

2022



LAPORAN

HASIL PENILAIAN
CYBER SECURITY MATURITY (CSM)
DINAS KOMUNIKASI DAN INFORMATIKA
PROVINSI BENGKULU

PENDAHULUAN

I. Umum

Tingkat kesiapan keamanan siber di setiap organisasi berbeda-beda, sehingga masing-masing organisasi juga membutuhkan strategi yang berbeda-beda pula dalam menghadapi ancaman, serangan, maupun ancaman siber. Dalam implementasi keamanan siber, beberapa organisasi baru fokus terhadap perbaikan penerapan kontrol keamanan yang lebih proaktif, penyusunan peraturan dan kebijakan keamanan siber, dan penyusunan strategi keamanan berdasarkan hasil deteksi insiden. Selain itu, sebagian organisasi telah mendorong investasi teknologi sebagai kebutuhan keamanan serta telah memberikan dukungan personel di bidang keamanan siber yang kompeten, serta mempertimbangkan risiko siber serta mendorong budaya keamanan siber secara menyeluruh untuk keberlangsungan organisasinya.

Setiap organisasi harus memahami kelemahan dari proses keamanan siber yang dimiliki. Sehingga dapat menentukan target tingkat keamanan siber yang akan dicapai dan memastikan bahwa organisasi tersebut telah siap dalam menghadapi ancaman siber dalam bentuk apapun. Oleh karena itu diperlukan suatu metode pengukuran kematangan keamanan siber agar organisasi dapat melakukan peningkatan dalam pengelolaan proses keamanan siber dan memastikan bahwa telah dioptimalkan sepenuhnya dan berfungsi secara menyeluruh. Untuk itu, Badan Siber dan Sandi Negara (BSSN) telah membentuk suatu *framework* untuk mengukur *cyber security maturity* yang dapat digunakan sebagai metode untuk mengukur tingkat kematangan keamanan siber suatu organisasi.

Tools Cyber Security Maturity merupakan alat bantu yang digunakan untuk mengukur kematangan keamanan siber di organisasi. Sektor pemerintahan sebagai salah satu domain yang memanfaatkan ruang siber diharapkan turut melakukan peningkatan pengelolaan keamanan siber serta memastikan pengelolaan tersebut berjalan dengan optimal dan berfungsi secara menyeluruh.

II. Tujuan Kegiatan

Kegiatan ini bertujuan untuk mengetahui tingkat maturitas keamanan siber di lingkungan Dinas Komunikasi dan Informatika Provinsi Bengkulu. Dengan adanya tingkat maturitas ini diharapkan dapat memberikan gambaran mengenai apa yang harus menjadi tindak lanjut baik oleh *stakeholder* maupun Badan Siber dan Sandi Negara (BSSN) untuk meningkatkan maturitas keamanan siber.

III. Ruang Lingkup Kegiatan

Kegiatan yang dilaksanakan meliputi pemetaan aspek penanganan insiden meliputi:

1. Aspek Tata Kelola
2. Aspek Identifikasi
3. Aspek Proteksi
4. Aspek Deteksi
5. Aspek Respon

IV. Metodologi Kegiatan

Metodologi yang digunakan berdasarkan hasil pengisian instrumen *Cyber Security Maturity (CSM)*, wawancara/diskusi, dan melihat ketersediaan dokumen keamanan siber. Hasil diberikan dalam bentuk Indeks Kematangan, Level Kematangan dan bagan berbentuk radar yang menjelaskan maturitas setiap aspek keamanan siber.

Penentuan Level Kematangan diukur berdasarkan Indeks Kematangan yang didapat. Konversi Indeks Kematangan menjadi Level Kematangan menggunakan formula:

$$\text{Level Kematangan (\%)} = \frac{\text{Indeks Kematangan}}{5} \times 100\%$$

Nilai Level Kematangan dikategorikan menjadi :

- Level 1 (*Initial*) : Rentang Level Kematangan 0 % s.d. 20 %
- Level 2 (*Repeatable*) : Rentang Level Kematangan 21 % s.d. 40 %
- Level 3 (*Defined*) : Rentang Level Kematangan 41 % s.d. 60 %
- Level 4 (*Managed*) : Rentang Level Kematangan 61 % s.d. 80 %
- Level 5 (*Optimized*) : Rentang Level Kematangan 81 % s.d. 100 %

V. Pelaksanaan Kegiatan

1. Pengisian Instrumen CSM

Pengisian Instrumen CSM dilakukan secara mandiri oleh *stakeholder* pada tanggal 4 s.d. 8 Juli 2022.

