari hal ini dapat menjadi kasus dimana *virus* memindahkan kode original ke lokasi yang baru dan mengambil identitas dari si *host*. Ketika *virus* telah selesai mengeksekusi, *virus* menerima kode program *host* dan mulai mengeksekusi. Hampir semua program *virus boot* (digambarkan dibawah ini) adalah tipe *Shell viruses*.



Gambar 2.1 Shell Virus Infection
(Sumber : Eugene H.Spafford, 1994)

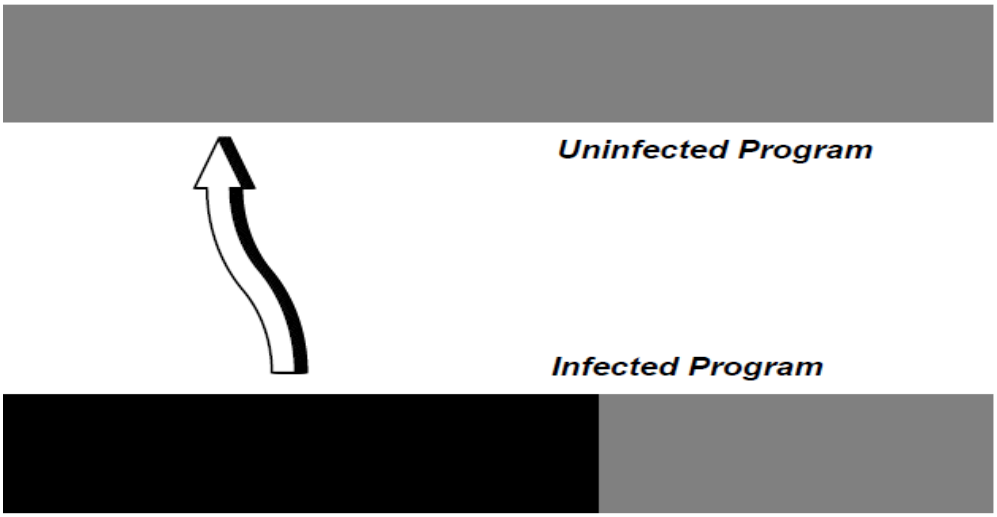
Add-on viruses, kebanyakan *virus* adalah *Add-on-virus,* cara kerjanya dengan menambahkan kode mereka pada kode *host*, atau memindahkan kode *host* dan memasukkan kode dari *virus*. *Add-on virus* lalu mengubah informasi awal dari program, mengeksekusi kode *virus* sebelum kode dari program utama. Kode *host* hampir dipastikan tidak di modifikasi; satu-satunya hal yang menandakan adanya *virus* adalah bertambahnya ukuran *file*, maka hal terssebut harus benar-benar di perhatikan.



Gambar 2.2: Add-on Virus Infection
(Sumber : Eugene H.Spafford, 1994)

Intrusive Viruses, *intrusive viruses* beroperasi dengan cara menulis ulang beberapa atau semua kode asli *host* dengan kode dari *virus*. Pergantian ini bisa menjadi selektif, sebagaimana mengganti sebuah *subroutine* dengan *virus*, atau memasukkan vektor pengganggu baru dan rutin. Pergantian ini juga bisa menjadi luas.

Seperti ketika porsi besar dari program *host* secara lengkap digantikan oleh kode *virus*. Dalam kasus terakhir, program original tidak dapat berfungsi secara benar. Beberapa *virus* merupakan *intrusive virus*.



Gambar 2.3: Intrusive Virus
(Sumber : Eugene H.Spafford, 1994)

2.2.1.5 Evolusi Dari *Virus*

2.2.1.5.1 Generasi Pertama: *Simple* (Sederhana)

Generasi pertama dari *virus* adalah tipe *virus* sederhana. *Virus* ini tidak melakukan sesuatu yang berarti selain hanya melakukan replikasi. Banyak *virus* baru yang ditemukan hari ini masih masuk kedalam kategori ini. Kerusakan dari tipe *virus* sederhana ini biasanya disebabkan oleh *bugs* atau tidak kompatibel dengan perangkat lunak yang belum diantisipasi oleh pembuat *virus*. Generasi *virus* pertama tidak melakukan aktivitas apa-apa dengan tujuan menyembunyikan keberadaaan mereka pada sistem, maka *virus* tersebut dapat ditemukan dengan artian sederhana seperti tidak adanya peningkatan ukuran *file-file* atau kehadiran dari pola khusus pada *file* yang terinfeksi.

2.2.1.5.2 Generasi Kedua: *Self Recognition* (Pengenalan Diri)

Satu masalah yang disebabkan oleh *virus* adalah infeksi pada *host* yang berulang-ulang, menghabiskan memori dan deteksi dini. Pada kasus dari *virus boot* sector, hal ini dapat menyebabkan rantai panjang dari sektor-sektor yang terhubung. Dalam kasus program yang terinfeksi oleh *virus* secara berulang-ulang bisa berdampak pada kelanjutan perpanjangan dari program *host* setiap kali terinfeksi ulang. Untuk mencegah perkembangan dari *file-file* yang terinfeksi, *virus* generasi kedua biasanya menanamkan *signature* unik yang memberi sinyal bahwa *file* atau sistem telah terinfeksi. *Virus* tersebut akan memeriksa signaturenya sebelum mencoba menginfeksi *file*, dan akan menggantinya ketika infeksi telah mengambil tempat; jika *signature* telah ada, *virus* tidak akan menginfeksi ulang *host*. *Signature virus* dapat berupa karakteristik urutan dari *bytes* pada *offset* yang dikenal dalam *disk* atau memori, fitur khusus pada direktori *entry* (contohnya; perubahan waktu atau panjang *file*), atau sistem panggil khusus yang ada ketika *virus* aktif di memori. *Signature* menyediakan keuntungan untuk *virus*. *Virus* tidak lagi menjalankan infeksi yang sia-sia, sehingga dapat meninggalkan jejak akan kehadirannya, tapi *signature* menyediakan metode dari deteksi. *Virus* menghapus progarm – program yang dapat melakukan *scan signature* pada *file* dalam *harddisk* untuk mendeteksi *virus* atau juga menanamkan sistem dengan menyediakan *signature virus* pada sistem yang bersih guna mencegah *virus* dari percobaan infeksi.

2.2.1.5.3 Generasi Ketiga: *Stealth* (Sembunyi)

Kebanyakan *virus* dapat di identifikasi pada sistem yang telah tercemar dengan cara melakukan *scan* pada *secondary storage* dan mencari pola data unik dari setiap *virus*. Untuk melakukan penetralan seperti *scan*, beberapa *virus* melakukan teknik *stealth*. *Virus* ini merusak sistem servis yang disebut *interrupts* ketika aktif. Permintaan untuk melakukan operasi ini telah diganggu oleh kode *virus*. Jika operasi dapat memaparkan kehadiran dari *virus*, operasi itu akan diulang kembali untuk mengembalikan kesalahan informasi.

Sebagai contoh, teknik umum sebuah *virus* adalah untuk memotong permintaan input dan output yang dapat membaca sektor-sektor dari *harddisk*. Kode *virus* memonitor permintaan ini. Jika operasi membaca terdeteksi, maka dapat mengembalikan blok yang berisi salinan *virus*, kode aktif mengembalikan salinan dari data yang terdapat dalam sistem yang tidak terinfeksi. Dengan cara ini, *scanner virus* tidak dapat menemukan *virus* pada harddsik ketika *virus* telah aktif dalam memori. Teknik serupa mungkin juga dilakukan untuk menghindari deteksi oleh operasi lain.

2.2.1.5.4 Generasi Keempat: *Armored* (Dipersenjatai)

Beberapa peneliti *anti virus* telah mengembangkan *tool* untuk menganalisa *virus-virus* baru, pencipta *virus* telah merubah metode untuk menyamarkan kode *virus* mereka. Teknik ini dilakukan dengan cara menambahkan kode-kode membingungkan dan kode-kode acak sehingga akan membuat sulit untuk menganalisa kode *virus*. Cara ini juga merupakan bentuk serangan langsung melawan *software anti-virus*, jika sudah menginfeksi sistem. *Virus – virus* ini muncul sejak 1990, *virus* generasi keempat ini cenderung berukuran lebih besar dari pada *virus* yang sederhana. Lebih lanjut, kompleksitas dari *virus* diperlukan untuk mempersulit usaha para ahli anti-*virus*.

2.2.1.5.5 Generasi Kelima: *Polymorphic* (Berubah-ubah)

Tipe *virus polymorphic* atau pandai bermutasi diri paling banyak ditemukan pada akhir-akhir ini. *Virus* ini yang menginfeksi target-target mereka oleh versi yang telah di enkripsi atau di modifikasi. Dengan memvariasi urutan kode-kode dituliskan ke *file* (tapi masih berfungsi sama dengan yang original), atau dengan menghasilkan perbedaan, kunci enkripsi acak, *virus* yang ada pada *file* yang dilakukan perubahan tidak akan diidentifikasi melalui metode pencocokan *byte*. Untuk mendeteksi kehadiran *virus* ini, dibutuhkan algoritma yang lebih kompleks untuk membuka penyamaran *virus* dan menentukan *virus* ini ada atau tidak.

Beberapa *virus* ini telah menyebar cukup luas. Beberapa pembuat *virus* telah membuat *virus toolkits* yang dapat digabungkan pada *virus* untuk memberi kemampuan *polymorphic*. *Toolkits* ini telah di sebar kepenjuru dunia melalui internet dan ditambahkan dalam beberapa macam *virus*.

2.2.1.6 Pertahanan Terhadap *Virus*

Ada beberapa metode pertahanan melawan *virus*. Sayangnya, tidak ada pertahanan yang sempurna. Fakta dilapangan telah membuktikan bahwa adanya fasilitas jaringan data, komunikasi dan media penyimpanan bersama telah membuka peluang adanya penyebaran *virus*. Lebih lanjut lagi, beberapa peneliti *virus* seperti *Cohen, Adleman*, telah membuktikan bahwa masalah dalam membuat program untuk secara tepat mendeteksi semua *virus* tidak dapat ditentukan, tidaklah mungkin untuk membuat program yang dapat mendeteksi setiap *virus* tanpa ada kesalahan. Pertahanan melawan *virus*, biasanya menggunakan salah satu bentuk ini:

Monitor Aktifitas (*Activity Monitors*) merupakan program yang ada pada sistem. Memonitor aktifitas, dan juga menaikkan peringatan atau mengambil aksi khusus jika ada aktivitas yang mencurigakan. Walaupun demikian, percobaan untuk mengubah gangguan tabel dalam *memory*, atau untuk menulis ulang *boot sector* dapat di ganggu oleh monitor semacam itu. Bentuk pertahanan ini dapat di hindari (jika diimplementasikan dalam *software*) oleh *virus* yang telah aktif terlebih dahulu pada rangkaian *boot* daripada kode monitor. Mereka lebih rentan terhadap *virus* jika digunakan pada mesin tanpa perlindungan *hardware* memori seperti yang terjadi pada beberapa personel komputer. Bentuk lain dari monitor adalah yang melakukan emulasi atau melacak eksekusi dari aplikasi terduga*virus*.

Monitor mengevaluasi aksi yang dilakukan oleh kode, dan menentukan jika ada aktifitas yang mirip dengan aktifitas *virus*. Peringatan yang tepat akan dijalankan jika aktifitas mencurigakan teridentifikasi.

Scanners *Scanners* menjadi tehnik pertahanan terhadap *virus* yang paling populer. Sebuah *scanner* beroperasi dengan membaca data dari *harddisk* dan menerapkan operasi persamaan pola dalam melawan pola *virus* yang telah dikenali. Jika persamaan pola ditemukan, peringatan akan *virus* akan dijalankan. *Scanners* sangatlah mudah dan cepat digunakan, tapi banyak memiliki kekurangan. Kekurangan yang paling menonjol adalah daftar pola harus selalu terbaharukan. Pada pemrogaraman *MS-DOS*, lusinan *virus-virus* baru bermunculan hampir setiap minggu. Menjaga pola *file* tetap terbaharukan dalam lingkungan yang secara cepat berubah-ubah sangatlah sulit.

Kekurangan yang kedua adalah adanya laporan kesalahan palsu. Ketika pola *virus* baru ditambahkan ke dalam list,seolah-olah salah satu pola baru tersebut menjadi kode yang sah. Kekurangan yang lainnya adalah tipe *virus polymorphic* tidak bisa dideteksi oleh *scanner*. Namun, kelebihan dari *scanner* adalah kecepatannya. Proses *scan* dapat dilakukan secara cepat. Proses *scan* juga dapat dilakukan secara *portable* dan disemua *platforms*, dan *file* pola *virus* dapat dengan mudah didistribusikan dan diupdate. Meskipun begitu, pola *virus* yang tidak terbaharukan masih memadai pada kebanyakan lingkungan. *Scanners* yang dilengkapi dengan algoritma atau pengecekan secara heuristik dapat mendeteksi kebanyakn *virus* tipe *polymorphic*. Kelebihan inilah yang membuat *scanners* digunakan secara luas dalam bentuk *software*.

Integrity checkers/monitors, *Integrity checkers* adalah program yang menghasilkan cek kode (sebagai contoh; pemeriksaan jumlah, pemeriksaan perputarn redundansi dan pengecekan hasil kriptografi) untuk memonitor *file*. Secara periodik, pengecekan kode ini akan di hitung ulang dan di bandingkan dengan versi yang tersimpan. Jika perbandingan gagal, perubahan yang dikenal telah terjadi pada *file*, dan ditandai untuk investigasi lebih lanjut. Monitor *integrity* berjalan secara terus-menerus dan mengecek integritas dari *file* pada basis regular. Pelapis integritas memeriksa ulang kode pengecekan sebelumnya pada setiap eksekusi.

Pengecekan Integritas adalah salah satu cara tertentu untuk menemukan perubahan pada *file*, termasuk *file* data. Dimana sebagai *virus* harus menambahkan *file-file* untuk menanamkan kode-kode berbahaya pada *file* yang telah terinfeksi. Pengecekan integritas akan menemukan perubahan - perubahan tersebut, lebih lanjut lagi, tidaklah penting jika *virus* itu diketahui atau tidak pengecekan integritas akan menemukan perubahan yang terjadi, apapun penyebabnya. Pengecekan integritas juga akan menemukan perubahan lain yang disebabkan oleh *bug* pada *software*, kesalahan pada *hardware*, dan kesalahan pengoperasian.

Pengecekan integritas juga mempunyai kelemahan. Pada beberapa sistem, *file* eksekusi mengalami perubahan ketika *user* menjalankan *file* tersebut, atau ketika sebuah menu pilihan baru sedang direkam. Pengulangan laporan kesalahan positif dapat mengarahkan *user* untuk mengabaikan laporan berikutnya atau menonaktifkan kegunaan lainnya. Merupakan sebuah kasus bahwa sebuah perubahan dapat tidak diperhatikan sampai sebuah penambahan *file* telah berjalan dan *virus* telah menyebar. Lebih penting lagi, kalkulasi inisial dari pengecekan kode harus di tampilkan pada perubahan versi dari tiap *file*. Jika tidak, monitor tidak akan melaporkan kehadiran dari *virus*, mungkin saja membuat *user* untuk mempercayai sistem tidak terinfeksi.

Beberapa vendor telah memulai untuk membangun pengecekan diri sendiri kedalam produk-produk mereka. Ini adalah bentuk dari pengecekan integritas yang ditampilkan pada waktu yang bersamaan. Jika fitur pengecekan sendiri mengungkapkan beberapa perubahan yang tidak diinginkan dalam memori atau pada *harddisk*, program akan menghapus atau memperingatkan *user*. Ini membantu untuk memberitahukan kehadiran dari *virus* baru secepatnya sehingga aksi lebih lanjut dapat dilakukan.

Jika tidak ada lagi *virus* komputer yang dibuat dari sekarang, akan tetap ada masalah *virus* komputer dalam beberapa tahun mendatang. Dari ribuan laporan *virus – virus*, beberapa ratus *virus* telah di sebar dan menginfeksi pada berbagai macam tipe komputer diseluruh dunia.

2.2.1.7 *Virus* Sebagai Kehidupan Buatan

Sekarang setelah kita tahu tentang *virus*, dan bagaimana cara penyebarannya, kita dapat menguji pertanyaan mengenai apakah mereka mempunyai bentuk sebuah kehidupan buatan. Pertanyaan pertama adalah "apakah arti dari kehidupan?" Tanpa sebuah jawaban untuk menjawab petanyaan ini, kita tidak akan bisa mengatakan bahwa *virus* itu hidup. Satu pernyataan kuat yang berhubungan dengan arti hidup telah direpresentasikan, dan pernyataan itu adalah:

- Kehidupan sebagai pola dalam ruang waktu lebih dari sebuah objek material khusus.
- Reproduksi sendiri, dalam dirinya ataupun organisme yang berhubungan.
- Penyimpanan informasi atau representasi sendiri.
- Sebuah metabolisme yang mengkonversi energi.
- Ketergantungan dari tiap – tiap bagian.
- Keseimbangan dibawah gangguan – ganguan dari setiap lingkungan.
- Kemampuan untuk berevolusi.
- Pertumbuhan untuk ekspansi.

