KEBIJAKAN DAN PROSEDUR MANAJEMEN INSIDEN DINAS KOMUNIKASI DAN INFORMATIKA KABUPATEN KLATEN

Nomor Dokumen	: 500.12.10.1/34/2024
Tanggal Terbit	: 5 Juni 2024
Nomor Revisi	: 1.0
Status	: Aktif
Klasifikasi	: Terbatas

Disetujui & Disahkan oleh	Diperiksa Oleh
Kepala Dinas Komunikasi dan Informatika Kabupaten Klaten	Kepala Bidang Informatika dan Persandian Dinas Komunikasi dan Informatika Kabupaten Klaten
Aris Pramana, S.E., M.M Pembina NIP. 197507182005011006	**Andi Hermanto,S.Kom., M.Eng** Penata Tingkat I NIP. 198304182009041003

DAFTAR RIWAYAT DOKUMEN

No. Versi	Tanggal Review & Revisi	Isi Perubahan	Bagian
1.0	5 Juni 2024	● Draft Awal	All

KEBIJAKAN DAN PROSEDUR MANAJEMEN INSIDEN

1. TUJUAN

Prosedur manajemen insiden bertujuan untuk memastikan pendekatan konsisten dan efektif untuk manajemen insiden keamanan informasi, termasuk komunikasi tentang kejadian dan kelemahan keamanan.

2. RUANG LINGKUP

Prosedur ini berlaku dalam ruang lingkup manajemen insiden keamanan informasi dalam proses bisnis di Dinas Komunikasi dan Informatika Kabupaten Klaten.

3. REFERENSI

A. ISO/IEC 27001:2022, Annex A5.7 Ancaman Kecerdasan
B. ISO/IEC 27001:2022, Annex A.5.24 Perencanaan dan Persiapan Manajemen Insiden Keamanan Informasi
C. ISO/IEC 27001:2022, Annex A.5.25 Penilaian dan Keputusan Keamanan Informasi
D. ISO/IEC 27001:2022, Annex A.5.26 Respon terhadap Insiden Keamanan Informasi
E. ISO/IEC 27001:2022, Annex A.5.27 Pembelajaran dari Insiden Keamanan Informasi
F. ISO/IEC 27001:2022, Annex A.5.28 Pengumpulan Bukti
G. ISO/IEC 27001:2022, Annex A.6.8 Pelaporan Peristiwa Keamanan Informasi

4. PERAN DAN TANGGUNG JAWAB

A. Manajemen puncak memegang tanggung jawab penuh atas pelaksanaan dari keseluruhan proses dan aktivitas yang dijabarkan dalam prosedur ini
B. CISO bertanggung jawab untuk mengkoordinasikan proses dan aktivitas yang dijabarkan dalam kebijakan ini termasuk pemeliharaan dari catatan (records) hasil proses dan aktivitas tersebut.
C. Tim TI dan jaringan dan Tim SMKI yang mewakili setiap divisi harus mengambil tanggung jawab lebih lanjut untuk memastikan adanya pengendalian insiden dengan cara senantiasa memperbarui review aktivitas yang berada di bawah kendalinya
D. Pengendali dokumen bertanggung jawab untuk mendokumentasikan setiap perubahan dan hasil tinjauan perubahan

5. DOKUMEN TERKAIT

A. Rekapitulasi Laporan Insiden

6. KEBIJAKAN DAN PROSEDUR

Prosedur manajemen insiden harus dilaksanakan dalam proses bisnis di Dinas Komunikasi dan Informatika Kabupaten Klaten.

1. Kejadian keamanan informasi adalah sebuah kejadian pada sistem, layanan ataupun jaringan yang dapat mengindikasikan adanya kegagalan keamanan atau kejadian yang mungkin memiliki keterkaitan dengan keamanan informasi.
2. Insiden keamanan informasi dibagi menjadi 2, yaitu insiden IT dan insiden Non IT.
    a. Insiden IT adalah semua insiden yang terkait dengan sistem informasi atau aplikasi yang dapat mengganggu proses bisnis perusahaan. Contoh: insiden IT adalah kerusakan pada perangkat sistem informasi, jaringan tidak dapat diakses, error pada aplikasi serta kegagalan proses backup dan restore, hilangnya notebook/PC, hilangnya/bocornya informasi perusahaan.
    b. Insiden non-IT adalah semua insiden yang tidak terkait dengan sistem informasi atau aplikasi namun berpotensi untuk menimbulkan gangguan terhadap keamanan informasi. Contoh insiden non-IT adalah kerusakan genset, akses kontrol pintu tidak berfungsi, pintu akses ke wilayah terbatas dalam keadaan terbuka saat tidak ada personel.
3. Kelemahan keamanan informasi adalah sebuah kelemahan yang teridentifikasi pada sistem, layanan atau jaringan yang dapat dieksploitasi oleh pihak yang tidak bertanggung jawab dan dapat menyebabkan pelanggaran terhadap kebijakan keamanan informasi.
4. Insiden keamanan informasi adalah kejadian keamanan informasi yang tidak diinginkan dan tidak diperkirakan dimana kejadian tersebut menimbulkan gangguan terhadap operasional bisnis dan mengancam keamanan informasi.
5. Kategori insiden:
    a. Weakness: belum adanya dampak secara langsung tetapi terdapat kelemahan dalam suatu kegiatan, contoh data tidak terbackup, password lemah, dan antivirus tidak terupdate. Kategori insiden ini harus diselesaikan dalam waktu 15 (lima belas) hari.

