Jurnal ABDIMAS-IBISA
Pengabdian Kepada Masyarakat

Vol.1 No.2
Juni 2023
Hal : 42-49

MANAJEMEN INSIDEN CYBER SECURITY

DI DINAS KOMUNIKASI DAN INFORMATIKA DIY

Eko Jhony Peranata, S.Kom., M.Kom[1]

Program Studi S1 Sains Data, Fakultas Sains Teknologi dan Kesehatan,

Institut Teknologi Bisnis Dan Kesehatan Bhakti Putra Bangsa Indonesia

Email: ekojhonypranata@gmail.com

Jl. Soekarno Hatta Borokulon Banyuurip Purworejo

Melisa Oktavia[2]

Program Studi Informatika, Universitas Perwira Purbalingga, Indonesia

Email: melisa.oktavia118@gmail.com

Jl. Letjen S Parman No.53, Kedung Menjangan, Kec. Purbalingga, Kabupaten Purbalingga, Jawa Tengah

ABSTRAK

Layanan teknologi informasi pemerintah dituntut untuk selalu berjalan optimal tanda kendala. Namun masih banyak ditemukan permasalahan insiden keamanan informasi yang dihadapi. Dari sisi sumber daya manusia, teknologi, maupun dari sisi kebijakan dan prosedural belum fokus pada aspek insiden keamanan informasi. Oleh karena itu diperlukan suatu sistem manajemen insiden keamanan informasi sebagai salah satu solusi sistematis yang harus disediakan untuk menjamin keberlangsungan layanan informasi dan sistem TI. Tujuan dari penelitian ini untuk menyediakan suatu sistem manajemen insiden keamanan informasi yang diadopsi dan dikembangkan berdasarkan standardisasi ISO/IEC 27035. Metode penelitian yang dilakukan menggunakan metode kualitatif dengan studi kasus. Penyusunan dokumen dilakukan mengacu pada pendekatan hasil assesmen antara kondisi saat ini (eksisting) dari proses bisnis dan manajemen insiden keamanan informasi yang telah dilakukan dengan klausul yang dipersyaratkan oleh ISO/IEC 27035. Hasil dari penelitian ini adalah dokumen kebijakan dan prosedur sistem manajemen insiden keamanan informasi yang didesain secara khusus sebagai standar acuan di pemerintahan. Melalui penggunaan kebijakan dan prosedur yang terstruktur akan dapat meningkatkan kinerja dalam penanganan insiden yang dihadapi pemerintah.

Kata Kunci: insiden, iso/iec 27035, keamanan informasi, manajemen.

ABSTRACT

The government services of information technology are required to always run optimally. On the other hand, many information services are still faced with security incidents. In terms of human resources, technology, policy, and procedural aspects, the focus problem has not been on security incidents of information. Therefore, we need information security incident management system as one of the system solutions that must be provided to ensure the sustainability of information services and IT systems. The purpose of this research is able to provide security information of incidents having a management system that was adopted and developed based on ISO/IEC 27035 standardization. The research methodology was carried out by using qualitative methods with case studies. The preparation of the document refers to the results of the assessment approach between the current conditions of business processes and the incident management of information security. It has been carried out with the clauses required by ISO/ IEC 27035. The results of this study are policy documents and procedures

Vol.1 No.2
Juni 2023
Hal : 42-49

for the incident management systems of information security specifically designed as a reference standard in government. Finally, the use of structured policies and procedures can improve performance in handling incidents faced by the government.

Keywords: *incident, information security, iso/iec 27035, management*.

A. PENDAHULUAN

Internet merupakan sebuah media pertukaran informasi dan data yang terbuka, artinya internet dapat diakses oleh siapa saja, kapan saja dan darimana saja. Dengan berbagai kecanggihan sarana komunikasi modern tersebut, internet sangat rentan terhadap serangan sistem informasi. Tanpa adanya sistem keamanan terhadap informasi membuat sistem informasi yang dimiliki individu, organisasi bahkan instansi pemerintahan menjadi sangat rentan terhadap adanya upayaupaya penyerangan sistem informasi. Semakin tingginya nilai (*value*) internet bagi masyarakat, maka semakin tinggi juga resiko, ancaman serta gangguan terhadap sumber daya informasi maupun interaksi yang dilakukan antar pengguna. Ancaman terhadap sumber daya informasi dan interaksi antar pengguna pada dasarnya diakibatkan oleh berbagai kelemahan yang dieksploitasi oleh pelaku dengan tujuan menguasai/ mengambil alih aset yang bernilai tersebut. Kelemahan (*vulnerability*) dapat berupa bencana alam dan kerusuhan maupun kekurangan pada sistem dan kelalaian manusia di dalam mata rantai keamanan