Mari kita tentukan tiap tiap dari karakter ini yang berhubungan pada *virus* komputer

2.2.1.7.1 *Virus* sebagai pola dalam ruang dan waktu

Ada kecocokan yang nyaris sama pada karakter ini. *Virus* di tampilkan oleh pola dari instruksi komputer yang ada spanjang waktu dalam banyak sistem komputer. *Virus* tidak di hubungkan oleh perangkat keras, tapi juga dengan eksekusi instruksi (kadang kala) oleh perangkat keras. *Virus* komputer, seperti kebanyakan fungsioanal pada kode komputer merupakan manifestasi sederhana dari algoritma. Algoritma itu sendiri juga mewakili pola yang digarisbawahi. Patut dipertanyakan jika pola ini ada dalam ruang, bagaimanapun juga, kecuali satu perpanjangan definisi dari ruang menjadi "ruang dunia maya," sebagaimana diwakili pada sistem komputer. Pola dari *virus virus* secara sementara merupakan rangkain elektronik dan medan magnet. Dengan kata lain, tiap tiap kode *virus* dapat di cetak pada kertas, sehingga menghasilkan keberadaan yang nyata. Bagaimanapun juga, hanya mewakili dari *virus* sebenarnya, dan seharusnya tidak dapat dilihat sebagai keberadaan yang tidak lebih dari sebuah gambaran kepribadian.

2.2.1.7.2 Kemampuan bereproduksi sendiri dari sebuah *Virus*

Salah satu karakteristik utama dari *virus* komputer adalah kemampuan mereka untuk mereproduksi diri mereka sendiri (atau penambahan versi dari diri mereka). One of the primary characteristics of computer *virus*es is their ability to reproduce themselves (or an altered version of themselves). Karakter ini seringkali ditemui. Salah satu kunci dari karakteristik ini adalah kemampuan mereka untuk bereproduksi. Bagaimanapun juga, mungkin saja bisa lebih menarik untuk menentukan aspek ini dalam sinar dari agen reproduksi.

Kode *virus* bukan merupakan agen tersebut, komputerlah yang merupakan agen tersebut. Merupakan hal yang dipertanyakan jika ini dapat di pertimbangkan dengan tujuan dari klasifikasi sebagai kehidupan buatan. Untuk melakukan itu dapat diartikan bahwa (sebagai contoh) cetak biru dari sebuah mesin *XEROX*

mampu melakukan produksi sendiri : ketika agen luar mengikuti instruksi, sangatlah mungkin untuk membuat mesin baru yang kemudian akan dapat digunakan untuk membuat tiruan dari mesin tersebut. Bukanlah cetak biru (algoritma; *virus*) yang merupakan agen dari perubahan, tetapi entitas yang menafsirkannya.

2.2.1.7.3 Media penyimpanan informasi dari perwakilan diri sendiri

Ini merupakan kecocokan pasti dari *virus* komputer. Kode yang mendefinisikan *virus* adalah sebuah contoh yang digunakan oleh *virus* itu sendiri untuk mereplikasi dirinya sendiri. Ini mirip dengan molekul DNA yang kita kenal sebagai kehidupan organik.

2.2.1.7.4 Metabolisme *virus*

Ciri-ciri ini melibatkan organisme yang mengambil energi atau materi dari lingkungan dan mempergunakannya untuk aktivitasnya sendiri. *Virus* komputer menggunakan energi dari komputasi yang diperluas oleh sistem untuk mengeksekusinya. Mereka tidak mengkonversi unsur, tapi memanfaatkan energi listrik yang ada pada komputer untuk melintasi instruksi dari pola mereka dan menginfeksi program lain. Pada kasus ini, mereka mempunyai metabolisme.

Sekali lagi, bagaimanapun juga, kita dipaksa untuk merubah pandangan ini jika kita menguji kasus ini lebih dekat. Penggunaan energi tidaklah digunakan oleh *virus*, tapi dengan memanfaatkan sistem komputer. Jika *virus* tidak aktif, dan permainan interaktif sedang berjalan, jumlah energi yang sama akan digunakan. Pada kebanyakan sistem, walaupun tidak ada program yang sedang berjalan, energi yang ada akan tetap stabil. Oleh karena itu, kita harus menyimpulkan bahwa sebenarnya *virus* tidak mempunyai metabolisme.

2.2.1.7.5 Interaksi fungsional pada lingkungan *virus-virus* fungsional

Virus menjalankan pemerikasaan dari lingkungan *host* mereka sebagai bagian dari aktifitas mereka. Mereka menambahkan, menginterupsi, memeriksa memori dan aristektur piringan, dan juga menambahkan alamat-alamat untuk menyembunyikan diri mereka dan menyebar melalui *host* lain. Mereka sangat jelas menambahkan lingkungan mereka untuk mendukung keberadaan mereka. Banyak *virus – virus* secara tidak sengaja menambahkan lingkungan mereka dikarenakan *bugs* atau interaksi yang tidak terlihat. Porsi kerusakan utama dari semua *virus-virus* komputer adalah hasil dari interaksi ini.

2.2.1.7.6 Saling ketergantungan antara bagian *virus*

Organisme hidup tidak dapat melakukan pembelahan secara asal tanpa menghancurkan diri mereka sendiri. Hal yang sama merupakan kebenaran dari *virus-virus*. Haruskah sebuah komputer *virus* mempunyai porsi dari pemotongan anatomi, *virus* mungkin saja dapat mempermudah untuk berfungsi secara normal, jika iya. Beberapa *virus* telah ditulis dengan kode-kode yang berlebihan oleh karena itu, kode operasional tidak dapat di bagi tanpa menonaktfikan *virus*.

Bagaimanapun juga, sangatlah menarik untuk menulis bahwa nantinya *virus* dapat di susun ulang dan mendapatkan kembali status fungsionalnya. Jika organisme hidup (seperti yang secara umum kita ketahui) telah di bagi kedalam bagian-bagian komponen untuk jangka waktu tertentu, lalu di susun ulang, tidak akan dapat hidup lagi. Dalam kasus ini, *virus* komputer akan telihat seperti mesin sederhana atau reaksi kimia dari pada perumpamaan dari makhluk hidup.

2.2.1.7.7 Stabilitas *Virus* dalam keadaan terganggu

Virus komputer berjalan pada setiap variasi mesin dalam sistem operasi yang berbeda. Banyak dari *virus virus* yang mampu melakukan kompromi (dan mengalahkan) anti-*virus* menyalin mekanisme proteksi. Mereka mungkin dapat

menyesuaikan pada kondisi yang dimana tidak tersedianya media penyimpanan, kesalahan *disk*, dan kondisi-kondisi buruk lainnya.

Beberapa *virus* mampu beroperasi pada varian-varian yang paling banyak digunakan dari komputer pribadi yang berjalan pada berbagai macam konfigurasi perangkat lunak, kestabilan dan kesukaran terlihat pada beberapa aplikasi komersial.

2.2.1.7.8 Evolusi *Virus*

Dalam hal ini, *virus* juga menampilkan perbedaan dari sistem yang kita sebut sebagai "hidup." Tidak ada *virus* komputer berevolusi sebagaimanayang kita perkirakan, walaupun, sebuah *virus* dapat menjadi sangat besar dan kompleks seperti kebanyakan *virus* lainnya.

Level yang lebih tinggi dari mutasi sebuah *virus* ternyata ada, bagaimanapun juga, ada beberapa varian-varian dari kebanyakan *virus* yang dikenali, dengan berbagai jenis dari beberapa *virus* komputer *IBM*. Variasi yang terkait dapat lebih kecil, dengan tujuan pada dua atau tiga perbedaan instruksi, untuk perbedaan utama yang melibatkan perbedaan pada pesan, aktivasi, dan replikasi. Sumber dari variasi – variasi ini berasal dari programmer (si pembuat *virus* itu sendiri) yang dimana melengkapi *virus* untuk menghindari mekanisme *anti virus*, atau untuk menyebabkan bentuk-bentuk lain dari kerusakan. *Virus polymorphic* juga melengkapi replika *virus*nya untuk menghindari deteksi, tetapi pola dari penambahan juga sangat jelas merupakan produk manusia. Perubahan ini bukan merupakan evolusi.

Yang membuat lebih menarik, ada sebuah kasus dimana ada dua *virus* macintosh diketahui dapat berinteraksi untuk melakukan infeksi tidak seperti pada "*parents*" walaupun initeraksi ini biasanya menghasilkan hasil yang steril yang tidak mampu bereproduksi lebih jauh. Hal ini bukanlan merupakan evolusi seperti yang kita kenal.

2.2.1.7.9 Berkembang

Virus secara pasti melakukan bentuk perkembangan, dalam hal yang kebanyakan dari *virus* berada dalam lingkungan yang baik untuk tumbuh dan berkembang. Sementara beberapa *virus* akan menginfeksi setiap *file* dalam sistem setelah melakukan beberapa aktivitas. Penyebaran *virus* melalui perangkat lunak komersial dan internet merupakan indikasi dari replikasi penyebaran luas dari *virus*. Walaupun hitungan akurat sangat sulit untuk diperoleh, laporan dari beberapa tahun lalu mengindikasikan bahwa setiap tahun ada peningkatan sebanyak dua kali lipat terhadap komputer yang terinfeksi oleh *virus* komputer.

Secara pasti, *virus* komputer telah menunjukkan pertumbuhan yang sangat signifikan setiap tahunnya.

2.2.1.7.10 Tingkah laku lainnya

Seperti sudah di beritahukan sebelumnya, *virus* komputer merupakan "*species*" dengan bentuk terbaik secara ekologi berdasarkan pada tipe mesin *host*, dan variasi-variasi dibarengi dengan spesies ini. Spesies ini beradaptasi kepada lingkungan khusus dan tidak akan bertahan jika berpindah menuju lingkungan lain.

Beberapa *virus* juga menunjukkan tingkah laku seperti pemangsa. Sebagai contoh, *virus DenZuk* akan mencari tahu dan menulis ulang di otak *virus* jika keduanya berada pada sistem yang sama. *Virus* lain menunjukkan tingkah laku yang berhubungan dengan wilayah kekuasaan, menjaga *domain* yang terinfeksi sehingga *virus* yang bertipe sama tidak akan masuk dan bersaing dengan *virus* originalnya.

Beberapa *virus* juga menunjukkan tingkah laku perlindungan sendiri, termasuk teknik kamuflase. Sangatlah penting untuk di catat, bahwa tidak ada satupun dari karakter ini berasal dari *virus* itu sendiri. Melainkan, setiap

perubahan dan penambahan kepada tingkah laku *virus* telah ditulis oleh pihak agensi luar: sang programmer.

Perubahan ini telah menjadi reaksi untuk merasakan kebutuhan akan fungsi "menambahkan fitur" pada *virus* yang bertujuan ntuk membuat *virus* susah untuk ditemukan.

Mungkin juga dapat menjadi perselisihan bahwa semakin banyak organisme tradisional hidup yang juga akan hidup tanpa melakukan perubahan. Sebagai contoh, efek dari radiasi mungkin saja dapat menimbulkan mutasi secara acak. Bagaimanapun juga, programmer – programmer adalah satu-satunya sumber dari perubahan *virus* komputer, dan sifat khusus ini sama sekali tidak berarti apa-apa. Sistem kehidupan lainnya melakukan perubahan terhadap diri mereka dan keturunan mereka tanpa campur tangan pihak luar.

2.2.2 *Worm*

Dikutip dari *Eugene H.Spafford Eugene, 1994. Computer Viruses as Artificial Life, Worms* adalah bentuk lain dari *software* yang biasanya disamakan sebagai *virus* komputer. Tidak seperti *virus*, *worms* merupakan program yang dapat berjalan secara independent dan beralih dari satu komputer ke komputer lain menggunakan koneksi jaringan; *worms* bisa mempunyai porsinya sendiri ketika berjalan pada komputer yang berbeda. *Worms* tidak merubah program lain, walaupun berisi kode-kode yang hampir sama seperti *virus*. Perilaku replikasinyalah yang membuat beberapa orang percaya bahwa *worms* merupakan bentuk dari *virus*, terutama orang-orang yang menggunakan Definisi formal *Cohen's* (yang dimana secara tidak disengaja dapat mengklasifikasikan program-program standar transfer *file* melalui jaringan sebagai *virus*). Merupakan fakta bahwa *worms* tidak merubah program-program yang ada merupakan perbedaan yang jelas antara *virus* dan *worm*.

2.2.3 *Trojans*

2.2.3.1 Definisi *Trojan*

Dikutip dari buku karya "Ahmad Yani, 2009. Cara ampuh membasmi *virus* komputer ", ***Trojan Horse*** atau yang lebih dikenal dengan nama ***trojan*** adalah aplikasi program ilegal yang bertujuan melakukan aktivitas rahasia yang tidak diinginkan. Program di dalamnya telah diubah dan ditambah kode untuk menjalankan suatu fungsi rahasia (dengan tujuan tertentu).

Trojan bukanlah *virus*, melainkan program yang sangat berbahaya, bahkan bisa lebih berbahaya dari *virus*. Biasanya *Trojan* bekerja dengan *system Remote Administration Tools (RAT's)*, yaitu terdapat *host* sebagai *server* dan targetnya adalah pengguna. Oleh sebab itu, *trojan* selalu menjadi masalah dalam sistem kemanan komputer. Biasanya *trojan* disisipkan atau menumpang pada aplikasi – aplikasi yang secara gratis bisa di *download* dari internet namun bukan dari sumber yang dapat dipercaya. Saat ini, banyak sekali tipe dan jenis *trojan*, baik yang sifatnya komersil ataupun yang tidak dipublikasikan (biasanya andalan beberapa *hacker*). *Trojan* bersembunyi didalam sistem (biasanya di *registry* pada *windows*) dan tidak terdeteksi oleh *anti virus*. Kecanggihan *trojan* semakin meningkat, yaitu dengan menambahkan fitur-fitur baru dan enkripsi yang lebih baik, sehingga program anti*virus* tidak dapat mendeteksinya. Penyebaran *trojan* hampir sama seperti penyebaran *virus*, biasanya mengandalkan program gratisan yang di *download* dari internet, khususnya *shareware* maupun *freeware*.

Para pengguna internet diharapkan berhati-hati terhadap program yang diunduh. Unduhlah program dari situs resminya (***official site***). Selain itu, kita juga perlu mewaspadai celah (*port*) yang terbuka pada komputer yang kita gunakan. Sebab, bisa saja *trojan* masuk melalui celah tersebut untuk mengambil alih komputer dan mencuri data-data yang ada di komputer.

2.2.3.2 Media Penyebaran *Trojan*

Bagaimana *trojan* bekerja menginfeksi korbannya? Biasanya *trojan* masuk melalui aplikasi yang di-install dan dikirim oleh seseorang ataun di *download* dari situs tertentu ketika *online* (internet ataupun jaringan). Ada beberapa aplikasi yang memungkinkan *trojan* menginfeksi komputer, diantaranya melalui *ICQ, Internet Relay Chat (IRC)* atau *mIRC*, *Yahoo! Messenger, skype,gtalk*, *e-mail attachment*, akses fisik jaringan (seperti *hotspot* dan *bluetooth*, dan dari media disket dan *flashdisk*.

2.2.3.3 Bahaya *Trojan*

Banyak orang yang belum mengetahui *trojan*. Ketika menjalankan *file executable* dan tidak mengganggu sistem komputer, kita tidak merasa khawatir, karena komputer tetap bekerja dan semua data baik-baik saja. Padahal yang terjadi adalah seseorang mengusai komputer yang kita gunakan dan dengan bebasnya mengunduh atau mengunggah *file* di komputer kita. Lebih parahnya, *trojan* dapat menghapus *file-file* di komputer (ini hanya contoh betapa bahayanya *trojan*). *Trojan* juga dapat menyisipkan *virus* komputer yang bisa merusak, contohnya adalah *virus CIH* yang bisa menghapus data *BIOS*. Beberapa *trojan* juga dapat mengambil informasi penting dari komputer korban. Beberapa data umum yang dicari adalah alamat rumah, alamat *e-mail, passwords,* informasi mengenai kartu kredit, informasi *account*, data *accounting*, database, *mailing list*, foto, informasi bisnis, *resume*, nomor telepon dan banyak lagi.

2.2.3.4 Macam-macam *Trojan*

2.2.3.4.1 *Trojan* Pengiriman *Password*

Trojan ini bekerja dengan mencari *passwords* yang tersimpan didalam komputer dan kemudian mengirimnya melalui *e-mail*. *Trojan* ini berbahaya, karena *passwords* yang tersimpan di dalam komputer akan dikirimkan ke pemilik *trojan*.

2.2.3.4.2 *Remote Access Trojan (RAT)*

Trojan ini dapat mengakses langsung ke *harddrive* korban menggunakan *Remote Access Trojans (RAT's).* Program ini sangat mudah digunakan, hanya dengan menjalankan *server* (program yang dijalankan oleh korban) dan mengetahui alamat *IP* korban, kita dapat mengakses komputer korban dan bisa melakukan apa saja, tergantung fasilitas yang disediakan oleh *trojan* yang digunakan. *RAT's* juga mempunyai fungsi akses seperti *keylogger, upload* dan fungsi *download*, membuat *screenshot*, dll.

