Prinsip dan Siklus Hidup Keamanan Informasi

Aji Supriyanto
Fakultas Teknologi Informasi –Universitas Stikubank Semarang
email : ajisup@gmail.com

Abstrak : Banyak organisasi yang memanfaatkan perangkat teknologi informasi berbasis jaringan baik local maupun global untuk mendukung tujuan pengembangan organisasinya. Namun banyak yang tanpa disadari mengimplementasikan sistem jaringan computer tersebut tanpa dibarengi dan diimbangi dengan sistem keamanan yang memadai sesuai dengan standar keamanan yang berlaku. Hal itu dikarenakan karena banyak yang tidak menggunakan prinsip-prinsip pengamanan sesuai standar, dan dalam mengimplementasikan tidak melalui tahap siklus hidup keamanan informasi. Untuk mengatasi kendala itu, maka dari itu sebuah organisasi harus memiliki patokan atau standar baku untuk menerapkan sistem keamanan sesuai dengan prinsip standar seperti yang dikeluarkan oleh NIST. Selain itu sangat penting sekali diperlukan komitmen implementasi keamanan, dengan cara menerapkan sesuai siklus hidup keamanan informasi oleh para user, *system engineer*, spesialis IT, manajer program dan petugas keamanan informasi.

Kata kunci : keamanan, informasi, prinsip, dan siklus hidup

PENDAHULUAN

Sistem Keamanan Informasi adalah usaha melindungi sistem informasi agar terpelihara integritas (*integraty*), ketersediaaan (*availability*), dan kerahasiannya atau kepercayaanya (*confidentiality*). Informasi yang bernilai adalah informasi yang dapat disajikan tepat pada waktunya, akurat, lengkap, dan konsisten. Sedangkan tujuan keamanan informasi adalah mengamankan sumber daya (*resources*) komputer seperti hardware, software, jaringan komunikasi, dan yang paling penting adalah dokumen (data/ informasi). Bentuk pengamanananya dapat berupa mencegah, mengendalikan, dan memulihkan atau mengembalikan sebuah sumberdaya dari berbagai bentuk ancaman dan kejahatan yang dapat terjadi pada sebuah sistem komputer.

Tujuan sistem keamanan informasi akan dapat tercapai jika dalam tahapan pengamanan memenuhi prinsip rekayasa keamanan teknologi informasi. Tujuan dari prinsip-prinsip rekayasa keamanan teknologi informasi (TI) adalah untuk memberikan gambaran tentang prinsip *system-level* keamanan yang akan menjadi pertimbangan dalam merancang, mengembangkan, dan mengoperasikan pada sistem informasi. Prinsip-prinsip tersebut akan digunakan oleh :

- User ketika megembangkan dan mengevaluasi kebutuhan fungsional, atau sistem informasi operasi dalam organisasi.
- *System Engineers* dan Arsitek yang merancang, mengimplementasikan, atau memodifikasi sistem informasi.
- Spesialis IT pada semua fase siklus hidup sistem (*system life-cycle*).
- Manajer program dan petugas keamanan sistem informasi. (*Program Managers and Information System Security Officers*-ISSO) untuk meyakinkan implementasi keamanan yang memadai pada semua fase *system life-cycle*.

PRINSIP KEAMANAN INFORMASI

Standar NIST dalam SP 800-27, Rev A yang ditulis oleh Gary Stoneburner, dkk, 2004 dengan judul *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)* telah menyajikan 33 prinsip tentang keamanan teknologi Informasi, yang dibagi kedalam 6 kelompok sebagai berikut :

1. Landasan Keamanan :

- Prinsip ke-1. Yaitu penetapan kebijakan ukuran keamanan sebagai "pondasi" dalam perancangan.
- Prinsip ke-2. Ancaman keamanan merupakan bagian integral dari rancangan sistem secara keseluruhan.
- Prinsip ke-3. Menggambarkan secara jelas tentang penentuan batasan keamanan fisik dan logic oleh asosiasi pembuat kebijakan keamanan.
- Prinsip ke-4. Adanya jaminan pengembang tentang adanya pelatihan bagaimana mengembangkan keamanan software.