Di masa kini, proses bisnis pemerintahan tidak terlepas dari proses manajemen data seperti mengirim, mengumpulkan, membuat maupun menggunakan data untuk menjalankan berbagai kegiatan atau aktivitas yang terkait dengan bisnisnya. Proses pengelolaan data tersebut menjadikan pemerintah memiliki risiko besar terkait ancaman terjadinya suatu insiden keamanan informasi dari layanan elektronik yang dimilikinya. Adanya ancaman tersebut menyebabkan setiap organisasi melakukan investasi besar untuk mengamankan teknologinya dengan kencenderungan yang semakin meningkat nilainya setiap tahun. Beragamnya jenis layanan yang dimiliki oleh pemerintah tentunya memiliki tingkat keamanan dan potensi gangguan insiden yang berbeda beda. Gangguan insiden tersebut disebabkan oleh manusia ataupun akibat kerusakan aplikasi dan perangkat jaringan. Insiden deface website milik pemerintah sering terjadi dan menyebabkan layanan tidak bisa diakses. Beragam jenis insiden lainnya seperti serangan DDoS, *malware, spamming, phising* maupun serangan Advanced Persisten Threat (APT) juga semakin marak terjadi.

Mesipun kejadian insiden semakin marak terjadi, namun pemerintah sampai dengan saat ini belum memberikan perhatian khusus pada penanganan insiden. Investasi yang dilakukan kecenderungannya hanya pada penyediaan infrastruktur teknologi saja. Sedangkan pada penyiapan sumber daya manusia (SDM) yang berkompeten masih belum optimal. Pegawai di lingkungan pemerintah banyak yang belum memiliki kesadaran (*awareness*) keamanan informasi sehingga sangat rentan terkena insiden keamanan informasi. Penyediaan pedoman kebijakan dan prosedur yang sistematis juga masih belum ada menjadikan penanganan dilakukan secara individual dan tidak terkelola dengan baik. Penanganan insiden secara sistematis penting dilakukan karena insiden dapat memberikan dampak buruk bagi pemerintah. Insiden menyebabkan terjadinya kegagalan teknis dan dapat menimbulkan kerusakan data permanen. Kegagalan teknis akan mengakibatkan terganggu atau terhentinya proses bisnis pemerintahan dalam melaksanakan tugas fungsinya untuk memberikan pelayanan publik. Setelah mengungkapkan informasi, platform media sosial biasanya menampilkan pedoman yang menekankan privasi pengguna sebelum penggunaan pertama mereka (Chris et al., 2021). Semenjak tidak ditangani secara benar dampak yang diterima akibat insiden dapat menyebabkan reputasi pemerintahan menjadi buruk dan menurukan tingkat kepercayaan publik terhadap pemerintah.

Penelitian mengenai manajemen insiden secara umum sangat berkembang saat ini. Pada perusahaan pernah dilakukan penelitian mengenai manajemen insiden menggunakan framework ITIL (Ilvarianto dan Legowo, 2017; Nugraha dan Legowo, 2017; Azizah dkk, 2020). Hasil dari beberapa penelitian tersebut adalah sebuah standar prosedur dalam penanganan insiden. Melalui penggunaan prosedur yang baik akan mempermudah dalam penanganan insiden. Selanjutnya penelitian mengenai manajemen insiden di perguruan tinggi juga pernah dilakukan menggunakan framework ITIL

(Palilingan dan Batmetan, 2018). Pemerintah Indonesia melalui Kementerian Komunikasi dan Informatika telah menghimbau kepada seluruh instansi pemerintah terutama instansi pemerintah penyelenggara pelayanan publik dan instansi pemerintah yang memiliki infrastruktur vital untuk meningkatkan kesadaran akan pentingnya keamanan informasi. Himbauan kepada instansi pemerintah penyelenggara pelayanan publik, baik di lingkungan pusat maupun daerah dilakukan melalui berbagai cara, mulai dari sosialiasasi maupun bimbingan teknis (bimtek) sehingga strategi untuk mengatasinya dapat diidentifikasi, memungkinkan penggunaan yang paling efisien dari infrastruktur jaringan komputer yang ada (Dewantara & Sugiantoro, 2021). Di samping itu, pemerintah juga telah mengeluarkan regulasi atau kebijakan yang terkait dengan penerapan tata kelola keamanan informasi dilingkungan instansi pemerintah. Regulasi atau kebijakan yang telah dikeluarkan tersebut baik berupa Undang-Undang, Surat Keputusan Menteri Komunikasi dan Informatika, Peraturan Menteri Komunikasi dan Informatika hingga Surat Edaran Menteri Komunikasi dan Informatika.