2.2.3.4.3 *Keyloggers*

Trojan ini cukup sederhana. Bekerja dengan menyimpan ketikan keyboard pada komputer korban dan memeriksa passwords yang tersimpan pada log *file*. Selanjutnya *Trojan* merekamnya ketika komputer *online*, atau ketika saat *offline*. Pada mode merekam secara *online*, mereka tahu jika korban sedang *online* dan merekam semua aktivitasnya. Namun pada mode *offline*, mereka dapat merekam semua aktivitas setelah *windows* aktif, kemudian menyimpannya pada *harddsik* korban untuk menunggu dikirimkan.

2.2.3.4.4 *Trojan* Perusak

Trojan jenis ini bekerja dengan menghancurkan dan menghapus *file*, sehingga *trojan* ini terlihat sederhana dan sangat mudah digunakan. *Trojan* akan otomatis menghapus semua *file* atau *file*.exe lainnya didalam komputer, sehingga sangatlah berbahaya. Sekali terinfeksi, banyak aplikasi yang tidak jalan dan bahkan OS pun bisa hancur.

2.2.3.4.5 *FTP Trojan*

Trojan ini membuka *port* 21 (*ftp-file transfer protocol)* di komputer korban dan mengizinkan setiap orang yang mempunyai FTP *client* untuk bisa tersambung ke komputer. Caranya dengan meminta *password*, mengupload, dan men-downloaad *file* secara bebas.

2.2.4 *Spyware*

Berdasarkan *Hackworth (2005). Spyware* adalah bentuk dari *malware* yang mengumpulkan informasi dari sistem komputer tanpa sepengetahuan si pemilik data. Data ini sering kali meliputi : *Keystrokes, screenshots, user name* dan kata sandi, alamat-alamat *e-mail* pribadi, data *form web*, *log* penggunaan *internet*, dan informasi pribadi lainnya. Seringkali, data yang telah dicuri akan dikirim ke pihak luar atau digunakan oleh si pencuri untuk melakukan kejahatan perbankan, penyalahgunaan identitas, atau menggunakannya untuk *marketing* atau *spam*. Untuk sebuah program seperti *spyware* harus mengumpulkan data tanpa sepengetahuan pemilik data dan harus segera dikirim dan terjamin ketersediaannya kepada pihak ke tiga yang tidak berhak atas data tersebut.

2.3 Perkembangan *Malware* dari masa ke masa

Malware ditemukan pertama kali pada tahun 1970, *malware* dalam bentuk *worm* dan *virus* pertama kali terlihat pada *Advanced Research Projects Agency Network (ARPANET)* yang merupakan salah satu fasilitas pengembangan departemen pertahanan amerika serikat.

Pada tahun 1974 *Virus Rabbit* ditemukan.di beberapa negara-negara dibenua amerika, eropa dan asia. Dilanjutkan pada tahun 1982 ditemukannya *Virus Elk Cloner* yang bertujuan menyerang sistem operasi komputer *Apple II*. *Virus* ini dibuat oleh *Rich Skrenta*, seorang remaja pria berusia 15 tahun yang sekolah di *Mt.Lebanon High School*. Kemudian tahun 1990 ditemukannya *virus polymorphic* dengan nama *Chameleon* yang dibuat oleh *Mark Washburn*.

Pada tahun 1992 ditemukannya *Virus Michelangelo* yang menyerang sistem operasi *DOS* dan menyebar melalui *internet* dan *floppy disk*. Tahun 1998 ditemukannya generasi pertama dari *virus CIH/ Chernobyl73* yang menyerang *BIOS* dengan cara menghapus *FLASH* pada *BIOS*.

Kemudian pada tahun 2001 Ditemukannya *virus Simile* yang dibuat menggunakan bahasa rakitan. Tahun 2004 ditemukannya *worm mydoom* yang menyebar melalui *e-mail*. Dilanjutkan pada tahun 2008 ditemukannya backdoor *Trojan* dengan nama *Rustock* yang menyerang akun para pengguna *social media* seperti *facebook* dan *twitter*. Dilanjutkan tahun 2009 ditemukannya *worm Downadup(a.k.a Kido or Conficker)* yang menyerang sistem operasi *microsoft windows*. Jutaan dari sistem operasi *windows* telah terinfeksi. Banyak perusahaan–perusahaan yang dirugikan oleh *virus* ini, termasuk juga perbankan.

Pada tahun 2010 Ditemukannya *worm ramnit* yang menyerang sistem operasi *windows* dengan cara membuat banyak *shortcut* dan menyembunyikan *file* asli. Selang beberapa bulan kemudian ditemukannya *worm stuxnet* yang awalnya bertujuan menyerang fasilitas nuklir iran, namun *worm* ini menyerang banyak pengguna sistem operasi *microsoft windows* di seluruh dunia termasuk indonesia.

Dan terakhir pada tahun 2011 ditemukannya *worm Morto* yang menyebar memanfaatkan protokol *windows* remote desktop. Masih ditahun yang sama ditemukan *worm Rootkit.Duqu***,** pengembangan dari *stuxnet, keylogger* dan aplikasi *backdoor*.

2.4 Jaringan Komputer

Jaringan komputer merupakan sekumpulan komputer otonom yang saling terhubung satu dengan yang lainnya menggunakan protokol komunikasi melalui media transmisi pada suatu jaringan komunikasi data.

Jaringan komputer memungkinkan suatu organisasi untuk menggunakan sistem pengolahan data terdistribusi yang menggunakan komputer dan dapat saling mengakses satu dengan lainnya. Jaringan komputer juga mendukung adanya *resource sharing, information sharing,* dan *network access*.

Resource Sharing, berarti penggunaan sumber data dan sumber daya secara bersama - sama oleh sejumlah stasiun komputer yang terhubung. Sumber data

dan sumber daya tersebut antara lain yaitu : *Harddisk*, memori, *printer*, *plotter*, *scanner*, CD ROM, dan lain sebagainya.

In*format*ion Sharing, berarti dalam suatu jaringan berlaku pemakaian program-program aplikasi secara bersama-sama. Misalnya jika pada komputer A tidak memiliki program *AutoCAD*, maka komputer A dapat mengambil dan menjalankan program *AutoCAD* tersebut pada komputer lain yang terhubung dan telah diisi dengan program tersebut.

Network Access, merupakan kondisi dimana para pengguna dalam suatu jaringan dapat pula mengakses jaringan komputer lain yang terhubung. Seperti misalnya kita mengakses Internet melalui komputer *server*, dan lain sebagainya.

2.4.1 Klasifikasi Jaringan Komputer

Dari sisi luas area cakupan yang dimilikinya, jaringan komputer dapat diklasifikasikan menjadi:

2.4.1.1 Local Area *Network*

Merupakan jaringan komputer lokal yang mencakup wilayah dengan garis tengah 20 KM. Namun pada implementasinya, kebanyakan LAN hanya digunakan dalam satu atau beberapa gedung dalam satu lingkungan saja seperti lingkungan kampus, pabrik, dan sebagainya.

2.4.1.2 Metropolitan Area *Network*

Merupakan jaringan komputer kelas menengah yang mencakup seperti pada satu kota besar. Menghubungkan satu lingkungan kantor ke lingkungan kantor yang lainnya atau satu pusat perbelanjaan ke pusat perbelanjaan yang lain dan sebagainya.

2.4.1.3 Wide Area *Network*

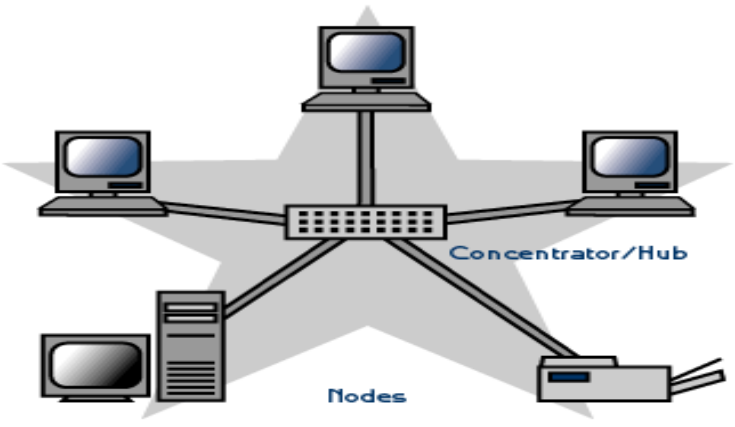
Merupakan jaringan komputer wilayah luas yang mencakup antarnegara atau antarbenua. Biasa disebut juga dengan *Global Area Network* (GAN) yaitu jaringan komputer yang wilayah jangkauannya mencakup seluruh dunia.

2.4.2 Topologi Jaringan Komputer

Topologi merupakan cara untuk menghubungkan komputer atau terminal-terminal dalam suatu jaringan. Dari sisi bentuk dan model hubungan antar komputer, jaringan komputer dapat berbentuk sebagai topologi *Star Network*, *Loop Network*, *Ring Network*, *Bus Network*, dan *Web Network*.

2.4.2.1 Topologi *Star Network*

Pada topologi ini *Local Area Network* terdiri dari sebuah *centralnode* yang berfungsi sebagai pengatur arus informasi dan penanggung jawab komunikasi dalam suatu jaringan. Jadi jika*node* yang satu ingin berkomunikasi dengan*node* yang lain maka harus melalui *centralnode*.

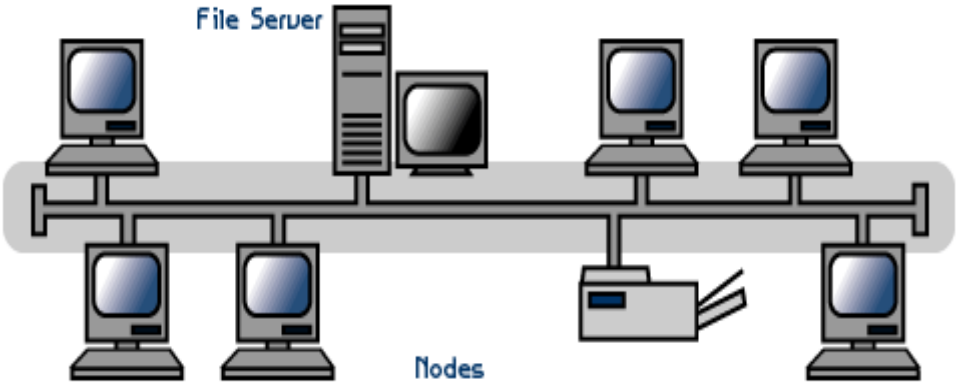


Gambar 2.4 Topologi Star Network
(Sumber :Teguh Wahyono, 2007)

Mengingat pentingnya fungsi dari *centralnode*, maka dalam sistem ini biasanya komputer yang digunakan sebagai *centralnode* merupakan komputer besar atau mainframe yang memiliki kemampuan dan kecepatan tinggi.

2.4.2.2 Topologi *Bus Network*

Pada topologi ini,*node* yang satu dengan*node* yang lain dihubungkan dengan suatu jalur data atau *bus*. Kekurangan dari topologi *BUS* adalah: kecepatan jaringan yang lambat, karena bekerja seperti sistem bis transportasi umum yang dimana akan berhenti di setiap stasium pemberhentian walaupun tidak ada permintaan akan layanan data dari unit yang di lalui, jika terjadi gangguan pada salah satu unit, maka akan berdampak pada seluruh unit yang ada

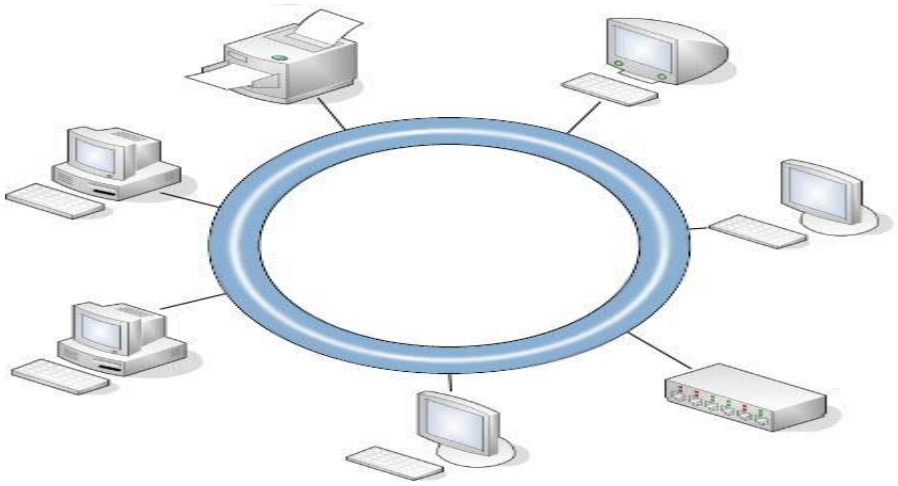


Gambar 2.5 Topologi Jaringan BUS
(Sumber :Teguh Wahyono, 2007)

Pada Gambar 2.5 dapat kita amati bahwa sistem topologi *bus* tidak memiliki *centralnode* dan semua *node* memiliki status yang sama antara satu dengan yang lainnya.

2.4.2.3 Topologi *Ring Network*

Topologi *ring network* atau topologi cincin ini merupakan topologi hasil penggabungan antara topologi *loop network* dengan topologi *bus network*. Keuntungannya adalah bahwa jika salah satu *node* rusak, maka tidak akan mengganggu jalannya komunikasi antar-node karena*node* yang rusak tersebut diletakkan terpisah dari jalur data.



Gambar 2.6 Topologi Jaringan RING Network
(Sumber :Teguh Wahyono, 2007)

2.5 Insiden Keamanan Jaringan Komputer

Berdasarkan penelitian sebelumnya tentang keamanan jaringan komputer, Tesis karya Nur Bagus Dheni T.H, ST, 2006. Analisis Kinerja Keamanan Jaringan Komputer Local Area *Network* (LAN), Program Pasca Sarjana Universitas Gunadarma. Insiden keamanan jaringan adalah suatu aktivitas terhadap suatu jaringan komputer yang dapat memberikan dampak negatif terhadap suatu jaringan komputer yang dapat memberikan dampak negatif terhadap keamanan sistem jaringan komputer tersebut. Secara garis besar terdapat 6 klasifikasi insiden, yaitu:

2.5.1 *Probe*

Sebuah *probe* dapat dikenali dari adanya usaha-usaha yang tidak lazim untuk memperoleh akses ke dalam suatu sistem atau untuk menemukan informasi tentang sistem tersebut. Salah satu contohnya adalah usaha untuk login kedalam sebuah *account* yang tidak digunakan. *Probing* ini dapat dianalogikan sebagai usaha untuk memasuki sebuah ruangan yang dengan mencoba-coba apakah pintunya terkuci apa tidak.

2.5.2 *Scan*

Scan adalah kegiatan *probe* dalam jumlah yang besar dengan menggunakan *tool* secara otomatis. *TOOL* tersebut secara otomatis dapat mengetahui *port-port* yang terbuka pada *host* lokal maupun *host remote, IP address* aktif, bahkan bisa untuk mengetahui sistem operasi yang digunakan pada *host* yang dituju.

2.5.3 *Account compromise*

Account compromise adalah penggunaan *account* sebuah komputer secara ilegal oleh seseorang yang bukan pemilik *account* tersebut. *Account compromise* dapat mengakibatkan korban mengalami kehilangan atau kerusakan data. Sebuah insiden *acount compromise* dapat berakibat lebih lanjut, yaitu terjadinya insiden *root comptomise,* yang dapat menyebabkan kerusakan lebih besar.

2.5.4 *Root compromiser*

Root compromise mirip dengan *account compromise,* dengan perbedaan *account* yang digunakan secara ilegal adalah *account* yang mempunyai *privilege* sebagai *administrator* sistem. Istilah *root* diturunkan dari sebuah *account* pada sistem berbasis *UNIX* yang mempunyai *privelege* tidak terbatas. Penyusup yang berhasil melakukan *root compromise* dapat melakukan apa saja pada sistem yang menjadi korban, termasuk menjalankan pogram. Mengubah kinerja sistem, dan menyembunyikan jejak penyusupan.

2.5.5 *Packet sniffer*

Packet sniffer adalah suatu device, baik perangkat lunak maupun perangkat keras yang digunakan untuk memperoleh informasi yang melewati jarngan komputer. Kegunaan dari *packet sniffer* adalah membuat NIC (*Network Interface Card*), contohnya *Ethernet*, dalam *mode promiscuous* sehingga dapat menangkap semua *traffic* dalam jaringan. *Mode promiscuous* adalah mode dimana semua *workstation* pada jaringan komputer "mendengar" semua *traffic*, tidak hanya *traffic* yang dialamatkan ke *workstation* itu sendiri. Jadi *workstation* pada *mode promiscuous* dapat "mendengarkan" *traffic* dalam jaringan yang dialamatkan kepada *workstation* lain. Sebuah *sniffer* dapat berupa kombinasi dari perangkat lunak dan perangkat keras. Keberadaan *sniffer* di dalam jaringan sangat sulit dideteksi karena *sniffer* adalah program aplikasi yang sangat pasif dan tidak membangkitkan apa-apa, dengan kata lain tidak meninggalkan jejak pada sistem.

