

Pengelolaan Kebijakan Keamanan Informasi



Kebijakan mengenai keamanan informasi (*IT security policy*) merupakan salah satu pilar utama dalam pengamanan sistem informasi. Kebijakan itu mengatur aset apa saja yang harus dilindungi. Sebagai contoh, kebijakan mengatur apa saja yang dapat dilakukan oleh seorang pengguna komputer di kantor (atau di sekolah). Misalnya kebijakan di kantor Anda tidak memperbolehkan Anda untuk memasang program sendiri tanpa izin dari unit tertentu. Kebijakan ini diambil untuk melindungi komputer dari virus, *trojan horse*, dan *spyware*.

Pembatasan akses ke situs tertentu di Internet juga merupakan sebuah contoh kebijakan. Kebijakan ini kemudian diimplementasikan secara teknis dengan menggunakan *firewall* atau *proxy* yang melakukan filtering terhadap situs tersebut. Tanpa ada kebijakan, akan sulit bagi pengelola *firewall* atau *proxy* untuk menentukan konfigurasi dari *firewall* atau *proxy* tersebut.

Akibat tidak adanya kebijakan, pengelola perangkat yang menerapkan filtering seperti di atas sering dimusuhi oleh pengguna, karena dianggap terlalu mengatur atau menyulitkan pengguna. Sayangnya, kebijakan keamanan informasi ini sering tidak ada karena kurang dianggap penting dan memang sukar dibuatnya.

Ada beberapa kegiatan yang terkait dengan pengelolaan kebijakan ini. Secara garis besar kegiatan tersebut adalah pengembangan (*development*), implementasi, dan perawatan. Masing-masing kegiatan ini memiliki subkegiatan yang lebih rinci. Tahap pengembangan kebijakan, misalnya, meliputi kegiatan pembuatan, *review*, dan persetujuan.

Proses pembuatan kebijakan sebaiknya melibatkan wakil-wakil dari *stakeholder* atau unit-unit yang ada di perusahaan. Pendekatan ini dilakukan agar ada rasa memiliki terhadap kebijakan tersebut. Sering kali pembuatan kebijakan keamanan informasi hanya dilakukan oleh divisi TI saja sehingga ada resistensi dalam penerimaannya. Selain itu, kebijakan umumnya terkait dengan proses bisnis perusahaan yang sering kali tidak dimengerti oleh orang TI secara rinci sehingga membutuhkan keterlibatan pihak lain.

Setelah kebijakan dibuat, dia harus mendapat persetujuan (*approval*) dari pucuk pimpinan agar bisa dieksekusi. Masalahnya,

untuk mendapatkan persetujuan ini tidak mudah. Apalagi jika kebijakan tersebut tidak dibuat secara bersama-sama. Proses untuk mendapat persetujuan ini dapat memakan waktu yang lama.


Setelah proses pengembangan selesai dengan adanya persetujuan, kebijakan keamanan tersebut harus diimplementasikan. Lagi-lagi implementasinya ternyata tidak mudah. Ada beberapa pertimbangan yang perlu diperhatikan, seperti kepatuhan terhadap regulasi yang spesifik terhadap industri dari perusahaan tersebut sehingga ada kemungkinan kebijakan perlu diubah. Sebagai contoh, industri Perbankan memiliki aturan "Basel II". Industri yang terkait dengan kesehatan di Amerika Serikat memiliki "HIPAA" (*Health Insurance Portability and Accountability Act*). Perusahaan terbuka yang tercatat dalam bursa saham harus patuh terhadap aturan tertentu, dan seterusnya.

Selain kepatuhan terhadap regulasi, ada juga pengecualian-pengecualian yang harus dilakukan. Kadang-kadang apa yang tertuang dalam kebijakan keamanan bertentangan dengan proses bisnis sehingga perlu dibuat pengecualian (*exception*). Ini menjadi bagian dalam proses implementasi.

Proses pengembangan dan implementasi telah selsai. Tiba saatnya kita melakukan penerapan. Langkah pertama yang dilakukan adalah

melakukan sosialisasi kepada semua pihak yang terkait dengan adanya kebijakan keamanan tersebut. Tanpa ada program sosialisasi, kebijakan hanya menjadi dokumen yang disimpan di rak (atau di sebuah direktori dalam sebuah server) dan tidak diketahui oleh pengguna.

Setelah itu semua dilakukan, ada kegiatan pemantauan. Kebijakan harus ditegakkan. Pelanggaran terhadap kebijakan harus mendapat hukuman atau sanksi. Jika pelanggaran dibiarkan, maka kebijakan menjadi tumpul dan semakin dilanggar. Banyak instansi yang tidak melakukan hal ini.

Jika kita perhatikan, pengelolaan kebijakan keamanan informasi tidak mudah. Itulah sebabnya dia sering tidak mendapat perhatian, meskipun dia merupakan komponen utama dalam pengamanan sistem informasi. Mudah-mudahan tulisan ini dapat membujuk Anda agar lebih patuh terhadap kebijakan keamanan informasi. 

Sayangnya, kebijakan keamanan informasi ini sering tidak ada karena kurang dianggap penting...