ANALISA RESIKO PENGELOLAAN JARINGAN KOMPUTER

Dedi Koswara

Sekolah Tinggi Manajemen Informatika dan Komputer LIKMI
Jl. Ir. H. Juanda 96 Bandung 40132

Abstract

Semakin berkembangnya implementasi teknologi informasi dalam suatu organisasi selain memberikan kemudahan juga menimbulkan resiko bagi organisasi itu sendiri. Setiap organisasi sebaiknya menyiapkan diri terhadap segala macam resiko yang mungkin timbul berkaitan dengan implementasi TI. Jaringan komputer dalam organisasi adalah salah satu contoh implementasi TI dalam organisasi yang memiliki resiko yang dominan.
Sebagai upaya awal setiap organisasi sebaiknya melakukan analisa resiko dalam pengelolaan jaringan komputer di lingkungannya. Dalam analisa ini diidentfikasi aset-aset yang dimiliki organisasi, serta ancaman-ancaman yang mungkin timbul dalam organisasi tersebut berkaitan dengan penggunaan jaringan komputer. Dari informasi aset dan ancaman, manajemen dalam organisasi dapat melakukan tindakan-tindakan perlindungan terhadap aset teknologi informasi yang dia miliki.

Key Word : resiko, jaringan komputer, aset, ancaman

Pengantar

Implementasi teknologi informasi terutama penggunaan jaringan komputer baik berkabel maupun nirkabel dalam organisasi sampai awal abad ke-21 sekarang ini sudah memiliki populasi yang cukup besar. Peningkatan jumlah jaringan/ kumpulan host yang terhubung dalam jaringan internet menunjukkan angka yang fantastis terutama sejak dekade terakhir abad ke-20. Seiring dengan meluasnya penggunaan jaringan komputer di berbagai organisasi, maka semakin meningkat pula insiden baik yang disengaja (oleh pihak internal atau eksternal organisasi) maupun insiden yang tidak disengaja (misalnya karena bencana alam). Setiap insiden tentu saja mengakibatkan kerugian yang bisa saja fatal, sehingga sangat perlu antisipasi terjadinya insiden dalam implementasi teknologi jaringan komputer dalam suatu organisasi. Makalah ini membahas tentang bagaimana melakukan analisa resiko yang dapat dilakukan oleh suatu organisasi yang mengimplementasikan teknologi jaringan komputer.

Masalah-Masalah Penting

Analisa resiko adalah langkah pertama dalam memperbaiki kesiapan organisasi terhadap insiden-insiden yang mungkin dihadapinya. Agar organisasi menjadi siap maka perlu dilakukan juga hal-hal berikut :

1. Organisasi harus menentukan kebijakan-kebijakan penggunaan aset-aset teknologi informasi di dalamnya secara benar dan teratur. Kebijakan-kebijakan tersebut didokumentasikan dalam bentuk standar prosedur, mulai standar prosedur operasional pekerjaan sehari-hari sampai dengan standar prosedur penanganan insiden.
2. Kebijakan dan standar-standar yang didefinisikan ada baiknya mengacu pada standar baku di negara yang bersangkutan atau bila perlu mengacu pada standar yang berlaku di negara-negara maju.
3. Organisasi harus melakukan sosialisasi tentang pentingnya menjaga dan memelihara aset-aset teknologi informasi dalam organisasi. Hal ini penting terutama bagi organisasi/ perusahaan yang menggantungkan hidupnya dari aset-aset teknologi informasi yang dimilikinya.