2.5.6 *Denial of service (DOS)*

Sumber daya jaringan yang berharga antara lain komputer dan *database*, serta pelayanan-pelayanan (*service)* yang disediakan oleh organisasi pemilik jaringan. Kebanyakan *user* jaringan memanfaatkan pelayanan-pelayanan tersebut agar pekerjaan mereka menjadi efisien. Bila pelayanan ini tidak dapat dipergunakan karena sebab-sebab tertentu, maka tentu saja akan menyebabkan kehilangan produktivitas. Sulit untuk memperkirakan penyebab *Denial of service*. Berikut ini adalah contoh penyebab terjadinya *Denial of service*:

- Kemungkinan jaringan menjadi tidak berfungsi karena kebanjiran *traffic*.
- Kemungkinan ada *virus* yang menyebar dan menyebabkan sistem komputer menjadi lamban atau bahkan lumpuh.
- Kemungkinan *device* yang melindungi jaringan dirusak.

2.5.7 Eksploitasi Terhadap Kepercayaan

Seringkali komputer-komputer di dalam jaringan mempunyai hubungan kepercayaan antara satu dengan yang lain. Sebagai contoh, sebelum mengeksekusi perintah, komputer akan memeriksa suatu set dari *file-file* yang menspesifikasikan komputer lain yang ada di dalam jaringan tersebut yang diizinkan untuk menggunakan perintah tersebut. Bila penyerang dapat membuat identitas mereka tersamar sehingga seolah-olah sedang menggunakan komputer yang dipercayai, maka penyerang tersebut akan memperoleh akses ke komputer lain secara ilegal.

2.5.8 Malicious Code

Malicious code adalah suatu program yang bila dieksekusi akan menyebabkan sesuatu yang tidak diinginkan di dalam *user*. *User* sistem biasanya tidak memperhatikan program ini hingga ditemukan kerusakan. Yang termasuk *malicious code* adalah *trojan horse* dan *virus* biasanya disusupkan ke dalam suatu *file* atau program. *Worm* adalah program yang dapat menduplikasikan diri dan menyebar tanpa *intervensi* manusia setelah program tersebut dijalankan. *Virus* juga mempunyai kemungkinan untuk menduplikasikan diri namun biasanya memerlukan *intervensi* dari *user* komputer untuk menyebar ke program atau sistem yang lain. *Malicious code* ini dapat menyebabkan kerusakan atau kehilangan data yang serius.

2.6 Sistem Informasi

Sistem informasi merupakan suatu kumpulan komponen yang bekerja sama untuk mengatur perolehan, penyimpanan, manipulasi dan distribusi informasi. Komponen sistem informasi terdiri dari perangkat keras, perangkat lunak, orang-orang yang membuat produk, menyelesaikan masalah, membuat keputusan, data yang menyediakan informasi, dan produsen yang memberitahu pengguna bagaimana mengoperasikan dan menggunakan sistem informasi.

Menurut Szymanski (1995), fungsi dasar sistem informasi adalah:

1) Menerima data (input)
2) Konversi data menjadi informasi (proses)
3) Menghasilkan informasi (output)

Menurut Stair (1986), beberapa karakterisitik sistem informasi yang baik, antara lain :

1) Tepat pada waktunya, yaitu informasi sampai pada penerimanya tidak terlambat.
2) Akurat, yaitu informasi tersebut bebas dari kesalahan dan tidak bias.
3) Fleksibel, yaitu informasi dapat digunakan masa kini dan masa depan.
4) Bernilai ekonomi, yaitu manfaat dari informasi lebih besar daripada biaya yang dikeluarkan untuk mendapatkannya.
5) *Reliabel*, yaitu informasi benar-benar nyata.
6) Singkat dan sederhana, yaitu mudah dibaca, dimengerti oleh penerima informasi.

2.7 Penelitian Terdahulu

Berdasarkan Penelitian sebelumnya, tesis karya Nur Bagus Dheni T.H, ST, 2006. Analisis Kinerja Keamanan Jaringan Komputer Local Area *Network* (LAN) (kasus pada kantor perusahaan "XYZ"), Program Pasca Sarjana Universitas Gunadarma. *Malware* juga menjadi gangguan dari keamanan sistem jaringan yang dimana *malware* juga menyebabkan data pekerjaan rusak atau hilang, lalu lintas jaringan yang padat, jaringan komputer yang mati yang pada akhirnya hal itu semua dapat mengakibatkan kerugian bagi perusahaan. Dan penulis tesis ini berkesimpulan bahwa sistem keamanan jaringan komputer yang diterapkan

perusahaan yang diteliti belum berfungsi secara optimal. Hal ini terbukti beberapa kali perusahaan yang diteliti mengalami gangguan keamanan sistem jaringan komputer seperti banyaknya komputer yang terinfeksi oleh *malware* sehingga berdampak pada rusaknya data pekerjaan, hilangnya data pekerjaan, matinya jaringan internet yang pada akhirnya mengakibatkan kerugian pada perusahaan.

Berdasarkan (*Logan And Logan, 2003)* serangan *malware* juga mempunyai dampak negatif bagi perusahaan yang dimana didalam jurnal tersebut disebutkan adanya dampak meruginya keuangan suatu perusahaan penjualan di amerika serikat yang menggunakan jaringan komputer dalam melakukan penjualan. Dan di bawah ini merupakan tabel dari jenis-jenis industri yang mengalami kerugian akibat serangan *malware*.

Tabel 2.1.JenisIndustri yang dirugikan oleh serangan malware

No	**Type of Industry**	**Cost per Hour**
1	Retail Brokerage	$6.45 million
2	Credit card sales authorization	$2.6 million
3	Infomercial or 800-number promotions	$199,500
4	Catalog Sales centers	$90,000
5	Airline reservations	$85,000
6	ATM *service*	$14,000

(Sumber : Logan And Logan, 2003)

Penulis Jurnal tersebut juga berkesimpulan bahwa matinya jaringan internet komputer yang dikenal dengan istilah "*downtime*" yang disebabkan oleh serangan *malware* bukan hanya merupakan gangguan yang mempengaruhi divisi Teknologi Informasi saja tapi juga mempengaruhi pada sisi penjualan dan pendapatan perusahaan, kerugian penjualan, harga saham yang turun dan rusaknya reputasi perusahaan. Dampak dari terputusnya komunikasi juga mempengaruhi kinerja dari peralatan-peralatan yang terhubuing kepada sistem jaringan seperti: *e-mail, web, file, database, print servers,* begitu juga dengan para karyawan yang menggunakan *laptop, PC*. *Malware* merupakan aktifitas dari penyerang sistem keamanan jaringan komputer yang mempunyai resiko rendah namun berdampak tinggi bagi si korban. Para *hacker* membantu mereka dalam mencari celah keamanan tiap-tiap perusahaan dan kemudian memperdaya pengguna komputer untuk mengunduh program yang telah disusupi *malware* sehingga akan terlihat seolah-olah, si pengguna komputerlah yang telah menyebarkan *file* yang telah disusupi *malware*.

BAB III
METODE PENELITIAN

3.1 Objek Penelitian

Penelitian ini dilaksanakan pada PT XYZ yang kantor pusatnya terletak di wilayah Jakarta Utara. Perusahaan ini dipilih karena merupakan perusahaan otomotif multi nasional terbesar di Indonesia dan menggunakan teknologi jaringan komputer demi mendukung operasional bisnis usahanya yang ada di berbagai negara.

3.2 Metode Pengumpulan Data

Metode yang digunakan dalam penelitian ini adalah studi kasus dengan mengadakan observasi langsung dilapangan, guna memperoleh gambaran yang mendalam dan lengkap dari suatu subjek yang diteliti sehingga dapat menentukan alternatif strategi keamanan sistem informasi yang tepat bagi perusahaan untuk masa yang akan datang. Teknik yang dilakukan adalah melalui wawancara, studi pustaka, dan survey lapangan.

Data yang diperoleh dari hasil pengamatan langsung di lapangan serta melalui wawancara dengan pihak perusahaan, yaitu berupa :

- Penggambaran mengenai kebijakan penggunaan *USB Storage*.
- Penggambaran tentang teknologi komputer baik *hardware* maupun *software* yang digunakan perusahaan.
- Penggambaran mengenai topologi jaringan komputer perusahaan.
- Penggambaran mengenai sistem keamanan jaringan komputer yang saat ini sudah diterapkan perusahaan.

3.3 Jenis Data

Sumber data yang tersedia disini merupakan sumber data sekunder yang diambil dari divisi T I (Teknologi Informasi) PT XYZ yang kantor pusatnya berlokasi di Sunter, Jakarta Utara.

Adapun data-data yang diperoleh melalui studi pustaka untuk mendukung penelitian ini diperoleh dari dokumen perusahaan (data sekunder), penelitian terdahulu maupun penelitian yang relevan dengan penelitian ini, yaitu berupa :

- Historical Log perusahaan.
- Jurnal-jurnal ataupun buku-buku yang membahas mengenai *Malware*.

3.4 Metode Analisis

Dalam melakukan proses analisis, penulis melakukan pengumpulan LOG dan incident report terhadap kinerja sistem jaringan komputer *LAN*, komputer, *server*, dari serangan *malware* dan dampaknya terhadap kinerja perusahaan. Kemudian penulis juga menggunakan beberapa tools bantuan berupa *software* atau program penguji keamanan jaringan komputer dengan cara melakukan *scan IP Address* dan *Port* scanning menggunakan *Advanced IP scanner*, *Port Scanner* dan *NMAP* untuk mendeteksi *port* yang terbuka yang biasa dilalui oleh *malware*.

Advanced IP Scanner, merupakan *tools* gratis yang bisa di *download* pada url: " *http://www.advanced-ip-scanner.com/"*. Yang berfungsi untuk menscan status dari kumpulan *IP Address* yang ada pada satu segmen sistem jaringan komputer.

Port Scanner, merupakan *tools* gratis yang berfungsi untuk melihat status *port* yang ada pada komputer yang menggunakan sistem operasi *windows* yang dimana *port-port* yang biasa dilalui oleh berbagai macam *malware* akan terlihat

status dari portnya terbuka atau tidak. *Port scanner* dapat di *download* pada url : "*http://www.radmin.com/download/previousversions/portscanner.php*".

NMAP, merupakan *tools* gratis yang biasa digunakan untuk melihat status PC per tiap segmen jaringan apakah terinfeksi *malware* atau tidak, dalam kasus ini *malware conficker*, yang menggunakan *port* 445 untuk menyebar dan menginfeksi korbannya. *NMAP* dapat di *download* secara gratis pada url : "http://nmap.org/".

Penulis juga menggunakan laporan serangan *malware* yang terjadi di PT XYZ dan menggunakannya sebagai sumber informasi mengenai sumber serangan *malware*, tersebut dan juga sebagai perbandingan jumlah serangan *malware* sebelum dan sesudah di terapkannya *USB Storage Controlling*. Dari perbandingan tersebut akan terlihat bahwa serangan *malware* mengalami penurunan setelah di terapkannya *USB Storage Controlling*.

Laporan serangan *malware* yang akan digunakan sebagai perbandingan adalah laporan bulanan bulan Juni 2012 sampai dengan Bulan Desember 2012. Dari laporan bulanan tersebut akan terlihat adanya pengurangan serangan *malware* mulai dari bulan Desember 2013.

Dari laporan bulanan tersebut juga akan dapat diketahui di area mana saja yang banyak terjadi serangan *malware*, apakah di area *office* atau pabrik.

BAB IV
ANALISIS DAN PEMBAHASAN

4.1 Gambaran Umum Perusahaan

PT XYZ merupakan perusahaan yang bergerak di bidang manufaktur otomotif, didirikan sejak tanggal 15 Juli 2003 di Indonesia dan memiliki pabrik-pabrik manufakturnya di berbagai wilayah di indonesia seperti di sunter dan karawang, untuk memenuhi kebutuhan otomotif yang semakin berkembang.

VISI PT XYZ ini adalah " ***menjadi pemain kelas dunia dalam bidang manufaktur dan kesempurnaan distribusi ".*** Sedangkan MISI perusahaan PT XYZ ini adalah:

- Untuk menjaga posisi nomor satu dalam industri otomotif dan jaringan distribusi di Indonesia.
- Menjadikan kepuasan pelanggan sebagai prioritas utama..
- Untuk memberikan kontibusi positif kepada perkembangan sosial ekonomi negara.
- Untuk mendukung perkembangan kesejahteraan diantara para karyawan, dealer-dealer dan para supplier.
- Untuk melindungi keberlangsungan lingkungan dan menjamin keselamatan kerja.
- Untuk mendukung kemampuan individu dan pada saat bersamaan juga mengembangkan semangat tim sebagai isu motivasi utama.

Filosofi PT XYZ adalah :

1. Memberikan kontribusi kepada negara, masyarakat, bangsa, dan dunia melalui langkah-langkah secara profesional dalam proses produksi dan pelayanan yang berkualitas global.

2. Berkembang bersama-sama karyawan, dealers dan supplier atas dasar kepercayaan dan saling menghargai.

PT XYZ memiliki kegiatan utama dibidang manufaktur otomotif sebagai :

1. Produsen mobil nomor satu di Indonesia.
2. *Research And Development Centre* untuk tipe mobil tertentu.
3. Produsen *Sparepart* mobil di Indonesia maupun ekspor ke mancanegara
4. Pengekspor beberapa tipe mobil untuk beberapa negara di asean.

4.1.1 Struktur Organisasi Perusahaan

Saat ini perusahaan melalui Departemen IT yang dimilikinya telah berhasil memiliki divisi infrastruktur TI yang diberi nama I T *Division* (*Information Technology Division*) yang bertugas menangani segala hal yang berhubungan dengan teknologi informasi baik *hardware*, maupun *software*.

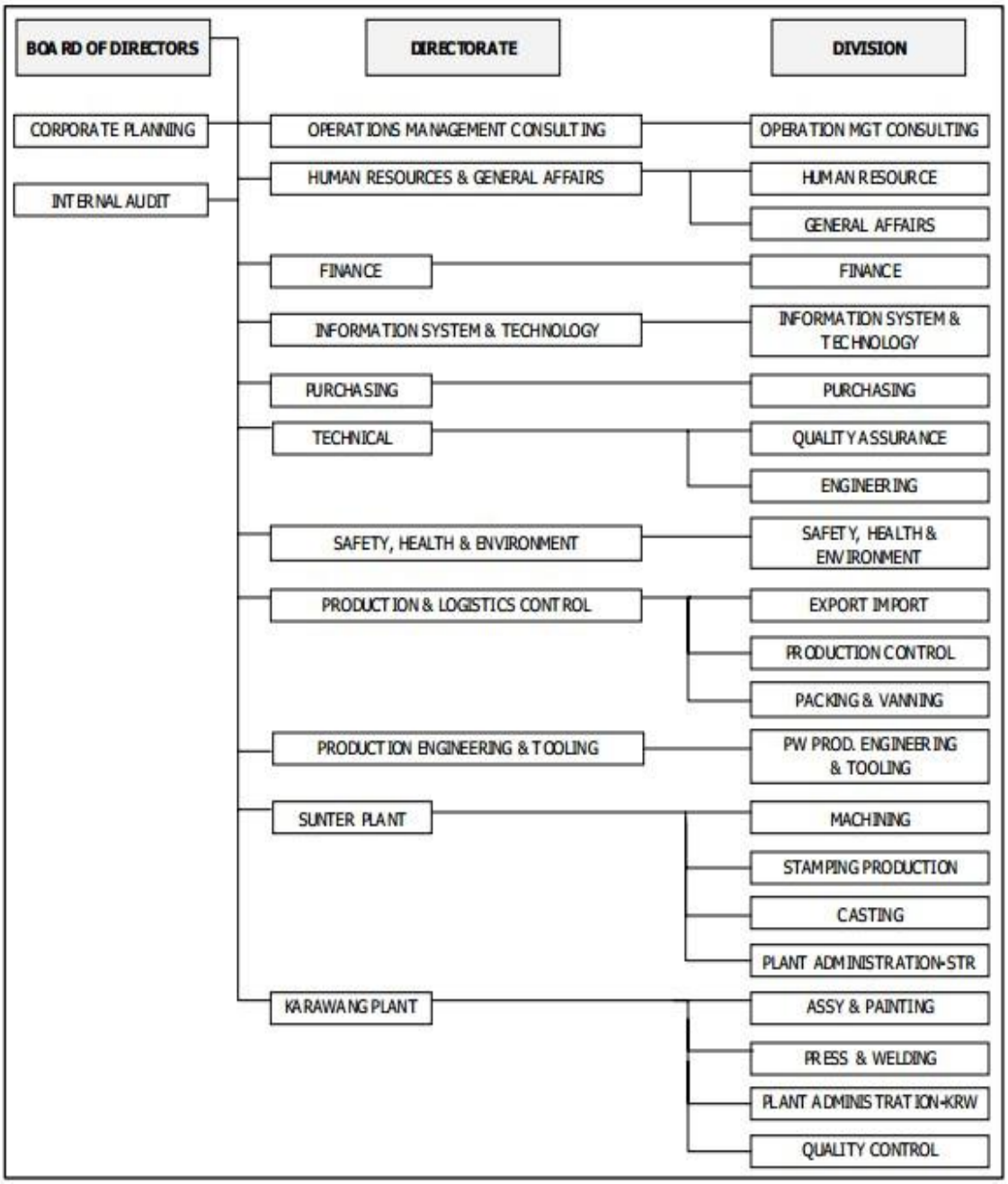
Struktur organisasi Divisi I T merupakan struktur garis. Dimana seorang bawahan hanya mempunyai seorang atasan dan hanya menerima perintah dari atasan tersebut. Adapun struktur organisasi divisi I T dan unit kerja yang ada di dalamnya dapat dilihat pada lampiran 2.

