Soal Responsi tentang bab 4: Security dalam referensi “Student edition: IBM e-business...”

1. Aplikasi e-bisnis yang dijalankan dengan fokus pada otorisasi dan otentikasi merupakan suatu hal yang mendasar. Mengapa demikian?
2. Salah satu perhatian utama dalam penerapan solusi sistem keamanan dewasa ini adalah faktor kompleksitas dan biaya secara keseluruhan. Sebutkan faktor-faktor yang sering disebutkan sebagai penghambat dalam penerapan solusi sistem keamanan pada suatu organisasi atau perusahaan!
3. Seberapa jauh dan seperti apa tingkat keamanan yang sebaiknya diterapkan oleh organisasi atau perusahaan?
4. Dengan begitu kompleksnya sistem keamanan saat ini, maka diperlukan suatu kerangka solusi yang mencakup berbagai area utama dalam hal keamanan teknologi informasi sebagai bagian dari arsitektur secara keseluruhan. Sebutkan area-area tersebut!

Jawaban:

1. Faktor keamanan merupakan hal yang tidak dapat dipisahkan dari e-bisnis, jika ingin menjalankan e-bisnis maka sistem keamanannya juga harus dibuat dengan baik. Hal ini karena pengguna, pelanggan, dan perusahaan menginginkan data mereka tidak dapat dirusak atau disalahgunakan oleh orang yang tidak berhak. Untuk menjalankan e-bisnis kita harus membangun "rantai kepercayaan" dan membiarkan setiap orang mengetahuinya.

2. Faktor-faktor penghambat dalam penerapan sistem keamanan dalam suatu organisasi atau perusahaan:
   - Sistem keamanan terlalu kompleks
   - Kebijakan sistem keamanan menjadi suatu hal yang tidak mungkin untuk diterapkan saat ini
   - Total biaya penerapan sistem keamanan meningkat
   - Topik tentang keamanan menghentikan inisiatif e-bisnis

3. Seberapa banyak dan sejauh mana tingkat keamanan yang sebaiknya diterapkan oleh organisasi atau perusahaan didasarkan pada penilaian perusahaan tentang risiko yang harus dihadapi bila tidak mengimplementasikan sistem keamanan tertentu dibandingkan dengan manfaat yang diperoleh perusahaan jika menerapkannya. Keputusan perusahaan untuk menerapkan keamanan bagi aplikasi e-bisnis akan melibatkan serangkaian keputusan dan kebijakan. Sistem keamanan yang seperti apa dan bagaimana akan tergantung dari sifat aplikasi perusahaan dan nilai bisnis dari transaksi yang didukung aplikasi. Biasanya jumlah uang yang dihabiskan perusahaan untuk menerapkan teknologi untuk melindungi asetnya, ditambah dengan biaya pengelolaan dan pemeliharaan teknologi itu, harus kurang dari nilai aset perusahaan yang coba diamankan.

4. Area-area utama tersebut adalah:
   - Kebijakan keamanan yang komprehensif; ketepatan definisi, penanganan, dan implementasinya; dan pelaksanaannya yang dikendalikan secara terpusat
   - Mengamankan batasan berbagai layanan e-bisnis dengan cara mengamankan jaringan komputer dengan firewall, serta fungsi VPN, dan program-program untuk versi perangkat bergerak.
   - Sistem pendeteksi pembobolan sistem (IDS=Intrusion Detection Systems) dan sentralisasi IDS yang real time serta kekebalan terhadap virus dalam rangka mendeteksi dan bertahan terhadap ancaman potensial
   - PKI (Public Key Infrastructure) untuk mengenali dan menangani identitas pengguna secara aman
   - Berbagai Toolkit yang menyediakan seperangkat antarmuka pemrograman aplikasi (APIs=Application Programming Interfaces) untuk menambahkan kebutuhan terhadap spesifikasi keamanan khusus kedalam perangkat lunak