2. Pokok Keamanan

- Prinsip ke-5. Mengurangi resiko hingga level yang tepat.
- Prinsip ke-6. Mengasumsikan bahwa sistem eksternal adalah tidak aman (*insecure*). Eksternal diartikan sebagai sistem yang diluar tanggung jawab kendali.
- Prinsip ke-7. Mengidentifikasi potensi *trade-offs* antara biaya yang diperlukan untuk mengurangi resiko keamanan dengan nilai atau biaya yang sistem diamankan (*operational effectiveness*).
- Prinsip ke-8. Menerapkan penyesuaian ukuran sistem kemananan untuk memenuhi tujuan keamanan organisasi
- Prinsip ke-9. Memproteksi informasi selama dilakukan pemrosesan, dalam perjalanan, dan penyimpanan.
- Prinsip ke-10. Biasa mempertimbangkan hasil yang mencapai keamanan yang memadai.
- Prinsip ke-11. Melindungi dengan cara melawan semua yang tergolong dalam "attacks".

3. Mudah Digunakan

- Prinsip ke-12. Dimanapun juga, dasar keamanan adalah standar terbuka untuk protabilitas dan interoprabilitas.
- Prinsip ke-13. Menggunakan bahasa yang umum dalam kebutuhan pengembangan keamanan.
- Prinsip ke-14. Model Keamanan dapat memberikan adopsi terhadap teknologi yang baru, termasuk proses upgrade teknologi dan pengamanan.
- Prinsip ke-15. Berusaha memudahkan operasi pemakaian.

4. Nyaman dan Menyenangkan

- Prinsip ke-16. Diterapkan pada lapis keamanan (sehingga tidak ada celah untuk menyerang)
- Prinsip ke-17. Dirancang dan dioperasikan sebagai sistem TI untuk membatasi kerusakan dan menjadi respon yang menyenangkan.
- Prinsip ke-18. Memberikan jaminan terhadap sistem, secara terus menerus, sehingga terhidar dari serangan.
- Prinsip ke-19. Membatasi atau terkena serangan.
- Prinsip ke-20. Mengisolasi sistem akses public dari sumberdaya tugas yang penting (seperti data, pemrosesan, dan sebagainya).
- Prinsip ke-21. Menggunakan mekanisme pembatasan untuk memisahkan sistem komputer dan infrastruktur jaringan.
- Prinsip ke-22. Mekanisme audit desain dan implementasi untuk mendeteksi penggunaan yang tidak berhak (*anauthorized*) dan untuk mendukung investigasi insiden. (monitoring jaringan keamanan).
- Prinsip ke-23. Pengembangan dan pelatihan kemungkinan atau prosedur recovery kejadian infeksi sehingga dapat tersedia kembali dengan tepat.

5. Mengurangi Ancaman Serangan (*Reduce vulnerabilities*)

- Prinsip ke-24. Mengusahakan tetap sederhana.
- Prinsip ke-25. Memperkecil elemen-elemen sistem yang dapat dipercaya.
- Prinsip ke-26. Menerapkan batasan hak akses (*least privilege*). Ini dapat diartikan menerapkan pembagian tugas yang tepat dan terbatas.
- Prinsip ke-27. Tidak menerapkan mekanisme keamanan yang tidak perlu.
- Prinsip ke-28. Meyakinkan keamanan yang tepat ketika *shutdown* atau ketika mengakhiri sistem.
- Prinsip ke-29. Mengidentifikasi dan mencegah kesalahan yang umum dan yang mudah terserang (*vulnerabilities*).

6. Merancang dan menjaga Jaringan

- Prinsip ke-30. Mengimplementasikan keamanan sampai pada kombinasi distribusi secara fisik dan logical.
- Prinsip ke-31. Mengukur formulasi keamanan pada *address multiple overlapping information domains*.
- Prinsip ke-32. Mengotentikasi user dan pemrosesan untuk menjaminkeputusan pengendalian akses domainnya.
- Prinsip ke-33. Menggunakan identitas yang unik untuk menjamin akuntabilitas.