Tingkat pendidikan yang dimiliki oleh rata-rata karyawannya adalah tamatan SMU, Diploma dan Sarjana. Perusahaan juga berupaya meningkatkan kualitas kerja para karyawannya melalui pelatihan-pelatihan yang diadakan oleh perusahaan sendiri maupun oleh perusahaan lain yang bergerak dalam bidang konsultan pelatihan teknologi informasi.

Wewenang pada perusahaan adalah wewenang garis, staff, dan fungsional. Wewenang garis ditujukan dengan adanya hubungan seorang atasan untuk memerintahkan secara langsung kepada bawahannya. Wewenang staf merupakan wewenang yang membantu personil garis dalam memberikan saran, pendapat,

atau usulan mengenai operasional perusahaan. Wewenang fungsional adalah wewenang yang dimiliki personil suatu departemen untuk memberikan saran atau usulan dalam bidangnya masing – masing terhadap personil di departemen lain.

Struktur perusahaan adalah struktur garis dan staff. Struktur garis adalah seorang bawahan hanya mempunyai seorang atasan dan hanya menerima perintah dari atasan tersebut. Struktur staf adalah terdapat unit yang membantu lini seperti *coorporate secretary, legal and tax* dan internal audit. Adapun struktur organisasi perusahaan secara global dapat dilihat pada gambar berikut ini.



Gambar 4.1 Struktur Organisasi PT XYZ

4.1.2 Uraian Pekerjaan

PT. XYZ yang merupakan perusahaan manufaktur otomotif besar dan terkenal di setiap bagiannya mempunyai tugas masing-masing untuk uraian pekerjaan di setiap bagiannya dapat dijelaskan sebagai berikut:

4.1.2.1 *Board Of Directors*

Board of Directors merupakan jajaran direksi yang terdiri dari *President Directors, Vice President directors,* dan *Directors* yang memegang manajemen tertinggi di perusahaan. Beberapa *directors* mengepalai sebuah direktori dengan satu atau lebih divisi di dalamnya.

4.1.2.2 *Corporate Planning*

Corporate Planning merupakan struktur organisasi yang terpisah dari direktorat dengan seorang *General Manager* yang mengepalainya. Fungsi utama *Corporate Planning* adalah sebagai badan *independent* yang menangani masalah yayasan PT XYZ, Komite TQM (*Total Quality Maintenance*), komite kesejahteraan karyawan meliputi keamanan kerja, kesehatan dan kenyamanan lingkungan, serta *reporting* yang harus dilaporkan ke jajaran *Board of Directors* terutama yang berhubungan dengan area kerja perusahaan.

4.1.2.2.1 *Plant* Karawang

PT. XYZ memiliki *Plant* Karawang yang tepatnya berada di Kawasan Industri KIIC (Karawang *International Industrial City*). Pada direktorat ini terdiri dari 2 divisi, yaitu *Assembly (Assy) and Painting*, serta *Press and Welding*.

Divisi Assembly and Painting

Divisi Assembly and Painting merupakan divisi yang memproduksi unit kendaraan mulai proses pengecatan (*painting*) hingga instalasi interior (*body/cabin*) dan *exterior* (*frame*) untuk kijang baru yaitu Kijang Innova yang baru di-launching pada bulan Septenber 2004. Pada umumnya *line* produksi *Assembly* terdiri dari 2 pos, yaitu *Trimming* dan *Chassis*. Beberapa komponen yang terpasang di setiap pos seperti contoh di pos *Trimming* adalah *wiring, weatherstrip, glass, instrument panel, receiver assy*dan sebagainya. Sementara di pos *Chassis* akan dipasang beberapa jenis komponen seperti *engine assy, axle, carpet, tyre assy, fuel tank, seat assy, battery*, dan sebagainya.

Divisi Press and Welding

Divisi Press and Welding adalah divisi yang menghasilkan produk *press part* dan dilanjutkan ke proses pengelasan (*welding*) untuk membuat *cabin assy* sebagai hasil akhir produk sebelum dilanjutkan ke proses *painting* dan *assembling*. Selain ini, divisi ini pun menghasilkan produk *press part* yang dipesan khusus oleh *Divisi Service Parts* sebagai produk *after market*. Untuk kebutuhan ekspor dihasilkan pula *side door* dan *engine hood* yang dikirimkan ke *packing plant*.

4.1.2.2.2 *Plant* Sunter I

Area produksi *Plant* Sunter I terdiri atas 5 divisi dengan hasil produk yang berbeda-beda antara satu divisi dengan yang lainnya.

Divisi Machining

Divisi Machining atau lebih sering disebut sebagai *Engine Plant* memproduksi *Engine Assy* baik untuk kebutuhan domestik maupun untuk ekspor. Selain itu diproduksi pula beberapa *Engine Components*. Divisi ini menyuplai unit *Engine Assy* untuk kendaraan model *Kijang, Dyna, Starlet, Forklift, Crown, Corona, Camry, Corolla*, dan *Soluna*. Selain itu negara-negara Jepang dan Malaysia juga menjadi tujuan ekspor untuk *Cylinder Block*, serta Malaysia,Taiwan, Philippine, dan Vietnam menjadi tujuan ekspor untuk *Engine Assy* dengan tipe engine 7K (1800 cc).

Divisi Jig Tooling

Divisi ini khusus memproduksi *jig-jig* untuk ekspor yang sudah dilakukan sejak 1987. Negara tujuan ekspor dari *Divisi Jig Tooling* yaitu Venezuela,Pakistan, Jepang, Malaysia, dan Philippine.

Divisi Kijang Pick-Up Project

Divisi ini khusus untuk memproduksi kendaraan Kijang jenis *Pick Up*. Divisi ini merupakan pengembangan dari divisi terdahulu yaitu Divisi *Assembly* yang terbagi karena terkait adanya relokasi *plant* Sunter I – Karawang.

4.1.2.2.3 *Plant* Sunter II

Merupakan area produksi yang lain berada di Sunter II dan terdiri atas 4 divisi. Hasil produk utamanya adalah *Press Part, Stamping Tools*, serta persiapan *Packing* dan *Vanning* untuk ekspor.

Divisi *Stamping Production*

Merupakan divisi yang memproduksi *Press Part* untuk kebutuhan produksi domestik dan ekspor melalui *Packing Plant*. Produk utamanya adalah *Stamping Parts* (untuk model Kijang, Dyna, Daihatsu Delta, Hino truck, dan Soluna), pembuatan frame (Kijang dan Dyna), pembuatan fuel tank (Kijang), serta ekspor *Packing Set* CKD/CBU Kijang ke Philippine, Taiwan, Malaysia, Vietnam, dan Afrika Selatan.

Divisi *Stamping Tools*

Produk utama divisi ini adalah *manufacturing dies* untuk *Inner Panel Corolla* dan Daihatsu (1993), *manufacturing dies* untuk Mitsubishi (1994), pembuatan *dies* untuk Kijang serta dirintis penggunaan CAD / CAM (1996), dan pembuatan *dies* untuk AFC (Affordable Family Car) suatu kendaraan yang dipersiapkan menjadi Asean Passenger Car(1997).

Divisi *Casting*

Divisi Casting memproduksi *Cylinder Block, Crank Cap, Crank Shaft*, dan *Flywheel*. Hasil produk divisi ini akan dikirimkan ke divisi *Stamping Production* dan *Machining*. Kapasitas produksinya cukup tinggi mencapai 1000 ton / bulan yang dikerjakan dalam 2 shift.

Divisi *Packing and Vanning*

Merupakan divisi yang khusus melakukan proses ekspor dan *vanning*. Beberapa pemasok lokal mengirimkan komponen ke Divisi *Packing and Vanning* dalam satuan *pieces* maupun *lot set*. Kemudian komponen-komponen tersebut dimasukkan dalam *case* dan di-*vanning* ke kontainer sebelum dikirim melalui pelabuhan Tanjung Priok.

4.1.2.2.4 *Technical*

Merupakan *directorate* yang menangani masalah-masalah tehnik yang terdiri dari Divisi *Engineering* dan Divisi *Quality*. Divisi *Engineering* merupakan salah satu divisi yang ada di PT. XYZ di sinilah *Accessories Development* dilakukan, yang merupakan *local development*, selain itu di Divisi *Engineering* juga menangani administratif yang menyangkut spesifikasi komponen / material. Semua komponen / material akan diterima dari perusahaan induk PT. XYZ di Jepang. *Routing parts* untuk yang pertama kali diterima, kemudian hasil gambar untuk setiap komponen / material akan diinformasikan kemudian. Divisi *Engineering* akan membuat suatu *prototype* atas drawing yang telah diterima, dan dilakukan trial sesudahnya. Hasil trial akan dikonfirmasikan ke kantor pusat di Jepang, apabila mendapat persetujuan maka divisi ini akan mengeluarkan ECI (*Engineering Change Instruction*) ke Divisi *Purchasing* untuk mulai dilakukan pembelian ke pemasok. Setelah komponen / material terpasang dalam unit produksi Divisi *Engineering* masih harus mengecek dimensinya agar tidak terjadi kesalahan ukuran.

4.1.2.2.5 *Quality*

Terdiri atas satu divisi saja yaitu Divisi *Quality* dengan definisi kerja untuk mengamankan jalannya produksi serta mengontrol semua kualitas bahan baku (*raw material*), komponen, barang setengah jadi (*semi-finished goods*), barang jadi (*finished goods / units)*, maupun kualitas kendaraan yang telah dijual serta melayani pengaduan konsumen atas produk yang telah dibeli. Divisi ini

mempunyai peran penting terhadap kepuasan pelanggan ditinjau dari kualitas produk karena akan mempertaruhkan kelangsungan produk di masa yang akan datang.

4.1.2.2.6 *Plant Administration*

Plant Administration juga terdiri atas satu divisi saja yaitu Divisi *Plant Administration* yang bertugas untuk menangani semua proses administratif produksi, seperti penyediaan *consumable parts* (bahan bakar, sarung tangan (*gloves*), *ear plug*, *safety shoes, helmet*,cat, dan sebagainya) serta keamanan dan kenyamanan kerja karyawan di lingkungan perusahaan seperti pengolahan limbah, pengurusan kepersonaliaan, fasilitas toilet, dan sebagainya.

4.1.2.2.7 *Production Control* dan *Export Import*

Production Control and *Export Import* merupakan satu-satunya divisi yang berwenang untuk mengatur penyediaan komponen untuk kebutuhan produksi, mengatur produksi, menentukan rencana produksi melalui MRP (*Material Requirement Plan*), menyuplai komponen ekspor dari gudang ke tempat produksi, merencanakan serta mengontrol sistem operasional logistik di seluruh *plant*, dan sebagainya.

4.1.2.2.8 *Purchasing*

Di dalam Direktorat *Purchasing* hanya terdapat satu divisi saja, yaitu *Purchasing Division*. Divisi ini memiliki tugas untuk mencari referensi komponen / material yang akan digunakan untuk proses produksi dengan harga yang murah dan berkualitas tinggi. Apabila harga penawaran telah disepakati, maka Divisi *Purchasing* akan membuat PO (*Purchase Order*) yang dikirimkan kepada semua pemasok, dan penagihannya oleh pemasok diteruskan langsung ke divisi *Finance*.

4.1.2.3 *Finance* dan Divisi I T

Pada bagian ini terdiri dari 2 divisi yang bertugas menangani masalah keuangan perusahaan dan sistem jaringan informasi internal (*Information Technology*).

Divisi *Finance*

Divisi Finance merupakan divisi yang berfungsi untuk mengatur keuangan perusahaan dan melakukan transaksi atas semua komponen/ material yang diperlukan untuk proses produksi. Sistem transaksi perusahaan telah difasilitasi oleh suatu sistem yang terintegrasi dengan nama SAP (*Speed, Accuration, Precision*). Sistem ini mampu memonitor pergerakan material di semua area untuk menjaga keakurasian asset perusahaan.

Divisi In*formati*on, and Technology (I T)

Divisi IT menangani masalah sistem jaringan komputer. *Database* mengenai *part list* disediakan oleh divisi ini dan bisa diakses oleh masing-masing *user* yang telah diberi wewenang untuk mengaksesnya. Selain itu divisi ini juga memiliki *workshop* untuk menangani masalah kerusakan komputer baik *software* maupun *hardware*. Penulis akan membahas lebih detail tentang divisi I T**.**

4.1.2.4 *Human Resources and General Affairs*

Terdapat 2 divisi dalam Direktorat ini.Secara umum kedua divisi ini bertugas untuk menangani masalah kepersonaliaan serta perawatan aset-aset fisik perusahaan.

Divisi *Human Resources*

Divisi ini menangani masalah administratif kepegawaian, seperti proses rekrutmen tenaga kerja, pengangkatan karyawan, pemberhentian kerja karyawan, penentuan jabatan, surat-surat perijinan, pembayaran gaji dan kesejahteraan karyawan lainnya.

Divisi *General Affairs*

Divisi General Affairs berfungsi untuk perawatan dan pengadaan aset-aset perusahaan seperti gedung, instalasi listrik/ air/ telepon, kendaraan pool, fasilitas parkir, keamanan perusahaan (*Security*), dan sebagainya.

4.1.3 Divisi I T

Divisi I T bertugas menangani masalah sistem jaringan komputer. *Database* mengenai *part list* disediakan oleh divisi ini dan bisa diakses oleh masing-masing pengguna yang telah diberi wewenang untuk mengaksesnya. Selain itu divisi ini juga memiliki *workshop* untuk menangani masalah kerusakan komputer baik *software* maupun *hardware*. Divisi I T juga mempuyai seksi *development* yang berfungsi untuk membuat aplikasi – aplikasi yang dibutuhkan oleh setiap divisi pada PT XYZ.

Struktur Organisasi I T merupakan struktur garis. Dimana seorang bawahan hanya mempunyai seorang atasan dan hanya menerima perintah dari atasan tersebut. Adapun struktur organisasi I T dan unit kerja yang ada didalamnya dapat dilihat pada lampiran 2.

Tingkat pendidikan yang dimiliki oleh rata-rata karyawannya adalah tamatan SMU, Diploma dan Sarjana. Perusahaan berupaya meningkatkan kualitas Sumber Daya Manusianya melalui pelatihan-pelatihan bersertifikasi yang diadakan oleh perusahaan sendiri maupun oleh perusahaan lain yang bergerak dalam bidang konsultan pelatihan teknologi informasi.

Visi dan Misi divisi I T

Visi divisi I T adalah :

- *Become good business patner and provide solution to user through IT.*
- *To be the leader of IT Solution within company groups operation in Indonesia towards the best IT Solution in ASEAN company Groups.*

Misi I T

Misi dari I T adalah : "*Propose IT Solution to contribute to business process improvement*."

4.1.4 Uraian Pekerjaan Divisi I T

Infrastructure Section

Bertugas melakukan pengembangan, *update*, dan pemeliharaan jaringan komputer pada PT XYZ.

Part *System Development* dan *Helpdesk*

Bertugas menyediakan dan memelihara fasililtas komputer yang digunakan oleh *pengguna*.

IT Planning And Management

Bertugas menyiapkan rencana koordinasi dan evaluasi laporan anggaran tahunan.

Vehicle And Engine System Development

Bertugas melakukan pengembangan, peningkatan kualitas dan mendukung semua sistem produksi.

Administration* And *System Development

Bertugas melakukan pengembangan, peningkatan kualitas dan mendukung produksi semua sistem untuk meraih administrasi proyek bisnis yang lebih baik.

Karawang Infra and System Development

Menyediakan dan memelihara Infra Struktur sistem informasi di area pabrik karawang.

Service Part Project

Mengadakan edukasi IT dan forum IT, Penghitungan *Pengguna* Akhir.

Pada divisi IT juga terdapat tempat untuk menginstalasi dan memperbaiki komputer yang baru datang dari supplier maupun komputer rusak, dan tempat ini dinamakan *I T Workshop***.** Didalam *I T workshop* yang berjumlah sekitar 10 orang, 8 orang diantaranya merupakan karyawan *outsource* termasuk juga penulis. untuk 2 orang lainnya merupakan karyawan PT XYZ. Didalam I T *Workshop* juga merupakan tempat dari para *pengguna* komputer di PT XYZ untuk melayangkan keluhan, melakukan perbaikan komputer, maupun permintaan akan komputer, dan perlengkapan IT lainnya.

4.2 Teknologi Sistem Jaringan Komputer LAN Kantor Pusat Perusahaan

Hasil pengamatan penulis pada perusahaan diketahui bahwa disain teknologi jaringan LAN & peripheral *hardware* jaringan yang digunakan perusahaan adalah sebagai berikut ini :

1. Tipe topologi fisik jaringan yang digunakan adalah gabungan dari topologi *Ring*, *Star*, dan Hierarchical. Topologi *Star* digunakan untuk menghubungkan antara komputer *client, host* dengan media *switch*, kemudian antara *switch* dengan *File Server*, dan digunakan pula antara *router* cabang dengan *router* utama di kantor pusat. Topologi

Hierarchical digunakan sebagai penghubung antara *switch*, dan *router* yang kemudian diteruskan menuju *Firewall,* dan kemudian hubungkan ke *Load Balancer* dan baru diteruskan ke internet menggunakan *internet service provider local, astra dan global network*.