Tahapan Analisa Resiko

Berikut pedoman umum untuk melakukan analisa resiko :

1. Tentukan ruang lingkup lingkungan yang dianalisis resikonya.

   Contohnya suatu divisi dalam perusahaan (divisi pemasaran, divisi keuangan). Sebaiknya sesuai dengan ruang lingkup sistem informasi berbasis komputer dan konfiturasi jaringan komputer. Ruang lingkup terkecil direkomendasikan sebesar subnet/ subjaringan yang terdapat dalam organisasi.
2. Tentukan dasar (baseline) untuk melakukan penilaian aset dan ancaman. Dasar penentuan nilai aset dan ancaman berguna sebagai tolok ukur terutama dalam lingkungan yang sangat dinamis.
3. Identifikasi aset-aset teknologi informasi yang ada dalam organisasi, serta lakukan pembobotan terhadap nilai aset-aset tersebut, untuk mengetahui seberapa pentingnya aset tersebut bagi organisasi/ perusahaan. Pembobotan dapat dilakukan secara kualitatif maupun kuantitatif.

   Pembobotan kuantitatif dapat diukur dengan nilai uang yang diinvestasikan untuk aset tersebut, atau besar uang yang harus dikeluarkan organisasi untuk mengganti/ memperbaiki jika aset tersebut mengalami kerusakan/ hilang.

Pembobotan kualitatif dapat dilakukan dengan angka 1 sampai dengan 3. Angka 1 diberikan bagi aset yang kurang penting bagi organisasi, angka 2 untuk aset yang cukup penting, dan angka 3 bagi aset yang sangat penting.

Aspek yang dapat ditinjau dalam pembobotan aset antara lain kerahasiaan (*confidentiality*), integritas (*integrity*) dan ketersediaan (*avaliability*).

Aspek kerahasiaan digunakan dalam konteks sensitivitas terhadap pengungkapan data. Dalam aspek kerahasiaan, RCMP Guide menggolongkan aset menjadi *unclassified*, *designated*, *confidential*, *secret* dan *top secret*.

Aspek integritas digunakan dalam konteks ketelitian dan kelengkapan dari informasi yang dapat diakses dalam sistem dan oleh sistem itu sendiri. Jadi harus diperhatikan bagaimana akibat dari data yang tidak akurat, serta akibat dari data yang tidak lengkap.

Aspek ketersediaan, maksudnya adalah sistem yang dapat digunakan adalah sistem yang ada dan dapat digunakan sesuai kegunaannya. Harus dicatat aset-aset dan layanan-layanan yang *mission critical*, yaitu layanan-layanan yang penting untuk selalu tersedia bagi kelangsungan sistem dalam organisasi. Apa saja akibat dari hilangnya ketersediaan serta berapa toleransi *downtime* bagi organisasi.

Hasil dari tahap ini adalah matriks/ tabel aset yang dimiliki organisasi serta bobot aset tersebut bagi organisasi.

4. Identifikasi insiden-insiden/ ancaman-ancaman yang mungkin terjadi terhadap aset-aset teknologi informasi yang dimiliki organisasi, tentukan berapa besar kemungkinan terjadinya, serta tentukan tingkat kerusakan/ kerugian yang mungkin harus ditanggung organisasi jika insiden tersebut terjadi. Uraikan aset-aset mana saja yang terpengaruh oleh ancaman-ancaman tersebut. Kelompokkan ancaman-ancaman tersebut menjadi ancaman yang akibatnya dapat ditoleransi oleh organisasi, dan yang akibatnya tidak dapat ditoleransi oleh organisasi.

   Contoh kelompok ancaman antara lain pengungkapan, interupsi, modifikasi, perusakan, dan penghilangan/ penghapusan. Sedangkan tingkat kemungkinan terjadinya ancaman dapat digolongkan menjadi tidak mungkin terjadi/ *not applicable*, rendah/ *low*, menengah/ *medium*, dan *high*/ tinggi.