Prinsip Desain Pengamanan

Prinsip Desain pengamanan komputer perlu dilakukan karena ancaman-ancaman keamanan data atau informasi begitu sangat membahayakan. Berbagai tindakan penyerangan terhadap suatu sistem komputer seringkali membuat para administrator kewalahan dan kehabisan akal untuk mendesain suatu sistem yang lebih aman (*secure*). Untuk itu perlu diterapkan prinsip-prinsip yang tepat agar bisa mengantisipasi dan menghindari adanya ancaman. Prinsip-prinsip tersebut adalah:

a. Least Privilege. Prinsip ini menyatakan bahwa setiap proses yang dilakukan user suatu sistem komputer harus beroperasi pada level terendah yang diperlukan untuk menyelesaikan tugasnya. Dengan kata lain setiap proses hanya memiliki hak akses yang memang benar-benar dibutuhkan. Hak akses harus secara eksplisit diminta, ketimbang secara default diberikan. Tindakan seperti ini dilakukan untuk mengantisipasi kerusakan yang dapat ditimbulkan oleh suatu penyerangan.

b. Economy of Mechanisms. Prinsip ini menyatakan bahwa mekanisme sekuriti dari suatu sistem harus ekonomis dan sederhana sehingga dapat diverifikasi dan diimplementasi dengan benar. Mekanisme tersebut harus merupakan bagian yang tak terpisahkan dari desain sistem secara keseluruhan.

c. Complete Mediation. Prinsip ini menyatakan bahwa setiap akses ke sistem komputer harus dicek ke dalam informasi kontrol akses untuk otorisasi yang tepat. Hal ini juga berlaku untuk kondisi-kondisi khusus seperti pada saat *recovery* atau pemeliharaan.

d. Open Design. Prinsip ini menyatakan bahwa mekanisme sekuriti dari suatu sistem harus dapat diinformasikan dengan baik sehingga memungkinkan adanya umpan balik yang dapat dimanfaatkan untuk perbaikan sistem keamanan. Selain itu desain sistem harus bersifat terbuka, artinya jika memiliki kode sumber (*source code*) maka kode tersebut harus dibuka, dengan maksud untuk meminimalkan kemungkinan adanya lubang (*hole*) keamanan dalam sistem.

e. Separation of Priviledge. Prinsip ini menyatakan bahwa untuk mengakses suatu informasi tertentu seorang user harus memenuhi beberapa persyaratan tertentu. Hal ini dapat implementasikan dengan menerapkan sistem akses bertingkat, di mana user dibagi dalam beberapa tingkatan dan mempunyai hak akses yang berbeda.

f. Least Common Mechanism. Prinsip ini menyatakan bahwa antar user harus terpisah dalam sistem. Hal ini juga dapat diimplementasikan dengan sistem akses bertingkat.

g. ***Psychological Acceptability.*** Prinsip ini menyatakan bahwa mekanisme pengendalian sistem sekuriti harus mudah digunakan oleh user. Hal ini dapat dilakukan dengan mengadakan survei mengenai perilaku user yang akan menggunakan sistem.

h. ***Defense in Depth***. yaitu menggunakan berbagai perangkat keamanan untuk saling membackup. Misalnya dapat dipergunakan multiple screening router, mirroring harddisk pada server, dua CDRW untuk satu kali backup data yaitu dua kali sehari (setiap pagi dan sore) pada masing-masing departemen sehingga kalau satu dijebol, maka yang satu lagi masih berfungsi.

i. ***Choke point.*** Sistem yang dibangun semuanya harus keluar masuk lewat satu (atau sedikit) gerbang. Syaratnya tidak ada cara lain keluar masuk selain lewat gerbang.

j. ***Fail-Safe Stance***. maksudnya kalau suatu perangkat keamanan rusak, maka secara default perangkat tersebut settingnya akan ke setting yang paling aman. Misalnya: kapal selam di Karibia kalau rusak mengapung, kunci elektronik kalau tidak ada power akan unlock, packet filtering kalau rusak akan mencegah semua paket keluar-masuk. Bila packet filtering pada firewall modem router ADSL rusak maka semua paket keluar-masuk akan dicegah.