Sasaran regulasi, kebijakan dan upaya yang dilakukan pemerintah melalui Kementerian Komunikasi dan Informatika tersebut adalah untuk terwujudnya penerapan tata kelola keamanan informasi di lingkungan instansi pemerintah baik tingkat pusat maupun daerah. Penelitian ini diharapkan dapat memberikan kontribusi bagi keilmuan, yakni dengan memanfaatkan nya sebagai alternatif yang lebih baik untuk menyelesaikan masalah peramalan dan dapat dimanfaatkan oleh para akademisi untuk pengembangan keilmuan lebih lanjut (Zuhrufillah et al., 2022). Dalam menerapkan tata kelola keamanan informasi di lingkungan instansi pemerintah dibutuhkan kesiapan baik yang mencakup beberapa aspek, di antaranya; infrastruktur, perencanaan, dana/finansial dan kesiapan sumber daya manusia. Dengan demikian, kajian ini ditujukan untuk menggali dan mengevaluasi sejauh mana kesiapan instansi pemerintah untuk menerapkan tata kelola keamanan informasi.

Beberapa tujuan utama manajemen insiden keamanan informasi adalah: menghindari terjadinya insiden kemanan informasi. Meminimalkan dampak insiden keamanan informasi terhadap kerahasiaan, ketersediaan, atau integritas layanan, aset informasi, dan operasi organisasi, mengurangi ancaman dan kerentanan saat terjadi insiden, meningkatkan koordinasi dan manajemen insiden keamanan informasi dalam industri investasi. mengurangi dampak biaya yang disebabkan oleh insiden keamanan informasi. melaporkan temuan kepada manajemen eksekutif.

B. METODE

Kegiatan pengabdian masyarakat ini dilakukan di Dinas Komunikasi dan Informatika Pemda DIY. Adapun tahapannya yaitu: perencanaan dan pembekalan sistem manajemen insiden keamanan informasi untuk lembaga pemerintah berdasarkan SNI ISO/IEC Dinas Komunikasi dan Informatika Pemda DIY. Pelaksanaan kegiatan dilaksanakan pada tanggal 28 Maret 2023 oleh dosen dan satu mahasiswa sebagai pendamping dan pelaksana. Langkah pelaksanaan: perijinan kepada pihak terkait, kemudian kegiatan diawali dengan pemaparan materi terkait dengan insiden *cyber security* pemerintahan agar terciptanya keamanan cyber dalam pemerintahan di Indonesia.

C. HASIL DAN PEMBAHASAN

Kegiatan pengabdian masyarakat ini dilakukan di Dinas Komunikasi dan Informatika Pemda DIY. Para audience ataupun peserta cukup antusias terhadap pemaparan materi yang disampaikan, Dalam mengembangkan dokumen kebijakan dan prosedur manajemen insiden keamanan informasi yang efektif, diperlukan sebuah proses awal untuk mengidentifikasi seluruh proses bisnis layanan teknologi informasi pada Dinas Komunikasi dan Informatika DIY. Aktifitas memahami proses bisnis yang dijalankan sangatlah penting agar ruang lingkup dan konteks yang ditentukan dapat tepat sasaran dan tidak menjadikan masalah baru. Pada aktifitas ini, berhasil diidentifikasi proses bisnis yang dilakukan oleh Dinas Komunikasi dan Informatika DIY. Materi yang disampaikan untuk meningkatkan pengetahuan terhadap pengelolaan keamanan *cyber internal* dan untuk menjamin berkembangnya Dinas Komunikasi dan Informatika DIY baik dari internal, public.

