

MENYUSUN KEBIJAKAN KEAMANAN INFORMASI

Prof. Richardus Eko Indrajit

Pentingnya Dokumen Kebijakan Keamanan

Keberadaan dokumen “Kebijakan Keamanan” atau “Security Policies” merupakan sebuah infrastruktur keamanan yang harus dimiliki oleh sebuah organisasi atau perusahaan yang ingin melindungi aset informasi terpentingnya. Dokumen ini secara prinsip berisi berbagai cara (baca: kendali) yang perlu dilakukan untuk mengontrol manajemen, mekanisme, prosedur, dan tata cara dalam mengamankan informasi, baik secara langsung maupun tidak langsung. Karena berada pada tataran kebijakan, maka dokumen ini biasanya berisi hal-hal yang bersifat prinsip dan strategis. Dengan adanya kebijakan ini, selain akan membantu organisasi dalam mengamankan aset pentingnya, juga menghindari adanya insiden atau tuntutan hukum akibat organisasi terkait lalai dalam melakukan pengelolaan internal terhadap aset informasi atau hal-hal terkait dengan tata kelola informasi yang berada dalam lingkungannya. Kebijakan yang dimaksud juga bersifat teknologi netral, artinya tidak tergantung atau spesifik terhadap penggunaan merek teknologi tertentu.

Elemen Kunci Kebijakan Keamanan

EC-Council melihat ada 7 (tujuh) elemen kunci yang harus diperhatikan dalam menyusun kebijakan keamanan, masing-masing adalah:

1. Komunikasi yang jelas mengenai arti dan pentingnya sebuah kebijakan keamanan untuk disusun dan ditaati oleh seluruh pemangku kepentingan perusahaan;
2. Definisi yang jelas dan ringkas mengenai aset informasi apa saja yang harus diprioritaskan untuk dilindungi dan dikelola dengan sebaik-baiknya;
3. Penentuan ruang lingkup pemberlakuan kebijakan yang dimaksud dalam teritori kewenangan yang ada;
4. Jaminan adanya sanksi, perlindungan, dan penegakan hukum terhadap para pelaku yang terkait dengan manajemen informasi sesuai dengan peraturan dan undang-undang yang berlaku;
5. Adanya pembagian tugas dan tanggung jawab yang jelas terhadap personel atau SDM yang diberikan tugas untuk melakukan kegiatan pengamanan informasi;
6. Penyusunan dokumen atau referensi panduan bagi seluruh pemangku kepentingan dan pelaku manajemen keamanan informasi untuk menjamin penerapan yang efektif; dan

7. Partisipasi aktif dan intensif dari manajemen atau pimpinan puncak organisasi untuk mensosialisasikan dan mengawasi implementasi kebijakan dimaksud.

Peranan dan Tujuan Keberadaan Kebijakan Keamanan

Secara prinsip paling tidak ada 2 (dua) peranan penting dari sebuah dokumen kebijakan keamanan, yaitu:

- Untuk mendefinisikan dan memetakan secara detail aset-aset informasi apa saja yang harus dilindungi dan dikelola dengan baik keamanannya; dan
- Untuk mereduksi atau mengurangi resiko yang dapat ditimbulkan karena:
 - Adanya penyalahgunaan sumber daya atau fasilitas perusahaan yang terkait dengan manajemen pengelolaan data dan informasi;
 - Adanya insiden yang menyebabkan hilangnya data penting, tersebarnya informasi rahasia, dan pelanggaran terhadap hak cipta (HAKI); dan
 - Adanya pelanggaran terhadap hak akses pengguna informasi tertentu sesuai dengan hak dan wewenangnya.

Oleh karena itulah maka perlu didefinisikan dan ditentukan serangkaian mekanisme atau protokol yang berfungsi sebagai panduan strategis dan operasional dalam hal semacam: (i) bagaimana setiap karyawan harus dan dapat berinteraksi dengan sistem informasi; (ii) bagaimana setiap sistem informasi harus dikonfigurasi; (iii) apa yang harus dilakukan jika terjadi insiden keamanan; (iv) bagaimana cara mendeteksi adanya kerawanan keamanan sistem yang terjadi; dan lain sebagainya.