b. Low impact incident: adalah insiden yang mempengaruhi user secara individu saja, contohnya user tidak dapat login/ data seorang user hilang. Kategori insiden ini harus diselesaikan dalam waktu 7 (tujuh) hari.
c. Medium impact incident: mempengaruhi beberapa user tetapi tidak mempengaruhi secara keseluruhan, contoh email tidak dapat diakses, beberapa data hilang, beberapa fitur tidak dapat diakses. Kategori insiden ini harus diselesaikan dalam waktu 3 (tiga) hari.
d. High impact incident: mempengaruhi seluruh sistem, contoh gangguan server, gangguan network ke server, domain, dan gangguan lainnya. Kategori insiden ini harus diselesaikan dalam waktu maksimal 8 (delapan) jam.

6. Tim IT yang bertanggung jawab atas manajemen insiden harus memiliki kesadaran dan pengetahuan yang cukup untuk mengidentifikasi kejadian, kelemahan dan insiden keamanan informasi.
7. Setiap kejadian, kelemahan dan insiden keamanan informasi harus terdokumentasi dan ditangani dengan memadai.
8. Tim IT bertanggung jawab untuk mengumpulkan informasi yang berkaitan dengan ancaman keamanan informasi dan dianalisis untuk menghasilkan pencegahan terhadap ancaman kecerdasan.
9. Bentuk risiko dan kerentanan ancaman kecerdasan :
    a. Serangan phising : memanfaatkan informasi, perilaku serta cara berperilaku daring untuk melakukan serangan phising (seperti situs palsu yang memiliki informasi terkini yang sedang terjadi seperti bencana alam dan/atau pandemic) yang isinya hampir jutaan spam.
    b. Infeksi malware : Jenis software berbahaya yang digunakan untuk merusak, mencuri, atau mengganggu operasi sistem komputer. Malware terbagi menjadi beberapa jenis seperti virus, worm, trojan, ransomware, spyware, adware, dan keylogger.
    c. Serangan DDoS (Distributed Denial of Service) : serangan yang dilakukan oleh pihak tidak bertanggungjawab dengan mengirimkan banyak permintaan koneksi secara bersamaan ke server atau situs web.

d. Injeksi Structured Query Language (SQL) : serangan yang dilakukan dengan memanipulasi input data pada sebuah aplikasi web yang menggunakan basis data untuk memanfaatkan celah keamanan pada sistem basis data dan memasukkan perintah SQL yang tidak sah.
e. Sniffing : tindak kejahatan penyadapan oleh pihak tidak bertanggungjawab yang dilakukan memakai jaringan internet untuk mencuri data dan informasi pribadi dari pemilik perangkat yang diretas.

10. Tim IT menggunakan tools *Sophos/Wazuh* sebagai upaya pencegahan ancaman kecerdasan, dan tim terkait senantiasa akan melakukan pembaharuan kemampuan penanganan ancaman kecerdasan tersebut.

6.1 PELAPORAN INSIDEN

1. Setiap kejadian, kelemahan dan insiden keamanan informasi harus dilaporkan secepat mungkin kepada koordinator manajemen insiden dan/atau Divisi Support.
2. Koordinator manajemen insiden yang menerima pelaporan kejadian, kelemahan dan insiden keamanan informasi harus membuat catatan tertulis terkait laporan yang diterima.

6.2 PENANGANAN INSIDEN

1. Setiap kejadian, kelemahan dan insiden keamanan informasi harus dianalisis dan dievaluasi.
2. Setiap insiden keamanan informasi harus ditangani dengan baik untuk mencegah meluasnya insiden, untuk memulihkan layanan atau informasi yang mungkin hilang dan untuk meminimalkan dampak dari insiden.
3. Setiap laporan akan menjadi bukti rekaman pelaporan internal yang harus dijaga dan dilindungi

6.3 PEMBELAJARAN DARI INSIDEN

1. Setiap proses penanganan setiap kejadian, kelemahan dan insiden keamanan informasi harus dianalisis untuk mencari penyebab utama. Proses ini mencakup pengumpulan dan analisis terhadap fakta terkait kejadian, kelemahan dan insiden keamanan informasi.
2. Proses analisis dan setiap tindakan korektif maupun peningkatan yang diambil harus didokumentasikan dengan baik.

7. FLOWCHART

7.1 PROSEDUR MANAJEMEN INSIDEN