

BAB I

PENDAHULUAN

1.1 Latar belakang

Saat ini, kemajuan teknologi digital telah menjadi unsur krusial dalam menunjang aktivitas operasional pemerintahan, termasuk di lingkup pemerintah Kota Surabaya. Pemakaian teknologi tersebut tampak dalam pengelolaan sistem aplikasi dan infrastruktur jaringan yang berfungsi mendukung penyediaan layanan masyarakat. Dengan demikian, Dinas Komunikasi Dan Informatika Kota Surabaya memiliki peran strategis sebagai salah organisasi perangkat daerah (OPD) yang bertugas mengelola serta melakukan perbaikan sistem, sehingga kelancaran layanan aplikasi yang digunakan masyarakat dapat terus terjamin.

Namun, jaringan sistem di Kota Surabaya cukup beragam aplikasi salah satunya adalah aplikasi sayang warga yang beroperasi harus selalu dipantau secara berkala, maka pengelolaan keamanan informasi menjadi sangat penting untuk mencegah adanya celah yang bisa dimanfaatkan oleh serangan siber. Informasi sendiri dipandang sebagai aset berharga bagi Dinas Komunikasi Dan Informatika Kota Surabaya. Sama halnya dengan aset bisnis lainnya, data dan informasi juga wajib dilindungi dengan baik sesuai ketentuan regulasi yang berlaku. Oleh sebab itu, penerapan keamanan informasi ditujukan untuk melindungi data dari ancaman siber berskala luas, menjaga keberlangsungan sistem informasi, sekaligus mengurangi risiko yang dapat mengganggu proses bisnis serta mendukung optimalisasi layanan.[1]

Dalam menghadapi potensi ancaman serangan siber yang mungkin terjadi, langkah penting yang perlu dilakukan Dinas Komunikasi Dan Informatika Kota Surabaya adalah merumuskan kebijakan serta regulasi khusus terkait keamanan informasi, dengan mempertimbangkan risiko perlindungan data pribadi yang akan diterapkan pada aplikasi sayang warga. Selain itu, penilaian kesiapan yang komprehensif memungkinkan instansi untuk mengenali, mengkaji, dan menentukan prioritas potensi risiko yang berhubungan dengan aksi peretasan digital.[2]

Penelitian ini menggunakan index KAMI versi 5.0 sebagai instrumen utama dalam mengukur kesiapan keamanan informasi sekaligus sebagai pedoman menguji kesiapan aplikasi sayang warga terhadap ancaman dari luar. Instrumen tersebut menawarkan kerangka kerja terstruktur yang mendukung penerapan tata kelola risiko teknologi informasi. Lewat cara ini, lembaga lebih cepat mengidentifikasi, mengelola, serta meminimalkan ancaman terkait keamanan informasi, sehingga aset penting dapat terlindungi secara optimal. Selain itu, penerapan index KAMI versi 5.0 memberikan dasar yang kuat dalam pengujian kesiapan secara efektif dan efisien. Hal ini memungkinkan potensi masalah diantisipasi sejak dini sekaligus membangun sistem perlindungan jangka panjang untuk menjaga keamanan aset informasi secara berkelanjutan.[3]

Karena itu, penelitian ini akan fokus pada pemeriksaan seberapa siap keamanan informasi di Dinas Komunikasi Dan Informatika Kota Surabaya, dengan menggunakan index KAMI versi 5.0. Dari hasil melihat seberapa siap sistem keamanan yang ada saat ini berfungsi, penelitian ini bertujuan untuk menyarankan area mana yang perlu ditingkatkan. Selain itu, diharapkan hasil penelitian ini dapat menjadi panduan yang berguna bagi organisasi dan perusahaan lain dalam menghadapi ancaman siber dan beradaptasi dengan teknologi digital terkini.

1.2 Rumusan masalah

1.2.1 Permasalahan

Penelitian ini mengkaji kesiapan sistem IT Dinas Komunikasi Dan Informatika Kota Surabaya terhadap keamanan informasi, khususnya dalam hal perlindungan data pribadi. Sebagai OPD yang mengelola aplikasi serta jaringan di kota surabaya, perusahaan ini menyimpan banyak data sensitif pengguna seperti nama, alamat, nik, dan juga hal sensitif lainnya. Maka dari itu, mekanisme yang berlaku saat ini masih rawan mengalami pelanggaran maupun kebocoran informasi, baik karena faktor teknis seperti sistem keamanan yang belum memadai maupun faktor manusia seperti kesalahan prosedur. Jika terjadi kebocoran data, bukan hanya merugikan pengguna tapi juga bisa berdampak pada reputasi instansi dan kepercayaan masyarakat terhadap layanan kepada masyarakat. Dengan penelitian ini diharapkan memberikan hasil yang relevan untuk memperkuat sistem keamanan data guna melindungi informasi pengguna.