k. ***Universal participation***. semua orang dalam organisasi harus terlibat dalam proses sekuriti. Setiap tiga bulan sekali dilakukan pelatihan untuk menyegarkan kembali ingatan akan pentingnya mengamankan perangkat keamanan komputer. Didalamnya dilakukan evaluasi untuk peningkatan efisiensi kinerja proses keamanan komputer.

l. ***Diversity of Defense***. mempergunakan beberapa jenis sistem yang berbeda untuk pertahanan. Maksudnya, kalau penyerang sudah menyerang suatu jenis sistem pertahanan, maka dia tetap akan perlu belajar sistem jenis lainnya.

m. ***Simplicity***. jangan terlalu kompleks, karena sulit sekali mengetahui salahnya ada di mana kalau sistem terlalu kompleks untuk dipahami. Untuk mempermudah mengetahui bila terjadi kesalahan maka setiap data yang disimpan dalam server akan teridentifikasi siapa yang menyimpan berdasarkan user name dan passwordnya, kapan tanggal dan waktunya, dari workstation yang mana, dan apa aksi yang dilakukan. Bila user tidak mempunyai hak untuk menambah dan mengubah data pada sistem aplikasi tertentu tersebut maka akan ada trigger yang memberitahu bahwa sistem menolak adanya perubahan data.

SIKLUS HIDUP SISTEM KEAMANAN INFORMASI

Sesuai dengan *National Institute of Standards and Technology* (NIST) Special Publication 800-14, "*Generally Accepted Principles and Practices for Securing Information Technology Systems*,". Siklus hidup pengembangan sistem (*system development life cycle* /SDLC) pada keamanan komputer adalah tahap-tahap atau fase yang harus dilalui pada pengembangan keamanan computer melalui proses siklus hidup. Fase atau tahap-tahap yang digunakan dalam prinsip dan praktek untuk sistem keamanan teknologi informasi adalah sebagai berikut :

1. **Inisiasi** (*initiation*). Merupakan fase awal yang dibutuhkan untuk menetapkan tujuan sistem seperti dokumentasi.
2. **Pengambangan dan akuisisi** (*development/acquisition*). Pada fase ini sistem dirancang, dibeli, diprogram, dikembangkan, atau dikonstruksikan.
3. **Implementasi** (*Implementation*). Merupakan fase dimana sistem ditest dan diinstall. Aktifitasnya termasuk menginstalasi dan mengendalikan, test keamanan, sertifikasi, dan akreditasi.
4. **Operasi dan Pemeliharaan** (*Operation/Maintenance*). Pada fase ini dimana sistem bekerja atau dijalankan. Sistem juga dilakukan modifikasi jika terjadi penambahan software atau hardware, dan memberikan identifikasi. Aktifitas lain yang dilakukan pada tahap ini adalah jaminan

operasional dan adminsitrasi, auditing dan minitoring.