Tabel 1. Identifikasi proses bisnis

Proses Bisnis	Fungsi Bisnis
Pelayanan data center	Penyediaan layanan hosting Penyediaan layanan subdomain Penyediaan layanan mail server Penyediaan layanan colocation server Pemeliharaan infrastruktur data center
Pelayanan jaringan	Penyediaan akses internet Penyediaan fasilitas video conference Pemeliharaan infrastruktur jaringan

Dalam tahap ini dilakukan proses identifikasi aset yang dikelola oleh Dinas Komunikasi dan Informatika DIY. Identifikasi aset akan digunakan untuk menentukan bagian area mana saja yang terdampak ketika sebuah insiden terjadi. Hasil identifikasi aset kemudian dituangkan dalam bentuk tabel aset register dengan rincian terdapat 165 buah aset fisik, 161 buah aset aplikasi, dan 8 buah sarana pendukung yang harus dilindungi dari ancaman terjadinya insiden. Proses identifikasi insiden dilakukan dengan mengambil klasifikasi jenis insiden dengan mengacu pada SNI ISO/IEC 27035 dan disesuaikan dengan kondisi maupun potensi yang dihadapi. Hasil klasifikasi insiden yang ditetapkan

ada 8 jenis,yaitu: 1. Akses tidak sah 2. Denial of Service (DoS) 3. Malware 4. Kebocoran Informasi 5. Penggunaan yang tidak benar 6. Kegagalan sistem 7. Web defacement 8. Gangguan jaringan Hasil dari proses identifikasi insiden akan dituangkan dalam dokumen kebijakan dan prosedur yang akan dibuat pada tahap berikutnya. Setelah selesai melakukan klasifikasi jenis insiden, dilakukan tahapan penentuan kriteria dampak yang diakibatkan oleh suatu insiden.

Hasil dari penentuan kriteria dampak digunakan untuk menentukan seberapa besar akibat yang dihasilkan oleh insiden yang terjadi. Setelah kriteria dampak ditetapkan dilanjutkan dengan penentuan standar tingkat layanan insiden. Hal ini diperlukan untuk memastikan bahwa insiden dikelola dan ditanggapi sesuai dengan tingkat layanan yang telah ditetapkan. Tingkat layanan ini berlaku sebagai komitmen respon untuk semua jenis insiden keamanan informasi. Waktu respons insiden bervariasi sesuai dengan tingkat prioritas yang ditetapkan untuk insiden tersebut. Standar tingkat layanan dituangkan dalam bentuk tabel yang disesuaikan dengan dampak insiden yang telah ditetapkan sebelumnya.

1. Atas dasar hasil tahapan sebelumnya, dilanjutkan dengan tahap perancangan dokumen manajemen insiden. Terdapat 2 aktifitas perancangan yang harus dilakukan untuk memperbaiki sistem manajemen insiden keamanan informasi di Dinas Komunikasi dan Informatika DIY, yaitu: Penyusunan dokumen kebijakan dan prosedur manajemen insiden keamanan informasi yang sesuai dengan SNI ISO/IEC 27035,
2. Penyusunan formulir pendukung aktifitas dalam dokumen kebijakan dan prosedur manajemen insiden keamanan informasi, pembuatan dokumen baru dilakukan mengacu pada seluruh kontrol dalam ISO/IEC 27035 dengan mempertimbangkan hasil assesmen pada Tabel 1. Dari hasil assemen awal, hanya 24 kontrol yang sudah dijalankan kemudian diperbaiki agar dokumen dapat meliputi seluruh kontrol yang sesuai standar.
3. Dokumen kebijakan dan prosedur manajemen keamanan informasi yang telah dihasilkan didalamnya terdiri dari beberapa unsur sebagai berikut:
   a. Tujuan dan sasaran
   b. Referensi
   c. Ruang lingkup
   d. Tanggung jawab dan komitmen manajemen
   e. Kebijakan umum
   f. Definisi insiden keamanan informasi
   g. Deskripsi kategori insiden keamanan informasi
   h. Deskripsi proses pelaporan insiden
   i. Alur proses insiden mulai dari deteksi sampai dengan resolusi
   j. Kebutuhan aktifitas peninjauan pasca insiden, seperti pembelajaran dan proses perbaikan yang disesuaikan dengan resolusi insiden yang telah dilakukan
   k. Definisi dari masing masing peran, tanggung jawab, dan wewenang pengambilan keputusan yang ditetapkan untuk setiap fase dari proses manajemen.