Sementara tujuan dari adanya Kebijakan Keamanan adalah:

- Memproteksi dan melindungi sumber daya sistem dan teknologi informasi organisasi dari penyalahgunaan wewenang akses;
- Menangkis serangan atau dakwaan hukum dari pihak lain terkait dengan insiden keamanan; dan
- Memastikan integritas dan keutuhan data yang bebas dari perubahan dan modifikasi pihak-pihak tak berwenang.

Klasifikasi Jenis Kebijakan Keamanan

Dilihat dari segi peruntukkan dan kontennya, dokumen kebijakan keamanan dapat dikategorisasikan menjadi beberapa jenis, yaitu:

1. User Policy – berisi berbagai kebijakan yang harus dipatuhi oleh seluruh pengguna komputer dan sistem informasi organisasi, terutama menyangkut masalah hak akses, proteksi keamanan, tanggung jawab pengelolaan aset teknologi, dan lain sebagainya;

2. IT Policy – diperuntukkan secara khusus bagi mereka yang bekerja di departemen atau divisi teknologi informasi untuk memastikan adanya dukungan penuh terhadap pelaksanaan tata kelola keamanan informasi, seperti: mekanisme back-up, tata cara konfigurasi teknologi, dukungan terhadap pengguna, manajemen help desk, penanganan insiden, dan lain sebagainya;
3. General Policy – membahas masalah-masalah umum yang menjadi tanggung jawab bersama seluruh pemangku kepentingan organisasi, misalnya dalam hal mengelola keamanan informasi pada saat terjadi: manajemen krisis, serangan penjahat cyber, bencana alam, kerusakan sistem, dan lain sebagainya; dan
4. Partner Policy – kebijakan yang secara khusus hanya diperuntukkan bagi level manajemen atau pimpinan puncak organisasi semata.

Panduan Rancangan dan Konten Dokumen Kebijakan Keamanan

Untuk setiap dokumen kebijakan keamanan yang disusun dan dikembangkan, terdapat sejumlah hal yang harus diperhatikan sebagai panduan, yaitu:

- Terdapat penjelasan detail mengenai deskripsi kebijakan yang dimaksud, terutama berkaitan dengan isu-isu keamanan informasi dalam organisasi;
- Adanya deskripsi mengenai status dokumen kebijakan yang disusun dan posisinya dalam tata peraturan organisasi dimaksud;
- Ruang lingkup pemberlakuan dokumen terkait dalam konteks struktur serta lingkungan organisasi yang dimaksud – terutama dalam hubungannya dengan unit serta fungsi struktur organisasi yang bersangkutan; dan
- Konsekuensi atau hukuman bagi mereka yang tidak taat atau melanggar kebijakan yang dimaksud.

Dipandang dari sisi konten, perlu disampaikan dalam dokumen kebijakan keamanan sejumlah aspek sebagai berikut:

- Pendahuluan mengenai alasan dibutuhkan suatu kebijakan keamanan dalam konteks berorganisasi, terutama dalam kaitannya dengan definisi, ruang lingkup, batasan, obyektif, serta seluk beluk keamanan informasi yang dimaksud;
- Pengantar mengenai posisi keberadaan dokumen kebijakan yang disusun, serta struktur pembahasannya, yang telah fokus pada proses pengamanan aset-aset penting organisasi yang terkait dengan pengelolaan data serta informasi penting dan berharga;
- Definisi mengenai peranan, tugas dan tanggung jawab, fungsi, serta cara penggunaan kebijakan keamanan yang dideskripsikan dalam dokumen formal terkait; dan

- Mekanisme kendali dan alokasi sumber daya organisasi yang diarahkan pada proses institutionalisasi kebijakan keamanan yang dipaparkan dalam setiap pasal atau ayat dalam dokumen kebijakan ini.