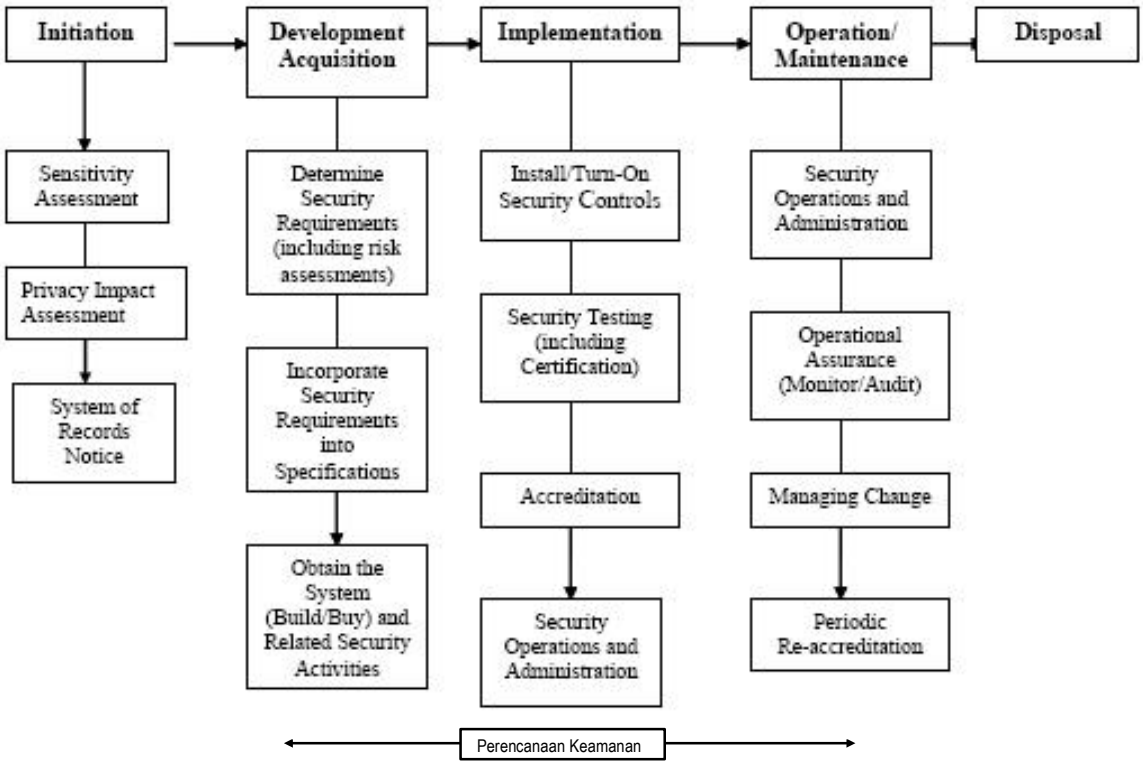
5. **Penyelesaian dan Pembuangan**(*disposal*). Fase ini merupakan bagian dari fase *life-cycle* yang melakukan disposisi pada informasi, hardware dan software. Aktifitas lain termasuk diantaranya adalah memindah (*moving*), mengarsipkan (*archiving*), menyingkirkan (*discarding*), atau memusnahkan (*destroying*) informasi dan sanitasi media.

Gambar dibawah ini merupakan tahapan (*fase*) dari siklus hidup (*life-cycle*) sistem keamanan computer.

a. Inisiasi

Inisiasi merupakan tahap awal sebuah proses keamanan, yang idealnya diimplementasikan dan diintegrasikan bersamaan ketika melakukan instalasi software sistem informasi. Namun pada kenyataanya bahwa proses keamanan dilakukan setelah sistem berjalan. Hal-hal yang dilakukan pada fase inisiasi yaitu :

- Definisi Konseptual. Yaitu memahami ruang lingkup (*boundary*) dari tanggung jawab sistem keamanan yang harus dilakukan.
- Penentuan Kebutuhan Fungsional. Yaitu melakukan spesifikasi detail dari tujuan ke target yang spesifik, seperti melakukan interview, review eksternal, analisis kesenjangan (*gap*) atau resiko.
- Pengembangan Spesifikasi Proteksi. Yaitu menciptakan sebuah desain terperinci dari sistem keamanan yang akan diterapkan, dimulai dengan sebuah model sistem umum yang sesuai dengan tujuan. Kemudian mencari teknologi tertentu yang sesuai, konfigurasi, prosedur, dan perubahan untuk memenuhi target. Hal-hal yang dilakukan adalah rangkuman eksekutif, metodologi pemilihan, alternative, dan membuat rekomendasi.
- Review desain. Merupakan tindakan untuk mempresentasikan desain dan implikasinya kepada para pengambil keputusan.