Proses verifikasi dan validasi dilakukan dengan membawa dokumen kebijakan dan prosedur manajemen insiden keamanan informasi kepada Kepala Bidang Keamanan Informasi, Administrator Jaringan, serta Administrator Data Center. Tahap verifikasi dilakukan dengan cara melakukan diskusi. Hal tersebut dilakukan untuk mengetahui apa saja kekurangan pada dokumen serta apakah dokumen sudah sesuai dengan kebutuhan dan ekspektasi yang diiharapkan. Berdasarkan hasil verifikasi terdapat dua poin perbaikan yaitu:

1. Penambahan dokumen referensi, yaitu dokumen SMKI yang dimiliki oleh Dinas,

2. Perbaikan alur penanganan insiden. Setelah melewati uji verifikasi atas dokumen yang telah dibuat, dilanjutkan dengan tahapan validasi. Tahapan ini dilakukan dengan cara pembuatan skenario pengujian prosedur serta membuat checklist kegiatan yang telah dibuat. Skenario kemudian dijalankan oleh Administrator Data Center dan Administrator Jaringan. Dari proses validasi ini disimpulkan bahwa dokumen kebijakan dan prosedur manajemen keamanan informasi yang telah dibuat dapat dijalankan dengan baik.

Gambar 1 kegiatan dan penyampaian materi

D. KESIMPULAN

Kegiatan Pengabdian masyarakat dengan pemberian penyuluhan dan edukasi tentang manajemen insiden *Cyber Security* Pemerintahan Indonesia agar terciptanya keamanan siber tehadap pemerintahan Indonesia dan juga pada Dinas Komunikasi dan Informatika DIY.

E. SARAN

Adapun saran terhadap Dinas Komunikasi dan Informatika DIY dan Lembaga terkait, untuk melakukan kegiatan serupa secara berkesinambungan untuk meningkatkan keamanan siber di Dinas Komunikasi dan Informatika DIY maupun pemerintahan Indonesia.

F. UCAPAN TERIMAKASIH

Selama melaksanakan kegiatan pengabdian kepada masyarakat ini peneliti telah banyak mendapat bantuan dari berbagai belah pihak. Dalam hal ini peneliti mengucapkan banyak terimaksih terhadap seluruh pihak yang telah membantu sesingga kegiatan pengabdian kepada masyarakay ini dapat berjalan dengan lancar dan juga hasil dari kegiatan ini juga dapat bermanfaat dan dapat di gunakan sebagaimana mestinya.

DAFTAR PUSTAKA

Azizah, N., Kusumawati, Y. dan Sani, R. R. (2020). Perancangan Manajemen Perancangan Manajemen Insiden pada Layanan Teknologi Informasi Inventory Menggunakan Framework ITIL Versi3 (Studi Kasus : PT. Genta Semar Mandiri Semarang). JOINS (Journal of Information System), 5(1), hal. 136–146.

Chris, N., Susanti, T., Donglas, N., & Yantson, C. (2021). Pengaruh Kesadaran Keamanan Informasi Dan Privasi Jaringan Sosial Terhadap Perilaku Perlindungan Privasi Pada Para Pengguna Jaringan Sosial. SOURCE: Jurnal Ilmu Komunikas, hal. 170–184.

Dewantara, R., & Sugiantoro, B. (2021). Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) pada Jaringan (Studi Kasus: UIN Sunan Kalijaga Yogyakarta). *Jurnal Teknologi Informasi Dan Ilmu Komputer*, *8*(6), 1137. https://doi.org/10.25126/jtiik.2021863123

Ilvarianto, D. S. dan Legowo, N. (2017). Incident management implementation using continual service improvement method at PT AOP. in Proceedings - 2017 International Conference on Applied Computer and Communication

Palilingan, V. R. dan Batmetan, J. R. (2018). Incident Management in Academic Information System using ITIL Framework. in IOP conferences Series : materials Science and Engineering. IOP, hal. 0–9.

Rizky, A. F., Herdiyanti, A. dan Susanto, T. D. (2017). Pembuatan Prosedur Operasional Standar Pengelolaan Insiden pada Government Resources Management Systems Kota Surabaya Berdasarkan ITIL V3. 06(02), hal. 199– 214.

Zuhrufillah, I., Anggraini, F., & Dewantara, R. (2022). Peramalan Jumlah Kasus Baru HIV Menurut Provinsi Menggunakan Machine Learning dengan Teknik Levenberg-Marquardt. *Journal of Computer System and Informatics (JoSYC)*, *3*(4), 212−221. https://doi.org/10.47065/josyc.v3i4.2172