Strategi Implementasi Kebijakan Keamanan

Belajar dari pengalaman organisasi yang telah berhasil menerapkan dokumen kebijakan keamanan secara efektif, ada sejumlah prinsip yang harus dimengerti dan diterapkan secara sungguh-sungguh, yaitu:

1. Mekanisme pengenalan dan “enforcement” harus dilaksanakan dengan menggunakan pendekatan “top down”, yang dimulai dari komitmen penuh pimpinan puncak yang turun langsung mensosialisasikannya kepada segenap komponen organisasi;
2. Bahasa yang dipergunakan dalam dokumen kebijakan keamanan tersebut haruslah yang mudah dimengerti, dipahami, dan dilaksanakan oleh setiap pemangku kepentingan;
3. Sosialisasi mengenai pemahaman cara melaksanakan setiap pasal dalam kebijakan keamanan haruslah dilaksanakan ke segenap jajaran manajemen organisasi;
4. Tersedianya “help desk” yang selalu bersedia membantu seandainya ada individu atau unit yang mengalami permasalahan dalam menjalankan kebijakan yang ada; dan
5. Secara konsisten diberikannya sanksi dan hukuman terhadap setiap pelanggaran kebijakan yang terjadi, baik yang sifatnya sengaja maupun tidak sengaja.

Contoh Model Kebijakan Keamanan

Dipandang dari segi prinsip, paradigma, dan pendekatan dalam menyusun strategi keamanan, dokumen kebijakan yang disusun dapat dikategorikan menjadi sejumlah model, antara lain:

Primiscuous Policy

Merupakan kebijakan untuk tidak memberikan restriksi apa pun kepada para pengguna dalam memanfaatkan internet atau sistem informasi yang ada. Kebebasan yang mutlak ini biasanya sering diterapkan oleh organisasi semacam media atau pers, konsultan, firma hukum, dan lain sebagainya – yang menerapkan prinsip-prinsip kebebasan dalam berkarya dan berinovasi.

Permissive Policy

Pada intinya kebijakan ini juga memberikan keleluasaan kepada pengguna untuk memanfaatkan sistem informasi sebebaskan-bebasnya tanpa kendali, namun setelah dilakukan sejumlah aktivitas kontrol, seperti: (i) menutup lubang-lubang kerawanan dalam sistem dimaksud; (ii) menonaktifkan port atau antar muka input-output yang tidak dipergunakan; (iii) mengkonfigurasi server dan firewalls sedemikian rupa sehingga tidak dimungkinkan adanya akses dari eksternal organisasi ke dalam; dan lain sebagainya.

Prudent Policy

Kebalikan dengan dua model kebijakan sebelumnya, jenis ini organisasi benar-benar menggunakan prinsip kehati-hatian dalam mengelola keamanan informasinya. Dalam lingkungan ini, hampir seluruh sumber daya informasi “dikunci” dan “diamankan”. Untuk menggunakannya, setiap user harus melalui sejumlah aktivitas pengamanan terlebih dahulu. Prinsip ekstra hati-hati ini biasanya cocok untuk diterapkan pada organisasi semacam instalasi militer, bursa efek, perusahaan antariksa, dan lain sebagainya.

Paranoid Policy

Pada model ini, kebanyakan individu dalam organisasi yang tidak memiliki relevansi sama sekali dengan kebutuhan informasi benar-benar ditutup kemungkinannya untuk dapat mengakses internet maupun sistem informasi apapun yang ada dalam lingkungan organisasi. Seperti selayaknya orang yang sedang “paranoid”, organisasi benar-benar “tidak percaya” kepada siapapun, termasuk karyawannya sendiri, sehingga akses terhadap hampir semua sistem informasi benar-benar ditutup secara ketat.

Acceptable-Use Policy

Dalam lingkungan kebijakan ini, organisasi menentukan hal-hal apa saja yang boleh dilakukan maupun tidak boleh dilakukan oleh sejumlah pengguna dalam organisasi – terkait dengan akses dan hak modifikasi informasi tertentu. Hasil pemetaan inilah yang kan dipakai untuk memberikan tingkat atau level hak akses keamanannya.

User-Account Policy

Ini merupakan kebijakan yang paling banyak diterapkan di organisasi kebanyakan. Dalam konteks ini, setiap pengguna, sesuai dengan tupoksi dan tanggung jawabnya, ditetapkan hak aksesnya terhadap masing-masing jenis informasi yang ada di organisasi. Dengan kata lain, wewenang akses yang dimiliki tersebut melekat pada struktur atau unit organisasi tempatnya bekerja dan beraktivitas.