Hasil dari tahap ini adalah matriks ancaman, seperti berikut ini :

ASET	PENILAIAN ANCAMAN					
	AGEN/ EVENT	**KEL. ANCAMAN**	**KEMUNGKINAN TERJADI**	**AKIBAT**	**KERUSAKAN**	**TINGKAT PENGUNGKAPAN**
Uraikan aset-aset dalam organisasi	Ungkapkan kejadian yang menjadi ancaman	Disclosure Interruption Modification Destruction Removal	Low Medium High	Uraikan konsekuensi yg harus ditanggung organisasi	Exceptionally grave, serious, less serious	Nilai 1 sd 9

5. Uraikan upaya-upaya yang telah dilakukan organisasi untuk menghadapi ancaman-ancaman tersebut. Sesuaikan kembali matriks dari tahap sebelumnya dengan upaya-upaya yang telah dilakukan organisasi. Misalnya kemungkinkan terjadi nilainya bisa menurun karena telah menggunakan hardware atau software khusus untuk ancaman tersebut.
6. Berdasarkan data aset dan ancaman di atas tentukan ukuran resikonya, dan berapa besar toleransi organisasi terhadap besar resiko yang dapat terjadi. Penilaian resiko penting untuk menilai sejauh mana tingkat kesiapan organisasi terhadap ancaman-ancaman yang mungkin muncul. Suatu organisasi mencapai keseimbangan jika upaya-upaya perlindungan seimbang dengan ancaman-ancaman yang mungkin timbul. Tetapi mungkin saja organisasi terlalu berlebihan melakukan upaya perlindungan terhadap sistem jika dibandingkan dengan ancaman terhadapnya. Mungkin juga organisasi belum memiliki upaya yang memadai untuk menghadapi ancaman terhadapnya. Hasil dari penilaian resiko ini adalah organisasi mengetahui di posisi mana dia berada, apakah ada dalam posisi keseimbangan, berlebihan, atau rapuh terhadap ancaman. Dari posisi yang berhasil dianalisa, maka organisasi harus melakukan upaya-upaya ke arah keseimbangan.

   Tabel berikut dapat membantu untuk mengetahui sejauh mana resiko yang ditanggung oleh organisasi.

ASET	ANCAMAN	PENILAIAN ANCAMAN		
		PERLINDUNGAN YG TERSEDIA	**KELEMAHAN**	**RESIKO**
Uraikan aset-aset	Uraikan ancaman-ancaman	Uraikan upaya perlindungan yg telah tersedia	Uraikan kelemahan/ kekurangan yang dapat diamati	Tentukan nilai/ tingkat resiko

7. Untuk setiap ancaman yang mungkin terjadi, tentukan alternatif solusinya. Dari matriks ancaman yang dihasilkan tahap sebelumnya, organisasi harus melakukan upaya-upaya sistematis untuk melengkapi sistem perlindungan diri terhadap ancaman. Untuk setiap ancaman mungkin terdapat lebih dari satu alternatif solusi.

Uraikan alternatif solusi tersebutbeserta konsekuensi biaya yang harus ditanggung oleh organisasi. Hasil dari tahap ini adalah alternatif-alternatif solusi untuk diajukan ke pihak manajemen organisasi untuk dipilih. Pada waktu melakukan evaluasi solusi, harus diperhatikan target tingkat resiko yang dapat ditoleransi organisasi, sesuaikan upaya-upaya yang diajukan ke manajemen organisasi dengan target level resiko.

8. Selaraskan setiap pilihan solusi untuk dalam setiap penanganan ancaman, sehingga dapat diperoleh suatu kombinasi solusi untuk penanganan semua ancaman dan kelemahan sistem.
9. Implementasikan solusi dan ukur tingkat keberhasilannya. Hasil dari implementasi perlindungan sistem dapat saja sangat memuaskan, atau memadai untuk sebagian besar aspek ancaman, atau belum memadai/ perlu peningkatan intensif.

Penutup

Penilaian resiko implementasi sistem dalam organisasi menjadi penting peranannya bagi organisasi yang menggantungkan keberadaannya pada sistem yang dipakainya. Oleh karena itu upaya penilaian resiko, serta melakukan upaya sistematis adalah langkah awal yang baik bagi organisasi agar memiliki suatu sistem yang handal dan dapat diandalkan untuk menunjang kelangsungan organisasinya.