2. Tipe media koneksi pasif yang digunakan adalah kabel jaringan jenis UTP kategori 5e, yang digunakan untuk menghubungkan masing-masing komputer dengan media *switch* dan kabel jaringan *fiber optic* yang digunakan untuk menghubungkan masing-masing *switch* dengan *switch* yang berfungsi sebagai *backbond* jaringan.
3. Tipe Media koneksi aktif yang digunakan terdiri dari *switch*, *access point*, *router*. *Switch* berfungsi sebagai: media yang menghubungkan / menggabungkan beberapa *host* komputer dengan menggunakan media kabel UTP, sehingga tebentuk suatu jaringan komputer. *Access point* berfungsi sebagai media koneksi antara *host* komputer yang menggunakan perangkat *wireless* ke dalam suatu jaringan. Sedangkan *router* dalam hal ini merupakan media yang menghubungkan antara jaringan komputer yang terbentuk menggunakan *switch* menuju jaringan internet global dengan menggunakan jasa penyedia layanan internet baik lokal maupun non lokal.
4. Mode akses jaringan yang digunakan adalah model jaringan menggunakan *domain controller* dimana menggunakan satu nama *domain* yaitu: sebagai contoh (ptxyz.co.id) dengan menggunakan beberapa sistem operasi seperti *Windows XP Pro*, Windows7, *Windows* 2000 sebagai sistem operasinya, dimana setiap *host* yang terhubung di dalam jaringan *domain* dapat mengakses *printer server, file server, intranet, internet*, dan lain-lain.

4.3 Sistem Keamanan Jaringan Komputer LAN Perusahaan

Pengendalian sistem keamanan jaringan komputer yang diterapkan perusahaan saat ini meliputi sistem keamanan secara fisik, sistem keamanan pengaksesan data,dan hasil pengolahan data.

4.3.1 Keamanan Fisik

Salah satu upaya yang dilakukan perusahaan dalam upaya pencegahan dari serangan *malware* yang bisa berdampak pada rusaknya data dan hilangnya data, adalah dengan menerapkan sistem keamanan fisik sistem jaringan komputer yang secara umum adalah sebagai berikut :

1. Membuat ruangan DRC (*Disaster Recovery Center*) yang dimana di dalamnya terdiri dari puluhan *File Server*, *Router* ,*Modem* dan *Switch*, *Magnetic Tape* yang berisi data-data hasil *backup* setiap harinya, pendingin ruangan agar suhu ruangan tetap terjaga agar tetap dingin. Alat monitoring suhu ruangan yang akan memberikan peringatan ketika suhu ruangan tidak dalam kondisi dingin, monitor suhu *server* yang akan memberikan peringatan jika ada salah satu *server* yang suhunya tinggi, alat pendeteksi kebakaran dan pintu yang dilengkapi *door access* yang menggunakan *magnetic card* yang hanya akan terbuka jika kartu yang bersangkutan sudah di daftarkan di *server* akses DRC.

   Fasilitas DRC pada PT XYZ mempunyai dua lokasi, yakni di *Head Office* Sunter dan di *branch office* kawasan industri Karawang.

2. Melakukan *backup* data *file server* di dua lokasi DRC (Sunter dan Karawang) ke media tape *backup* secara berkala sebanyak dua kali, yaitu pada pagi hari dan sore hari. Hasil *backup* tersebut akan dikirmkan silang, yang dimana hasil *backup* DRC *Head Office* akan dikirim dan disimpan ke DRC Karawang dan pengiriman menggunakan fasilitas mobil *commuter*, begitu juga sebaliknya.

3. Pengecekan aset peralatan komputer yang dilakukan secara berkala setiap bulan namun hanya sebatas perlengkapan perangkat kerasnya guna tindakan pencegahan dari pengrusakan, pencurian secara fisik.

4. Untuk kabel *fibre optic*, pihak perusahaan melapisi perangkat tersebut dengan pipa baja guna menghindari rusaknya kabel *fibre optic* yang disebabkan oleh : gigitan tikus (hal ini sering terjadi, banyak kabel jaringan yang rusak dikarenakan digigit oleh tikus), bencana alam, adanya pekerjaan penggalian (kabel *fibre optic* yang ditanam di dalam tanah). Penulis juga pernah mengalami peristiwa dimana jaringan di kantor cabang cempaka putih terputus dan produksi terpaksa berhenti selama hampir satu hari yang dimana penyebabnya adalah adanya kabel *fibre optic* di area pabrik yang digigit oleh tikus, maka sejak saat itu semua kabel-kabel jaringan baik UTP maupun *Fibre Optic* yang berada di area pabrik, dilapisi oleh pipa baja.

5. Untuk tipe laptop, perusahaan melakukan tindakan pencegahan dari pencurian yakni dengan mengunci laptop menggunakan gembok untuk laptop yang dihubungkan ke bawah lantai dan hanya bisa di buka kuncinya oleh yang bersangkutan, serta melakukan pendataan terhadap staff yang bertanggung jawab atas komputer maupun laptop berikut dengan kuncinya.

4.3.2 Keamanan Hasil Pengolahan Data

Hasil pengolahan data yaitu berupa informasi, yang tidak luput dari kemungkinan - kemungkinan tindakan yang tidak semestinya, seperti : pencurian data, perubahan data, penghapusan data, dan lain-lain yang sejenis dengan tindakan itu.

Hal-hal yang dilakukan perusahaan dalam mengamankan hasil pengolahan data dari berbagai gangguan yang dapat merugikan perusahaan secara umum adalah sebagai berikut:

1. Setiap komputer harus bergabung ke *domain*, sehingga untuk masuk diharuskan memasukkan *user name* (nama pegawai yang telah didaftarkan ke divisi I T) dan memasukkan *password* untuk *login* ke sistem operasi *windows*.

2. Setiap komputer dilengkapi aplikasi enkripsi, guna melindungi data penting yang akan dikirim dan diterima melalui *E-mail*.
3. Setiap Komputer dan Laptop di lengkapi dengan perangkat lunak anti *malware* ternama guna memproteksi dari serangan *malware* yang dapat menyebabkan kerusakan data, hilangnya data, dan bahkan rusaknya sistem operasi *windows*.

4.4 Analisis Dampak Dan Pengendalian Serangan *Malware*

Pada tahap ini penulis akan mencoba menganalisa hal-hal apa saja yang dapat dilakukan guna mencegah adanya serangan *malware* dengan adanya standardisasi keamanan pada komputer *client*, *server* dan juga sistem jaringan komputer pada PT XYZ. Serta melakukan analisa apakah dampak dari serangan *malware* dan dari manakah sumber serangan *malware* berasal.

4.4.1 Analisisis Standarisasi Keamanan Sistem Jaringan Komputer

Pada tahap ini penulis akan mencoba menganalisa apakah sistem keamanan jaringan komputer yang ada pada PT XYZ sudah memenuhi standar keamanan yang berlaku . Insiden keamanan jaringan komputer yang seringkali dialami perusahaan seperti komputer atau laptop terkena serangan *malware* dan terinfeksi *malware*, data pekerjaan rusak, hilang maupun dicuri, dan sistem jaringan internet mati. Jelas sangat merugikan bagi perusahaan. Beberapa faktor yang sangat berkaitan dengan sumber lubang keamanan pada sistem jaringan komputer PT XYZ, diantaranya *access controls management*, *authentification management*, *physical management*, *anti malware management*. Dalam tahap analisis ini penulis dibantu oleh beberapa *tools* berupa *software sistem* jaringan komputer seperti *NMAP, Port Scanner, Advanced IPScanner*.

4.4.2 Analisis Komputer *Client*

Tipe komputer yang digunakan adalah komputer jenis desktop, *Thin Client*, Laptop dengan berbagai macam sistem operasi seperti *windows* 2000, *Windows XP*, *Windows* 7. Secara *default* sistem operasi ini sudah memiliki *service* yang baik dalam *security management*. Tetapi *service* tersebut belum akan maksimal, kecuali jika memang sudah di konfigurasi secara benar seperti pengaturan *Firewall*, *USB Port*, *user account*, *auto update*, *sharing folder*, *windows patches* dan lain – lain sebagainya. Berdasarkan pengamatan penulis di lapangan masih banyak komputer *client* yang belum terkonfigurasi dengan benar, seperti berikut:

4.4.2.1 *Access Control*

Mengatur agar informasi yang tersedia bagi *user* aman dari berbagai hal yang dapat merusak informasi tersebut. Faktor-faktor yang akan dianalisa adalah sebagai berikut:

4.4.2.1.1 *User Access Administration*, meliputi *accounts* dan *password*

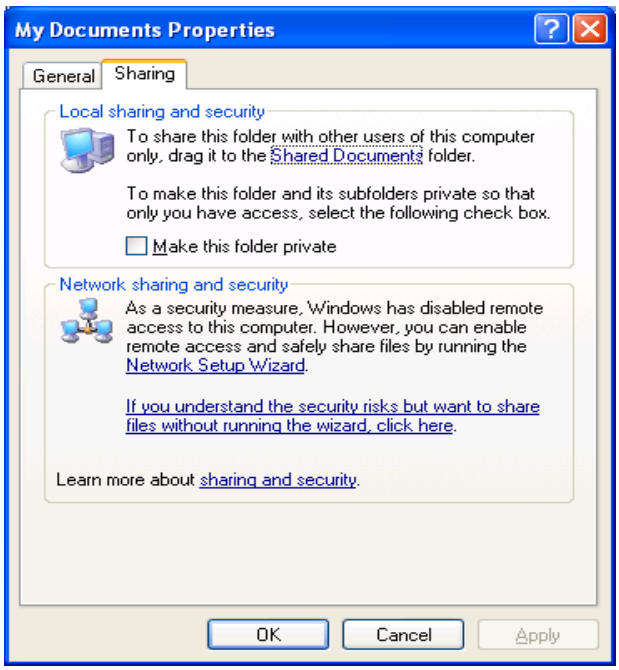
- Ditemukan sebagian besar PC *client* masih menggunakan *password* yang mudah ditebak, seperti: nama pribadi, 12345, abcd, dan lain-lain.
- Ditemukannya *sharing password* dan *user name* sehingga banyak staf di area tersebut yang mengetahui *username* dan *password* tersebut, hal ini sangatlah tidak dianjurkan, dikarenakan bisa dengan mudahnya mengakses data pribadi seseorang, juga bisa mengakses *e-mail* yang bersangkutan dikarenakan sudah terintegrasi dengan nama *domain* dan *user name* yang sudah diberikan.
- Ada beberapa *user account user account* yang wewenangnya setara dengan *administrator* lokal, hal ini sangatlah tidak diperbolehkan, dikarenakan si *pengguna* dapat menginstall aplikasi-aplikasi illegal yang akan sangat merugikan perusahaan ketika diadakan audit *software* oleh

pemerintah yang dikenal dengan HKI (Hak Kekayaan Intelektual) yang biasa diadakan setiap tahun.

- Ada beberapa komputer yang ditempel *user name* dan *passwordnya* di monitor komputer ataupun di keyboard komputer. Hal ini tidak diperkenankan karena siapapun bisa mengakses komputer yang bersangkutan, termasuk pihak luar seperti petugas kebersihan, *staff outsource*, bahkan penjaga keamanan kantor.

4.4.2.1.2 *File* / data *access Administration*, meliputi *permission* dan *file protection* :

- *Windows* Xp merupakan sistem operasi yang memiliki kemampuan untuk membuat beberapa *profile account user* sekaligus. Sehingga masing-masing *account user* hanya dapat mengakses data pada *profile*nya masing-masing. Tetapi pada kenyataannya penulis masih banyak menemukan bahwa setiap data yang ada dapat diakses oleh setiap *account* yang ada dalam sistem *windows* tersebut. Hal ini disebabkan karena setiap *account* tidak memanfaatkan fasilitas *private folder* yang disediakan *windows* xp.

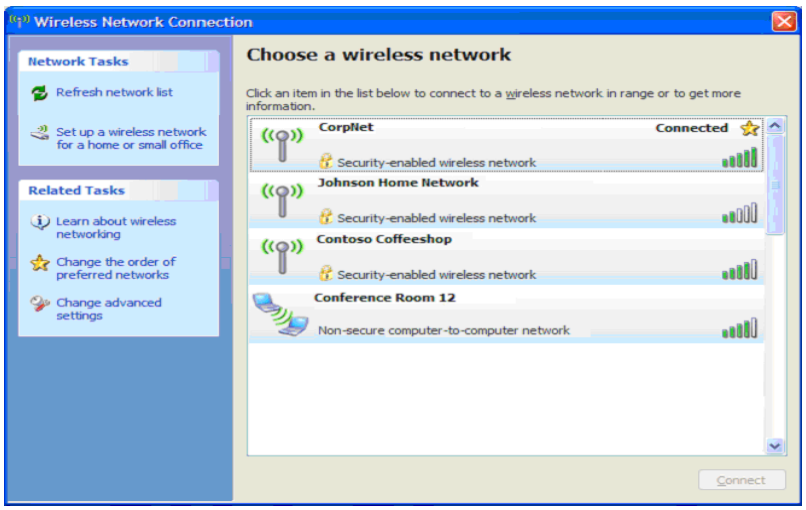


Gambar **4.2** Konfigurasi *Private Folder*

- Ditemukan beberapa *file-file microsoft office* yang sangat penting tidak diproteksi *password*, sehingga dengan mudah siapapun bisa mengaksesnya.

4.4.2.1.3 Access to LAN, meliputi data dan *printer sharing:*

- Mode Akses ke jaringan LAN yang digunakan adalah model jaringan *domain*, dimana setiap komputer *client* yang terhubung ke jaringan tersebut tidak dapat mengakses segala *resources* yang di *sharing* seperti data dan *printer* tanpa adanya hak akses yang harus di daftarkan pada *server active directory*.
- Untuk menghubungkan komputer atau laptop ke dalam jaringan komputer PT XYZ, terlebih dahulu di lakukan pendaftaran MAC (*Media Access Control*) *Address* melalui staff *I T Workshop* dengan menyerahkan form yang sudah mendapat persetujuan atasan langsung yang bersangkutan, hal ini guna menghindari masuknya pihak yang tidak berkepentingan untuk masuk ke dalam jaringan komputer PT XYZ.
- Selain menggunakan kabel jaringan UTP untuk saling menghubungkan komputer ke *switch*, ternyata PT XYZ juga menyediakan koneksi jaringan *wireless access point*. Dalam hal ini setiap komputer atau laptop yang akan menggunakan *wireless access point* diwajibkan mendaftarkan MAC (*Media Access Control*) *Address* melalui staff *I T Workshop* dengan menyerahkan form yang sudah mendapat persetujuan atasan langsung yang bersangkutan.



*Gambar **4.3** Wireless Network Connection*

4.4.2.2 *Autentifikasi*

Autentifikasi merupakan proses verifikasi suatu *input* oleh atau untuk sistem. Sistem akan melakukan pengecekan apakah *user* tersebut telah memiliki hak untuk mengakses sistem. Faktor yang akan dianalisa adalah *password management*, yang meliputi:

4.4.2.2.1 Panjang *password*

Divisi I T sudah memberi peraturan mengenai *password* yang minimal 8 karakter dan banyak *user-user* yang keberatan dikarenakan susah mengingatnya, oleh sebab itu banyak yang menempelkan *password* di komputer / laptop masing-masing.

4.4.2.2.2 *Format password*

Format password yang dibuat cenderung tidak menggunakan karakter kombinasi seperti huruf dengan angka atau simbol. Ataupun kombinasi dengan huruf kapital.

4.4.2.2.3 *Terminal lockout*

User seringkali meninggalkan komputer atau laptop dalam keadaan menyala tanpa mengunci sistem windowsnya dengan *password*, sehingga *user* lain dapat mengoperasikannya dengan mudah.

4.4.2.3 *Malware Management*

Sesuai dengan pengamatan dilapangan *malware management* yang ada pada PT XYZ sangat baik, dikarenakan ada dua *server anti virus* yaitu di *Head Office* Sunter dan *Branch Office* Karawang dan kedua *server anti virus* tersebut hampir setiap hari selalu dicek apakah terupdate atau tidak dan selalu dilakukan pemeliharaan secara rutin setiap minggu, baik secara *hardware* maupun *software*.

- Penulis menemukan ada beberapa komputer *client* yang belum menggunakan program *anti virus* untuk memproteksi sistem dan datanya dari serangan grup dari *malware* seperti *virus*, *worm*, *trojan*, *spyware* dan sejenisnya.
- Ada beberapa komputer dan laptop dimana *anti virus* tidak *terupdate virus* definition *file*, hal ini biasa disebabkan oleh *Harddisk* yang penuh, rusaknya *anti virus* itu sendiri dikarenakan oleh sering matinya komputer tanpa melalui cara yang benar (biasanya disebabkan oleh mati lampu).
- Ada beberapa komputer dan laptop dimana *anti virus* tidak berfungsi (rusak) hal ini dikarenakan adanya serangan *malware* yang terus menerus sehingga *anti virus* yang ada tidak dapat menahan serangan dari *malware*.
- Selama dua tahun ini antara Februari 2010 sampai Desember 2012, banyak terjadi serangan *malware* yang hampir 90% berasal dari *USB Storage* yang dimana belum ada kebijakan untuk melarang *penggunaan USB Storage* dikarenakan belum ada solusi alternatif lain *penggunaan USB Storage*.