Remote-Access Policy

Kebijakan ini erat kaitannya dengan manajemen hak akses terhadap sumber daya sistem informasi organisasi yang dapat dikendalikan dari jarak jauh (baca: remote). Hal ini menjadi tren tersendiri mengingat semakin banyaknya organisasi yang memperbolehkan karyawannya untuk bekerja dari rumah atau ranah publik lainnya sejauh yang bersangkutan memiliki akses ke internet. Karena sifatnya inilah maka perlu dibuat kebijakan khusus mengenai hak akses kendali jarak jauh.

Information-Protection Policy

Jika dalam kebijakan sebelumnya fokus lebih ditekankan pada hak akses pengguna terhadap sumber daya teknologi yang ada, dalam kebijakan ini fokus kendali atau perlindungan ada pada aset informasi itu sendiri. Dimulai dari definisi informasi apa saja yang dianggap bernilai tinggi dan perlu diprioritaskan untuk dijaga, hingga model pencegahan penguasaan orang lain yang tidak berhak dengan cara melakukan enkripsi, perlindungan penyimpanan, model akses, dan lain sebagainya.

Firewall-Management Policy

Sesuai dengan namanya, kebijakan ini erat kaitannya dengan prinsip dan mekanisme konfigurasi firewalls yang harus diterapkan dalam organisasi. Karena sifatnya yang holistik, biasanya kebijakan ini menyangkut mulai dari perencanaan, pengadaan, pengkonfigurasian, penginstalan, pemasangan, penerapan, hingga pada tahap pengawasan dan pemantauan kinerja.

Special-Access Policy

Disamping kebijakan yang bersifat umum, dapat pula diperkenalkan kebijakan yang secara khusus mengatur hal-hal yang diluar kebiasaan atau bersifat ad-hoc (maupun non-rutin). Misalnya adalah hak akses terhadap sumber daya teknologi yang diberikan kepada penegak hukum ketika terjadi proses atau insiden kejahatan kriminal; atau wewenang akses terhadap pihak eksternal yang sedang melakukan aktivitas audit teknologi informasi; atau hak khusus bagi pemilik perusahaan atau pemegang saham mayoritas yang ingin melihat kinerja organisasi atau perusahaan yang dimilikinya.

Network-Connection Policy

Seperti diketahui bersama, terdapat banyak sekali cara untuk dapat menghubungkan sebuah komputer atau notebook ke jejaring komputer maupun dunia maya (baca: internet), antara lain melalui: (i) hot spot secara langsung; (ii) wireless dengan perantara komputer lain sebagai host; (iii) modem; (iv) telepon genggam; (v) sambungan fisik teritorial; dan lain sebagainya. Agar aman, perlu dikembangkan sebuah kebijakan keamanan terkait dengan aturan dan mekanisme kebijakan menghubungkan diri ke dunia maya.

Business-Partner Policy

Sebagai pihak yang berada di luar lingkungan internal perusahaan, mitra bisnis perlu pula diberikan akses terhadap sejumlah informasi yang relevan untuknya. Dalam kaitan ini maka perlu dikembangkan kebijakan keamanan khusus yang mengatur hak dan tanggung jawab akses informasi dari mitra bisnis.

Other Policies

Setiap organisasi memiliki karakteristik, budaya, dan kebutuhannya masing-masing. Oleh karena itu, maka akan berkembang sejumlah kebijakan sesuai dengan kebutuhan yang ada. Beberapa di antaranya yang kerap dikembangkan oleh organisasi di negara berkembang seperti Indonesia adalah:

- Kebijakan mengenai manajemen pengelolaan kata kunci atau password;
- Kebijakan dalam membeli dan menginstalasi software baru;
- Kebijakan untuk menghubungkan diri ke dunia maya (baca: internet);
- Kebijakan terkait dengan penggunaan flash disk dalam lingkungan organisasi;
- Kebijakan yang mengatur tata cara mengirimkan dan menerima email atau berpartisipasi dalam mailing list; dan lain sebagainya.