1.2.2 Manfaat penelitian

Penelitian ini menghadirkan kontribusi positif untuk Dinas Komunikasi Dan Informatika Kota Surabaya dalam mengukur tingkat kesiapan keamanan informasi serta menjadi dasar perbaikan sistem yang masih rentan terhadap ancaman. Dengan standar index KAMI versi 5.0, celah keamanan dapat teridentifikasi sehingga strategi menuju sertifikasi nasional dan kepatuhan regulasi perlindungan data dapat disusun. Selain itu, penelitian ini juga memberi kontribusi akademis sebagai studi kasus penerapan index KAMI di sektor komunikasi dan informatika serta memperkaya kajian tata kelola keamanan informasi.

1.2.3 Metode usulan

Penelitian ini merekomendasikan penerapan index KAMI versi 5.0, sebab pendekatan tersebut dibuat secara khusus untuk menunjang organisasi pemerintahan, termasuk Dinas Komunikasi Dan Informatika Kota Surabaya yang beroperasi pada ranah sektor publik. Berbeda dengan standar internasional yang terlalu umum, index KAMI versi 5.0 sudah disesuaikan dengan kebutuhan dan regulasi di Indonesia, khususnya untuk instansi pemerintah. Standar ini membantu pemerintahan menilai kesiapan risiko keamanan IT secara lebih tepat, mulai dari ancaman kebocoran data pribadi hingga gangguan sistem operasional. Dengan mengadopsi index KAMI versi 5.0, dinas komunikasi dan informatika kota Surabaya bisa mendapatkan panduan yang lebih relevan dan praktis dalam memperkuat keamanan informasi mereka, sekaligus memenuhi kewajiban sebagai opd yang mengelola aplikasi serta jaringan di Kota Surabaya.

1.2.4 Pertanyaan penelitian

- 1) Sejauh mana kesiapan tata kelola keamanan informasi di Dinas Komunikasi Dan Informatika Kota Surabaya apabila ditelaah melalui index KAMI versi 5.0?
- 2) Area atau domain manakah yang paling mendesak untuk ditingkatkan Dinas Komunikasi Dan Informatika Kota Surabaya menurut hasil penilaian memakai index KAMI versi 5.0?

1.3 Tujuan dan manfaat penelitian

1.3.1 Tujuan

Kajian ini bertujuan menilai tingkat kesiapan komprehensif sistem proteksi informasi pada Dinas Komunikasi Dan Informatika Kota Surabaya melalui dua tahap pelaksanaan: (1) mengukur tingkat kesiapan sistem informasi terhadap standar index KAMI versi 5.0, (2) mengidentifikasi area yang perbaikan. Dengan pendekatan ini, perusahaan akan mendapatkan peta jelas tentang kondisi aktual sistem keamanannya, titik-titik kerentanan yang perlu diperbaiki, serta langkah strategis untuk meningkatkan pertahanan ancaman sekaligus memenuhi standar nasional yang berlaku bagi pemerintahan di Indonesia.

1.3.2 Manfaat

Penelitian Memberikan Manfaat Bagi Berbagai Pihak, Terutama Dinas Komunikasi Dan Informatika Kota Surabaya Dalam Mengukur Tingkat Kematangan Keamanan Informasinya. Bagi Pemerintahan, Hasil Evaluasi Akan Menjadi Dasar Perbaikan Sistem Keamanan Informasi Yang Selama Ini Rentan Terhadap Serangan *Cyber* Seperti *Ransomware* Dan Kebocoran Data. Dengan Mengidentifikasi Celah Keamanan Informasi Berdasarkan Standar Index Kami Versi 5.0, Dinas Komunikasi Dan Informatika Kota Surabaya Dapat Menyusun Langkah Strategis Menuju Sertifikasi Nasional Sekaligus Memenuhi Regulasi Perlindungan Data Di Indonesia. Implementasi Rekomendasi Dari Penelitian Ini Diharapkan Dapat Mengurangi Gangguan Operasional Dan Meningkatkan Keandalan Layanan Bagi Masyarakat.

Secara Akademik, Penelitian Ini Memberikan Kontribusi Penting Sebagai Studi Kasus Penerapan index KAMI versi 5.0 Di Sektor Komunikasi Dan Informatika Indonesia Yang Masih Terbatas. Temuan Penelitian Juga Memperkaya Ilmu Di Bidang Tata Kelola Keamanan Informasi, Khususnya Terkait Keamanan Informasi.

1.4 Sistematika kepenulisan

1. Bab I: pendahuluan – bagian ini menguraikan latar belakang penelitian, perumusan masalah, serta arah, tujuan, dan kegunaan studi, disertai gambaran umum susunan skripsi.

2. Bab II: tinjauan pustaka – pada bab ini dipaparkan konsep-konsep teoritis yang relevan dengan topik, beserta ringkasan hasil riset terdahulu sebagai dasar pijakan kajian.
3. Bab III: metode penelitian – menggambarkan pendekatan riset yang diterapkan, meliputi alur kerja, strategi yang dipilih, dan tahapan pelaksanaan penelitian
4. Bab IV: pembahasan – bagian ini menyajikan temuan penelitian, implementasi skenario pengujian, serta analisis yang dilakukan berdasarkan rancangan alur penelitian.
5. Bab V: kesimpulan – bab terakhir merangkum hasil penelitian dan memberikan saran