4.5 Evaluasi Sistem Keamanan LAN

Sesuai dengan hasil pengamatan dilapangan, PT XYZ memiliki banyak *server* dan menurut data yang penulis terima, ada sekitar 60 *server* yang bebentuk fisik maupun virtual *server* dan semuanya itu mempunyai peranan penting dan saling keterkaitan dalam mendukung proses produksi PT XYZ.

Dalam hal ini, penulis hanya akan membahas beberapa *server* saja, yaitu *mail server, database server, file server, Firewall dan Anti Malware server*. *Mail server* bertugas untuk mengatur lalu-lintas *e-mail* PT XYZ. *Database server* bertugas untuk mengatur data-data perusahaan yang dipakai oleh *user* secara bersama-sama. *File server* berfungsi untuk menyimpan data-data perusahaan tiap divisi dan bagian dan hanya dapat diakses oleh staff yang sudah mendaftarkan *user name* nya pada divisi I T. *Firewall* yang merupakan suatu kombinasi dari perangkat lunak dan perangkat keras yang di desain untuk memeriksa aliran lalu-lintas jaringan dan permintaan *servis* berfungsi untuk menjaga keamanan sistem jaringan komputer dari serangan luar dan pihak-pihak yang tidak berhak masuk ke dalam sistem jaringan komputer perusahaan. *Anti malware server* merupakan *server anti virus* yang berbentuk *virtual* dan ada dua buah *server anti virus* yang dimana berlokasi di kantor pusat dan di kantor cabang, *server* ini berfungsi untuk melakukan manajemen terhadap *client-clientnya* yang berjumlah hampir 1100 *client* yang harus tetap *ter-update virus definitionnya*, mengumpulkan *malware attack log, anti virus status log, connection client status, virus definition log*. *Server anti virus* ini juga penting dalam menjaga keamanan sistem jaringan komputer agar tidak ada *malware* yang masuk dan menyebar kemudian melakukan serangannya.

Secara garis besar sistem keamanan yang dimilki komputer *server* sudah jauh lebih optimal baik dari sisi keamanan secara fisik maupun hasil pengolahan data. Hanya saja ada hal yang perlu menjadi perhatian, yaitu:

- Kurang tertatanya dokumentasi dari konfigurasi sistem yang telah dibuat. Dengan banyaknya jumlah *server* yang ada hampir sekitar 60 *server*, maka

jika terjadi *server* mati mendadak, ada beberapa *server* yang sulit ditemukan lokasinya. Jika hal ini terjadi, maka tentunya akan mengganggu proses produksi yang menggunakan *server* tersebut.

- Kurangnya koordinasi antara pihak I T *server management* dengan pihak IT security dimana ketika ada *server* yang baru terinstall baik fisik maupun virtual, belum di laporkan ke pihak I T security sehingga ada beberapa *server* baru yang tidak memenuhi standar I T security seperti tidak adanya *anti virus*, sistem operasi *windows* yang belum standar, sistem operasi *windows* yang belum terupdate *security patchesnya*, adanya *port USB Storage* yang masih terbuka, *password administrator* lokal yang tidak standar dan sebagainya.

4.6 Optimalisasi Pengendalian Keamanan LAN

Walaupun perusahaan telah menerapkan strategi sistem keamanan jaringan komputer dalam mengamankan sistem informasinya dari hal-hal yang dapat merugikan perusahaan, namun pada kenyataannya seringkali terjadi insiden-insiden keamanan jaringan komputer dan berdampak negatif bagi kegiatan seperti kehilangan ataupun rusaknya data pekerjaan, jaringan internet yang mati, komputer atau laptop yang terserang berbagai macam tipe *malware* yang masuk melalui *USB Storage* dan kemudian menyebar menggunakan sistem jaringan komputer dan lain sebagainya. Hal ini disebabkan oleh beberapa hal, antara lain:

- Kesalahan konfigurasi. Kadang-kadang karena kurang ketelitian atau lupa, konfigurasi sebuah sistem kurang benar sehingga menimbulkan lubang keamanan. Misalnya mode (permission atau kepemilikan) dari berkas yang menyimpan *file* penting secara tidak sengaja diubah sehingga dapat diubah atau ditulis oleh orang-orang yang tidak berhak.
- Implementasi kurang baik. Lubang keamanan yang disebabkan oleh kesalahan oleh kesalahan implementasi sering terjadi. Banyak program yang diimplementasikan secara terburu-buru sehingga kurang cermat dalam pengkodean. Akibatnya pengecekan atau *testing* yang harus dilakukan menjadi tidak dilakukan.

- Komputer / laptop masih menggunakan konfigurasi awal dari *vendor* (dengan *password* yang sama).
- Kurangnya koordinasi antara setiap seksi di *I T*, terutama seksi *server management*, *I T workshop, dan I T security* yang dimana banyak komputer / laptop belum memenuhi standar dari *I T security*.

4.7 Analisa Celah Keamanan

Pada umumnya, pengamanan dapat dikategorikan menjadi dua jenis yaitu pencegahan (*preventif*) dan pengobatan (*recovery*). Usaha pencegahan dilakukan untuk meminimalkan celah lubang keamanan, sementara usaha-usaha pengobatan dilakukan apabila sistem telah mengalami gangguan keamanan. Usaha-usaha untuk mengoptimalkan pengendalian keamanan sistem jaringan komputer dapat dilakukan dengan cara-cara sebagai berikut:

4.7.1 Mengatur *Autentifikasi* dan Hak Akses

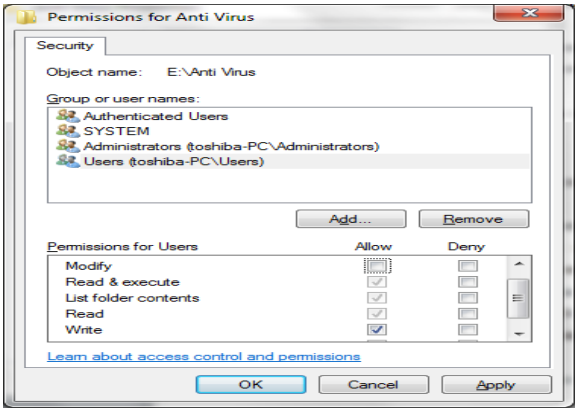
Salah satu cara yang digunakan untuk mengamankan informasi adalah dengan mengatur akses ke informasi melalui mekanisme "authentication" dan "*access control*". Implementasi dari mekanisme ini antara lain dengan menggunakan "*password*". Jika akan menggunakan sebuah sistem atau komputer, *user* diharuskan melalui proses *authentication* dengan menuliskan "*userid"* dan "*password*". Informasi yang diberikan ini dibandingkan dengan *userid* dan *"password"* yang berada di sistem. Apabila keduanya valid, *user* yang bersangkutan diperbolehkan menggunakan sistem. Apabila ada yang salah, pemakai tidak dapat menggunakan sistem. Informasi tentang kesalahan ini biasanya dicatat dalam berkas *log*. Besarnya informasi yang dicatat bergantung kepada konfigurasi dari sistem setempat. Misalnya, ada yang menuliskan informasi apabila *user* memasukkan *userid* dan *password* yang salah sebanyak tiga kali , maka *userid* tersebut akan di blok dan tidak akan bisa *login* sampai

pengguna yang bersangkutan melapor ke divisi I T. Informasi tentang waktu kejadian juga dicatat.

Proses pemilihan *password* juga menjadi salah satu faktor yang harus diperhatikan dalam proses *Autentifikasi*. Dengan adanya kemungkinan *password* dijebol misalnya dengan menggunakan program *password cracker*, maka memilih *password* sebaiknya tidak menggunakan daftar informasi yang berhubungan dengan hal-hal berikut :

- Nama diri sendiri, nama ayah / ibu, nama pacar / istri.
- Tanggal kelahiran.
- Alamat rumah.
- Dan hal-hal lainnya yang mudah ditebak oleh orang lain

Setelah proses *authentication*, pemakai diberikan akses sesuai dengan level yang dimilikinya melalui sebuah *access control*. *Access control* ini biasanya dilakukan dengan mengelompokkan pemakai dalam "group". Ada group yang berstatus pemakai biasa, ada tamu, dan ada juga *administrator* atau *super user* yang memiliki kemampuan lebih dari group lainnya. Pengelompokan ini hendaknya disesuaikan dengan kebutuhan dari *penggunaan* sistem pada perusahaan.



Gambar 4.4 Pengaturan access control

4.7.2 Memasang Proteksi

Perusahaan dapat menambahkan suatu sistem proteksi untuk lebih meningkatkan keamanan sistem jaringan komputernya. Proteksi ini dapat berupa *Firewall* dan *anti virus*. *Firewall* dapat digunakan untuk memfilter *e-mail*, informasi, akses, atau bahkan dalam level paket. Sebagai contoh, digunakan untuk membatasi akses kepada servis atau aplikasi tertentu. Misalnya, servis untuk "*telnet*" dapat dibatasi untuk komputer tertentu saja atau membatasi *user* untuk melakukan akses ke situs-situs *web* yang membawa dampak negatif bagi perusahaan. Sedangkan untuk proteksi dengan menggunakan sistem *anti virus* seperti *Symantec Anti virus, Mcafee, Trend micro, Kapersky* akan sangat berguna sekali untuk memproteksi sistem jaringan komputer dari serangan berbagai macam tipe *malware*, dan dalam hal ini PT XYZ telah memiliki *server anti virus*, sehingga dapat dengan mudah mengontrol serangan – serangan *malware* yang terjadi.

4.7.3 Menggunakan Program Enkripsi

Salah satu mekanisme untuk meningkatakan keamanan adalah dengan menggunakan teknologi enkripsi. Enkripsi merupakan suatu teknik yang mentransformasikan suatu input ke dalam suatu output sehingga tidak dapat terbaca tanpa kunci pembukanya. Data-data yang akan dikirimkan diubah sedemikian rupa sehingga tidak mudah disadap. Perusahaan dapat menggunakan program enkripsi ini untuk melindungi data-data yang sifatnya sangat rahasia, sehingga tidak dapat dimanfaatkan oleh orang yang tidak berhak. Teknik ini juga dapat dimanfaatkan oleh perusahaan untuk proses *Autentifikasi password* dan transfer data antar komputer melalui sistem jaringan komputer, khususnya yang memakai jaringan *wireless*.

4.7.4 Mengontrol *penggunaan USB Storage*

Salah satu media penyebaran *Malware* adalah dengan menggunakan *USB Storage* atau yang kita kenal dengan *flashdisk*. Berdasarkan laporan bulanan serangan *malware* yang menyerang PT XYZ, terdapat ribuan serangan *malware* yang menyerang komputer yang ada dalam sistem jaringan komputer PT XYZ dan sebagian besar serangan *malware* bersumber dari *USB Storage* yang dimana *penggunaan*nya tidak dikontrol oleh si pengguna komputer PT XYZ dengan kata lain, *USB Storage* yang digunakan dipakai diluar area kerja PT XYZ seperti, rumah, warnet, dan area – area lainnya diluar area kerja PT XYZ.

4.7.5 *Backup* Secara Rutin

PT XYZ juga melakukan *backup* rutin yang dilakukan sebanyak dua kali sehari, hasil *backup* disimpan di tiap cabang yang berbeda, hasil *backup* dari kantor pusat sunter di simpan pada kantor cabang karawang, begitupun juga sebaliknya dan setiap minggu hasil dari data *backup* di *restore* guna mengetahui hasil dari *backup* data berhasil atau tidak. Kegiatan *Backup* ini juga akan terasa manfaatnya jika ada data-data maupun informasi yang terkena *virus* sehingga mengalami kerusakan maupun hilang dan perlu dilakukan pengembalian data sebelumnya.

4.8 Laporan Serangan *Malware*

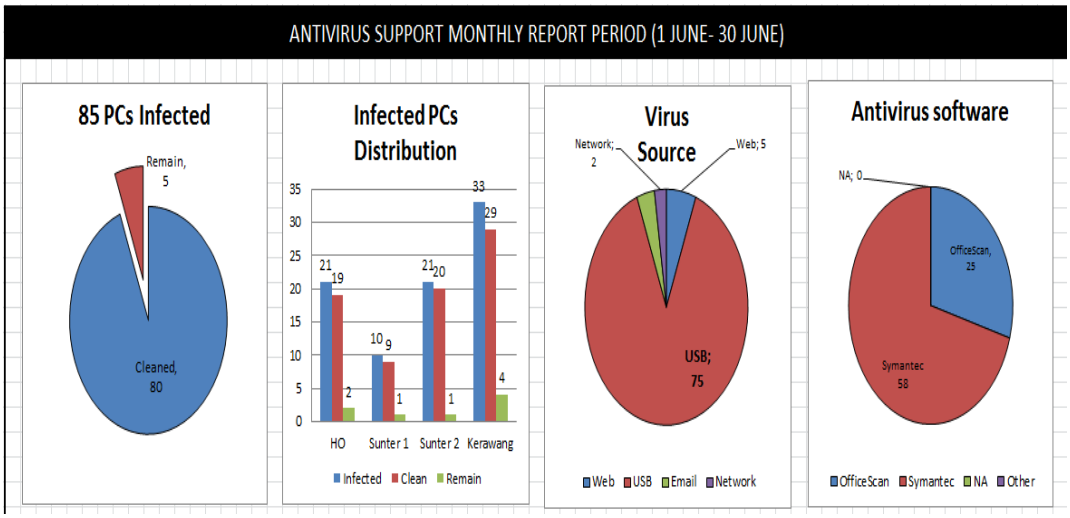
Pada tahap ini penulis menggunakan satu buah laporan bulanan yang berisi mengenai serangan *malware* pada periode 1-30 Juni 2012 yang dimilki oleh *PT XYZ* dan digunakan untuk mengevaluasi sumber *malware*, jenis *malware*, total serangan *virus* dan total komputer yang terinfeksi oleh *malware*.

4.8.1 Penjabaran Laporan bulanan *Anti virus* PT XYZ

Melalui laporan bulanan *Anti virus* ini, penulis akan menjelaskan tentang berapa banyak jumlah komputer yang terinfeksi dalam bulan Juni antara tanggal 1-30 Juni 2012, berapa banyak jumlah komputer yang terinfeksi oleh berbagai macam tipe *malware* yang ada pada tiap cabang PT XYZ, baik di cabang Sunter maupun Karawang, kemudian dapat diketahui pula berasal dari mana sumber serangan *malware* tersebut, apakah dari Internet, *USB Storage*, *E-mail* ataupun dari sumber lain, dan dari laporan bulanan tersebut juga akan diketahui *Anti virus* apa saja yang digunakan oleh komputer PT XYZ, dan *Anti virus* yang digunakan menggunakan *Anti virus* ternama.

Laporan Bulanan ini juga akan dijadikan dasar untuk melakukan tindakan selanjutnya dalam mengatasi serangan *malware* ini yang semakin hari semakin banyak dan beraneka ragam bentuknya serta ada beberapa tipe *malware* varian terbaru yang belum dapat terdeteksi oleh *anti virus* ternama, sehingga hal ini akan sangat mengganggu kinerja sistem jaringan komputer PT XYZ yang pada akhirnya akan mengganggu kinerja dari PT XYZ khususnya para karyawan yang menggunakan fasilitas sistem jaringan komputer PT XYZ seperti mengirim *E-mail*, Intranet, *File Server*, mengupload gambar, audio, video dan lain sebagainya.

Laporan Bulanan ini juga digunakan untuk bahan evaluasi divisi IT dari PT XYZ mengenai status keamanan sistem jaringan komputer PT XYZ, adakah jenis-jenis varian *malware* baru yang belum bisa terdeteksi oleh *Anti virus* yang digunakan oleh PT XYZ. Karena dalam beberapa bulan ini ada beberapa tipe *malware* yang belum bisa terdeteksi dengan baik oleh *anti virus* yang digunakan oleh PT XYZ dalam operasionalnya.



Gambar 4.5 Laporan bulanan bulan Juni 2012 serangan malware PT XYZ

Dari gambar diatas dapat diketahui bahwa ada sekitar 85 komputer yang terinfeksi oleh berbagai macam serangan *malware* dan area serangan *malware* paling banyak berada di area karawang yang merupkan area pabrik, kemudian sumber dari serangan *malware* tersebut sekitar 75 komputer yang terinfeksi *malware* tersebut berasal dari *USB Storage* yang dimana pada PT XYZ *penggunaan USB Storage* masih belum dikontrol dan diawasi dengan baik dan dari sisi *anti virus* yang digunakan ada 85 komputer yang menggunakan *anti virus* ternama dan selalu terupdate, dari laporan itulah penulis berkesimpulan bahwa *USB Storage* merupakan media perantara serangan *malware* yang paling mudah digunakan oleh *malware* dalam menyebarkan dan menyerang sistem jaringan komputer PT XYZ.