Gambar 1. Siklus Hidup Sistem Keamanan Komputer (Sumber NIST Pub:800-12)

b. Pengembangan dan Akuisisi

Pada fase ini dilakukan pembelian sehingga perlu dirancang tool termasuk prototype dan sistem tes untuk melakukan verifikasi bahwa konfigurasi berfungsi dengan benar sesuai dengan harapan. Tindakan yang dilakukan berupa :

- Review Komponen dan Code. Yaitu melakukan evaluasi dalam lingkungan laboratorium dan prototype. Langkah-langkah review yang dapat dilakukan adalah :
  - Fungsionalitas Komponen. Yaitu melakukan verifikasi, bahwa teknologi sekuriti yang dipilih adalah benar-benar berfungsi sesuai dengan harapan.
  - Konfigurasi Komponen. Menguji konfigurasi berjalan sesuai dengan yang direncanakan.
  - Pemeliharaan Komponen. Menetapkan prosedur yang dapat dijalankan dan metode untuk pemeliharaan, updating, dan melakukan troubleshooting terhadap komponen.
  - Review terhadap code. Yaitu tindakan akhir untuk mengeksplorasi bagian yang sensitive dan kritis dari code program untuk mencari *bug* atau masalah desain program yang fundamental.
- Review Pengujian Sistem. Yaitu membuat prototype dan melakukan review terhadap tool dan teknologi, serta membuat prototype yang mewakili seluruh sistem. Hal ini akan membantu dalam :
  - Fungsionalitas sistem. Langkah ini dapat mengungkapkan efek samping negatif yang sulit diprediksi sebelumnya, karena mencampurkan sebuah range teknologi dan konfigurasi yang bervariasi dari procedure yang ditetapkan sebelumnya.
  - Konfigurasi Sistem. Hal ini dapat dilakukan dengan merubah konfigurasi yang disusun sebelumnya, sehingga dapat menemukan masalah dan kelemahan yang tersembunyi.
  - Pemeliharaan Sistem. Yaitu melakukan pemeliharaan yang terencana, *upgradeing*, dan troubleshooting.
  - Training Sistem. Yaitu melakukan pelatihan terhadap semua user yang menerapkan sistem keamanan yang serupa agar tindakan pengamanan computer dapat dilakukan pada semua lini.
  - Implementasi Sistem. Yaitu menerapkan sistem secara sesunguhnya dan serentak, serta mempelajari kendala yang didapat selama implementasi.
- Sertifikasi. Ini dilakukan ketika memverifikasi terhadap desain prototype telah berhasil, dan selanjutnya dapat dinyatakan layak untuk dapat melakukan tindakan yang utama yaitu implementasi.

c. Implementasi

Merupakan fase penting dan utama dalam memperoleh tujuan keamanan computer. Implementasi dilakukan oleh Adminsitrator, user atau tim yang menyandang 'sertifikasi' (yang memperoleh kepercayaan) untuk melakukan penerapan keamanan pada komputernya sampai dengan melakukan tugas-tugas pengamanan dan pemantauan terhadap operasi keamanan yang berjalan. Implementasi dapat dilakukan dari mulai melakukan instalasi, melakukan pengetesan terhadap kemampuan operasi keamanan, sekaligus menerapkan administrasi operasinya. Fase implementasi, pada saat ini juga melakukan tindakan terhadap akreditasi terhadap sistem keamanan yang dibangun.

Akreditasi untuk menunjukkan kemampuan, keandalan, dan jaminan (*assurance*) terhadap keamanan sistem. Akreditasi akan meyakinkan pada semua

pengguna baik pada internal organisasi, terutama pada eksternal organisasi bahwa mereka akan merasa yakin atas sistem keamanan yang diterapkan pada organisasi tersebut, sehingga akan memberikan kepercayaan konsumen dalam melaksanakan transaksi bisnis yang memanfaatkan sistem keamanan computer. Contoh saja sistem perbankan yang memanfaatkan transaksi keuangan secara *on-line*, konsumen akan merasa aman dan nyaman dalam memanfaatkan teknologi computer *on-line* tersebut jika terdapat jaminan atau asuransi terhadap sistem keamanan bank tersebut. Akreditasi juga akan membantu meyakinkan kepada para pemegang saham misalnya untuk menanamkan modalnya.