Berdasarkan laporan tersebut maka divisi Teknologi Informasi PT XYZ akan membuat kebijakan berupa *USB Storage Controlling Management* yang dimana *penggunaan USB Storage* akan di kontrol *penggunaannya*, diawasi dengan ketat dan hanya boleh digunakan di dalam internal PT XYZ jika sudah mendapat persetujuan dari manajemen Teknologi Informasi.

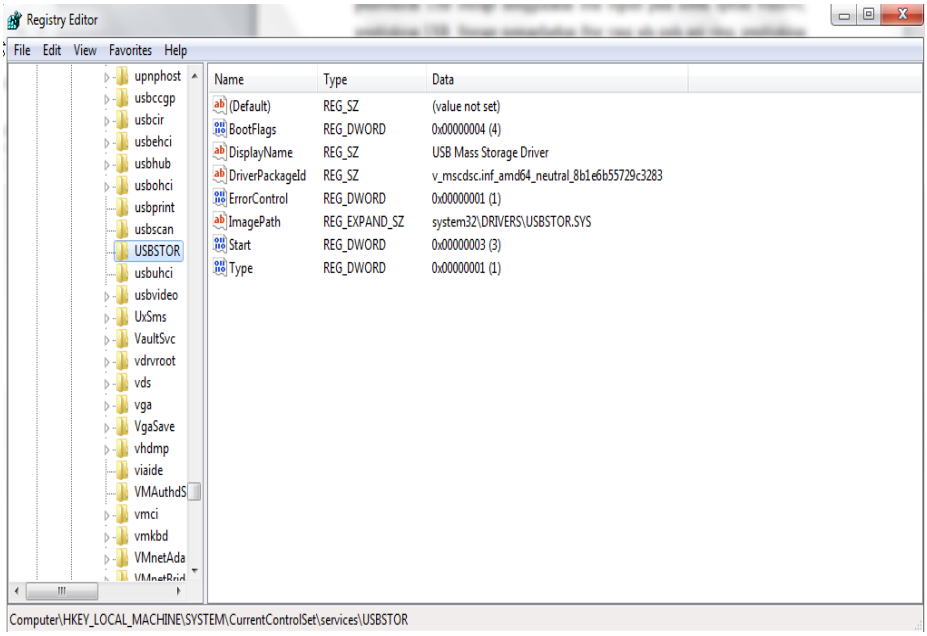
4.8.2 *USB Storage Controlling Management*

Divisi Teknologi Informasi menerapkan *USB Storage Controlling Management* yang bertujuan untuk mengurangi jumlah serangan *malware* dan mengurangi jumlah komputer yang terinfeksi oleh *malware* dan juga mengurangi insiden gangguan sistem jaringan komputer, karena berdasarkan laporan yang ada, ketika terjadi serangan *malware*, maka sistem jaringan komputer PT XYZ mengalami gangguan seperti melambatnya kinerja sistem jaringan komputer.

Ada beberapa cara dalam menerapkan *USB StorageControlling Management* yaitu: pemblokiran *USB Storage* menggunakan fitur *regedit* pada sistem operasi *windows*, pemblokiran *USB Storage* memanfaatkan fitur yang ada pada *anti virus*, pemblokiran *USB Storage* melalui *BIOS* yang ada pada tiap komputer.

4.8.2.1 Pemblokiran *USB Storage* menggunakan *Fitur Regedit* Pada Sistem Operasi *Windows*

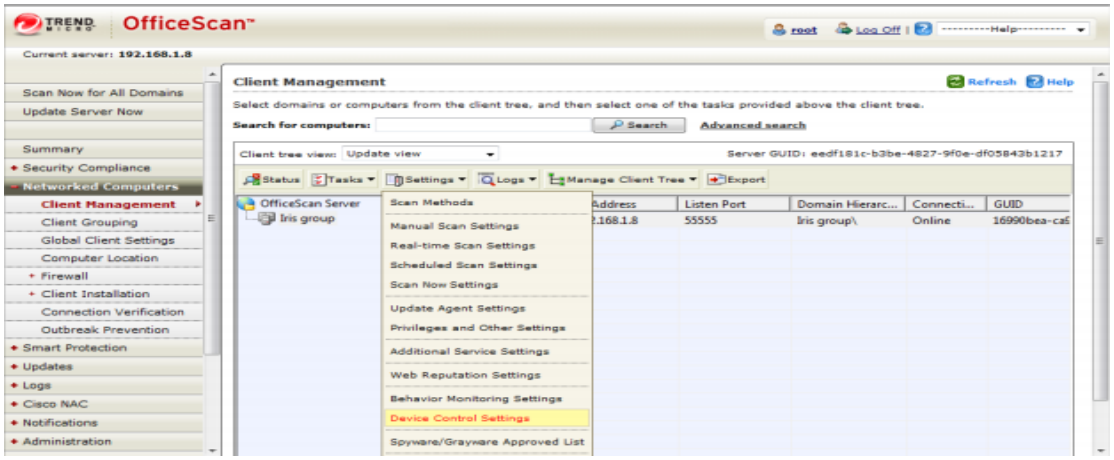
Cara pemblokiran ini dilakukan memanfaatkan *fitur regedit* pada sistem operasi *windows* dan cara ini dilakukan menggunakan fasilitas *active directory* pada *server* OS *Windows* sehingga ketika si *pengguna* login ke dalam *domain* PT XYZ, maka secara otomatis *USB Storage* akan diblokir sehingga tidak dapat digunakan, namun jika ingin menggunakan *USB Storage*, maka si *pengguna* diharuskan melalui prosedur yang telah dibuat oleh divisi teknologi informasi PT XYZ dan *USB Storage* yang akan digunakan diharuskan dipakai pada lingkungan internal PT XYZ. Berikut ini merupakan gambar fitur regedit untuk pemblokiran *USB Storage* pada sistem operasi *windows*.



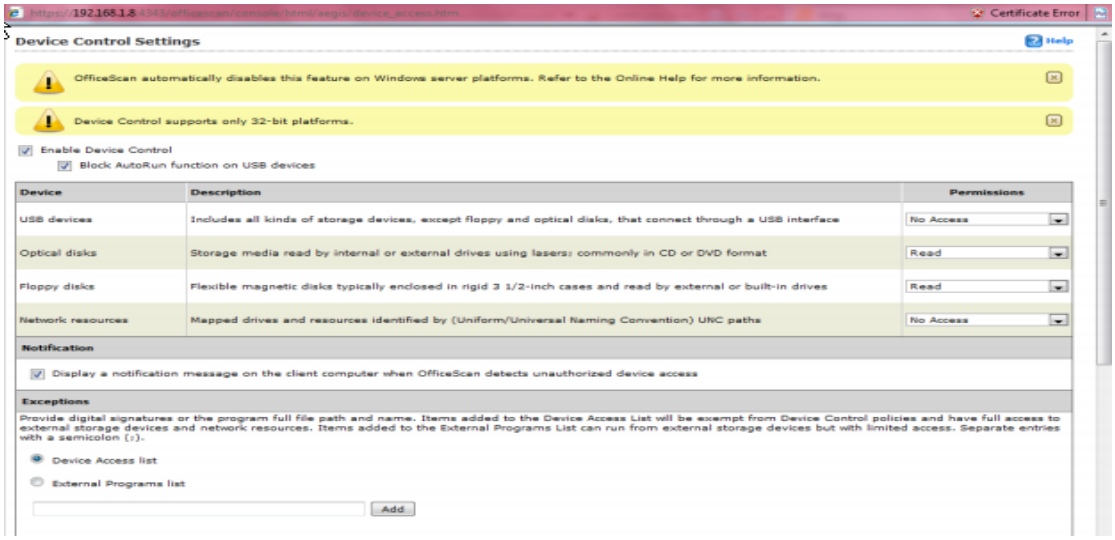
Gambar 4.6 Pemblokiran USB menggunakan regedit pada OS Windows

4.8.2.2 Pemblokiran *USB Storage* Menggunakan *Fitur* yang ada pada *Anti Virus* Ternama

Cara pemblokiran ini dilakukan memanfaatkan fitur yang ada pada *server anti virus manager* ternama, cara ini hanya dapat digunakan jika komputer telah terinstall *Anti virus*, dan cara ini bisa dikatakan efektif dikarenakan komputer dan *notebook* yang ada pada PT XYZ telah terinstall *Anti virus* ini, melalui fitur ini, *USB Storage* yang akan digunakan harus di periksa dan di daftarkan terlebih dahulu ke divisi teknologi informasi sehingga *USB Storage* yang akan digunakan benar benar terbebas dari *virus*. Berikut ini merupakan gambar dari fitur yang ada pada *server anti virus* manager untuk memblokir penggunaan *USB Storage*.



Gambar 4.7. Pemblokiran USB Menggunakan Fitur pada server Anti virus



Gambar 4.8. Pemblokiran USB Menggunakan Fitur pada server Anti virus

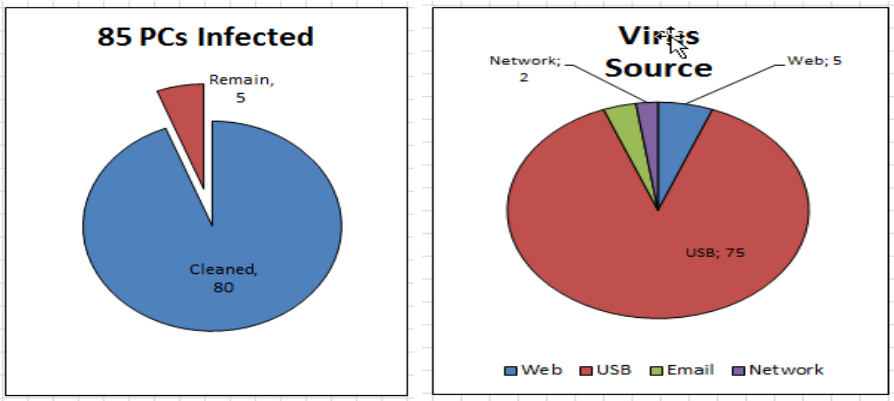
Dari gambar diatas dapat di lihat bahwa fitur yang ada pada *server Anti virus* tidak hanya dapat melakukan pemblokiran *USB Storage*, tapi juga bisa mendaftarkan *USB Storage* yang akan di gunakan, sehingga tidak sembarangan *USB Storage* dapat digunakan oleh karyawan – karyawan PT XYZ, hal ini dilakukan dengan tujuan meminimalkan serangan *malware* yang berasal dari *penggunaan USB Storage* yang tidak terkontrol.

4.8.3 Perbandingan Sebelum *USB Storage Controlling* dan setelah *USB Storage Controlling*

Kali ini penulis akan membandingkan hasil dari *USB Storage Controlling* dengan menggunakan laporan bulanan *anti virus* bulan 2012 sebelum di terapkannya *USB Storage Controlling* dan laporan bulanan *anti virus* bulan Desember 2012 sesudah diterapkannya *USB Storage Controlling* yang dimana jumlah serangan *malware* menurun drastis setelah adanya *USB Storage Controlling*. Hal ini dilakukan dengan cara memberikan akses *USB Storage* hanya kepada staf-staf tertentu dan *USB Storage* yang digunakan berasal dari divisi IT PT XYZ, yang diberikan setelah disosialisasikan dahulu cara *penggunaannya*.

4.8.3.1 Laporan Bulanan *Anti virus* Juni 2012

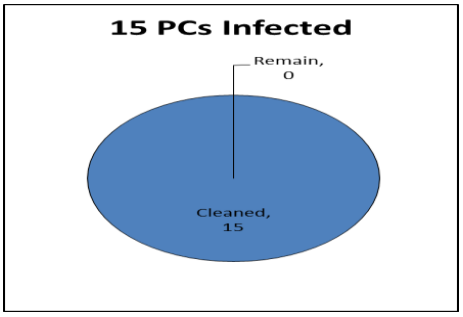
Pada laporan Bulanan *anti virus* bulan juni 2012, sebelum adanya *USB Storage Controlling*, tampak bahwa jumlah komputer yang terinfeksi *malware* adalah 85 unit komputer dan sebanyak 75 komputer yang terinfeksi *malware* berasal dari *USB Storage*.

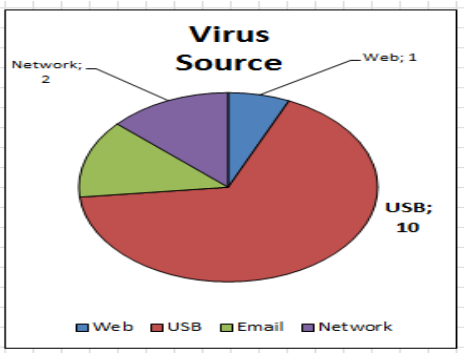


Gambar 4.9. Laporan bulanan anti virus bulan Juni 2012

4.8.4 Laporan Bulanan *Anti virus* Desember 2012

Pada laporan Bulanan *anti virus* bulan Desember 2012, setelah adanya *USB Storage Controlling Management*, tampak bahwa jumlah komputer yang terinfeksi *malware* adalah 15 unit komputer dan sebanyak 10 komputer yang terinfeksi *malware* berasal dari *USB Storage*.





Gambar 4.10. Laporan bulanan anti virus bulan Desember 2012

4.9 Pembahasan Hasil Dari *USB Storage Controlling Management*

Dari hasil perbandingan yang dilakukan dengan menggunakan laporan bulanan *Anti virus* bulan Juni 2012 dan *Anti virus* bulan Desember 2012. Dapat disimpulkan bahwa sebagian besar serangan *malware* yang terjadi berasal dari *USB Storage*, oleh karena itu divisi Teknologi Informasi PT XYZ mengambil tindakan berupa *USB Storage Controlling* yang dimulai diterapkan pada bulan Oktober 2012 sampai sekarang dan dari tindakan tersebut, berdasarkan laporan *anti virus* bulan Desember 2012 terlihat bahwa jumlah komputer yang terinfeksi *malware* menurun menjadi 15 komputer dan sumber serangan *malware* yang berasal dari *USB Storage* mengalami penurunan menjadi 10 komputer. Sistem jaringan komputer PT XYZ juga jarang sekali mengalami gangguan yang disebabkan oleh serangan *malware*

Dari hasil perbandingan tersebut, maka penulis berpendapat bahwa sistem *USB Storage Controlling* bisa dikatakan efektif menurunkan serangan *malware* dan menurunkan gangguan sistem jaringan komputer PT XYZ.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil penelitian yang penulis lakukan, maka penulis mengambil kesimpulan bahwa terganggunya sistem jaringan komputer dan rusaknya data dan bahkan hilangnya data merupakan dampak dari serangan *malware* pada keamanan sistem jaringan komputer PT XYZ. Sebagian besar serangan *malware* yang terjadi menggunakan media perantara *USB Storage*. Setelah dilakukan *USB Storage Controlling management*, dampak dari serangan *malware* yang terjadi bisa dikatakan berkurang.

5.2 Saran

Perlunya pengawasan ekstra dalam *penggunaan USB Storage* di dalam lingkungan kerja PT XYZ. Penulis melihat dibutuhkannya solusi alternatif dari *penggunaan USB Storage* guna mengurangi serangan *malware* yang berasal dari *USB Storage*. Perlu adanya sosialisasi dan kampanye kepada seluruh karyawan PT XYZ didalam lingkungan PT XYZ mengenai bahaya dari serangan *malware* yang penyebarannya menggunakan media *USB Storage*.

Penulis juga melihat diperlukannya pengecekan rutin mingguan atau bulanan kepada komputer-komputer atau *notebook* yang tidak terupdate *anti virus*nya atau tidak terinstallnya *anti virus*.

DAFTAR PUSTAKA

Aaron, Hackworth (2005) Hackworth CERT Coordination Center www.cert.org/archive/pdf/*spyware*2005.pdf. Akses Terakhir 30 Desember 2012.

Ahmad, Yani (2009) *Jurus Ampuh membasmi Virus komputer*.

Eugene, H.Spafford, Eugene Department of Computer Sciences Purdue University West Lafayette, IN 47907–1398 spaf@cs.purdue.edu (1994) *Computer Viruses as Artificial Life* http://spaf.cerias.purdue.edu/tech-reps/985.pdf. Akses Terakhir 30 Desember 2012.

Gil, Tahan. Lior, Rokach. Yuval, Shahar Department of In*format*ion Systems *Engineering* Ben-Gurion (2012) *Mal-ID: Automatic Malware Detection Using Common Segment Analysis andMeta-Features Malware* http://jmlr.csail.mit.edu/papers/volume13/tahan12a/tahan12a.pdf. Akses Terakhir 30 Desember 2012.

Nur Bagus Dheni T.H, ST (2006): *Analisis Kinerja sistem Keamanan Jaringan Komputer Local Area Network Kasus pada kantor perusahaan "XYZ"*, Program Pasca Sarjana Universitas Gunadarma.

Patricia, Y. Logan .Stephen, W.Logan (2003) *Bitten by a Bug: A Case Study in Malware Infection*. http://www.jise.org/Volume14/14-3/Pdf/14%283%29-301.pdf. Akses terakhir 30 Desember 2012.

Sadia, Noreen (2009*) Evolvable Malware*. http://www.geneticprogramming.org/hc2009/3-Noreen/Noreen-Paper.pdf . Akses Terakhir 30 Desember 2012.

Teguh Wahyono, S.Kom (2007) *Building and Maintenance PC Server*.