Sudah barang tentu bahwa akreditasi yang objektif harus dilakukan dan dikeluarkan oleh organiasasi atau perusahaan lain yang independent yang memiliki kemampuan dan memenuhi sertifikat sebagai akredator.

d. Operasi dan Pemeliharan

Fase operasi merupakan fase untuk melakukan operasi rutin terhadap keberlangsungan sistem keamanan yang telah diimplementasikan. Pekerjaan operasi seperti memantau (monitoring) merupakan pekerjaan rutin yang harus dilakukan termasuk *updateing*, pemeliharaan, auditing, dan *scanning,* dan *backup*. Operasi juga melakukan tindakan untuk mempertahankan dan memulihkan sistem dari segala ancaman keamanan. Tindakan-tindakan yang dilakukan akan lebih banyak berupa pekerjaan adminsitrasi.

e. Penyelesaian dan Pembuangan

Fase ini merupakan langkah akhir (penyelesaian) yang harus dilakukan dari tindakan-tindakan fase sebelumnya dari siklus hidup sistem keamanan komputer. Bukan berarti bahwa dengan melakukan langkah ini telah menyelesaikan segala sesuatunya terhadap sistem keamanan computer. Jika permasalahan-permasalahan timbul sewaktu-waktu, maka tindakan yang perlu dilakukan harus sesuai dengan kejadian yang timbul dan penanganannya sesuai dengan fase siklus hidup diatas.

Fase Pembuangan, merupakan langkah yang harus dilakukan ketika menghadapi situasi yang mengharuskan memilih apakah yang digunakan adalah sistem yang baru atau sistem yang lama. Belum tentu bahwa sistem yang baru merupakan sistem yang lebih baik dari sistem yang sudah ada dan selama ini digunakan.

Jika sebuah pilihan telah dibuat dalam fase ini maka tindakan yang dapat dilakukan adalah memindah sistem jika perlu yang baru, memindahkan backup atau data ke media seperti CD misalnya, memisahkan dokumen yang perlu dipisahkan atau mengarsipkan tersendiri, seperti dokumen yang pernah terkena serangan virus perlu dipisah untuk dilakukan monitoring, serta memusnahkan virus itu sendiri dari sistem.

KESIMPULAN

Tujuan sistem keamanan informasi akan dapat tercapai jika dalam tahapan pengamanan memenuhi prinsip rekayasa keamanan teknologi informasi. Tujuan dari prinsip-prinsip rekayasa keamanan teknologi informasi (TI) adalah untuk memberikan gambaran tentang prinsip *system-level* keamanan yang akan menjadi pertimbangan dalam merancang, mengembangkan, dan mengoperasikan pada sistem informasi.

Prinsip keamanan informasi akan digunakan sebagai acuan dalam mengembangkan sistem keamanan dalam sebuah organisasi oleh para user, rekayasa sistem, spesialis IT, manajer program dan petugas keamanan sistem informasi. Prinsip tersebut memiliki 6 kelompok yaitu sebagai landasan keamanan, pokok keamanan, mudah digunakan, nyaman dan menyenangkan, dapat mengurangi ancaman serangan, serta digunakan untuk merancang dan menjaga keamanan.

Selanjutnya dari prinsip yang telah ditentukan akan digunakan untuk landasan dalam pengembangan siklus hidup informasi yang meliputi tahapan inisiasi, pengembangan dan akuisisi, implementasi, operasi dan pemliharaan, penyelesaian dan pembuangan.

DAFTAR PUSTAKA

1. Gary Stoneburner, dkk, 2004, "*Computer Security:Engineering Principles For Information Technology Security (Baseline for Achieving Security), Revisian A*", NIST.
2. http://bebas.vlsm.org/v06/Kuliah/MTI-Keamanan-Sistem-Informasi/2005/128/128M-05-final1.0-security-architecture-model.pdf
3. http://www.securitytechnet.com/crypto/standard/fips.html
4. http://www.wikipedia.org
5. NIST Special Pub. 800-86:, 2005, "Guide to Computer and Network Data Analysis: Applying Forensic Techniques to Incident Response (Draft) ", http://csrc.nist.gov/publications/drafts/Draft-SP800-86.pdf.