2. Validasi Penilaian CSM

BSSN melakukan validasi pengisian instrumen CSM pada tanggal 11 dan 12 Juli 2022, dengan cara diskusi dengan perwakilan tim Diskominfo Provinsi Bengkulu. Tim BSSN yang terlibat:

- 1) Nurhaerani, S.E.
- 2) Melita Irmasari, S.ST, M.M.
- 3) Ni Putu Ayu Lhaksmi Wulansari, S.Tr.TP.
- 4) Siti Rahmawati, S.Kom

HASIL KEGIATAN

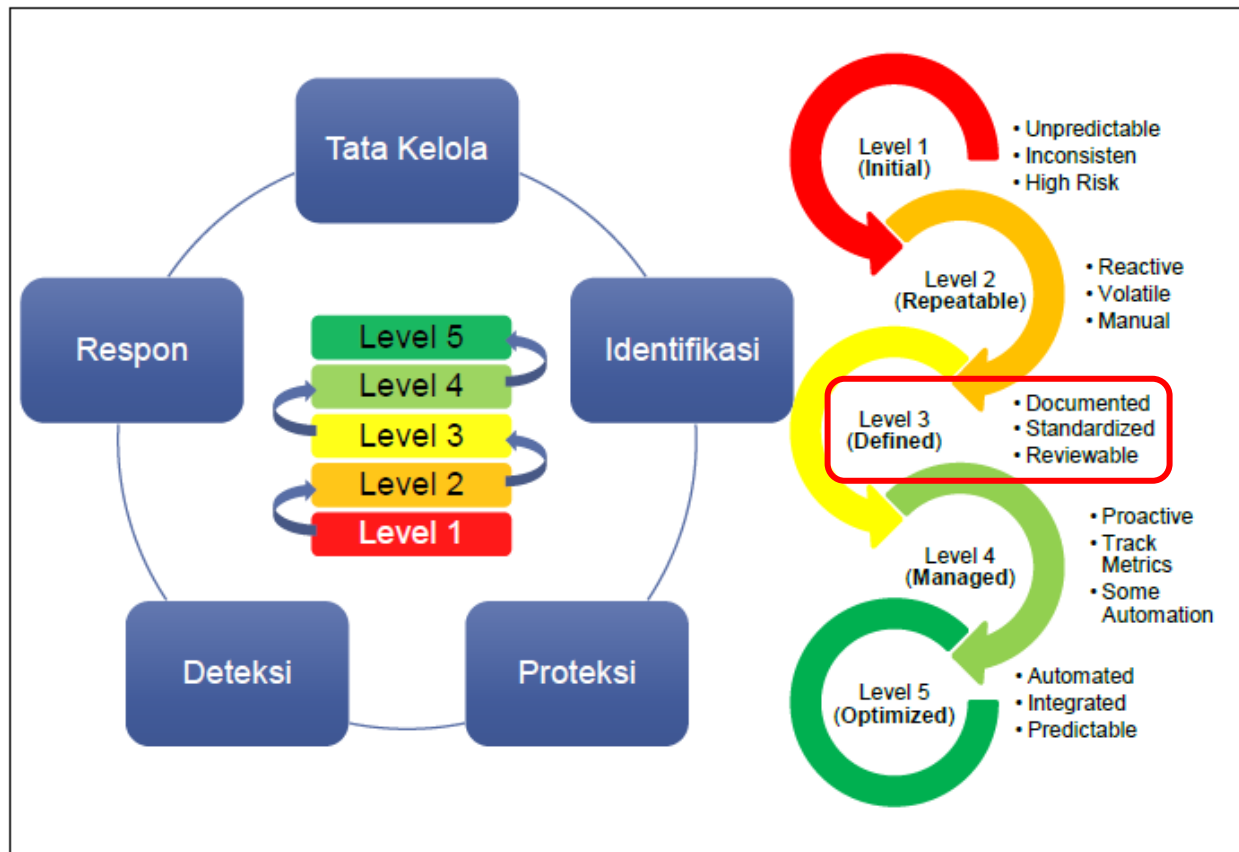
I. Informasi *Stakeholder*

Nama Instansi/Lembaga : Dinas Komunikasi dan Informatika Provinsi Bengkulu
Alamat : Jl. Basuki Rahmat No. 06 Sawah Lebar Baru, Ratu Agung, Kota Bengkulu 38222
Nomor Telp./Fax. : (0736) 7325176 / 0736 7325837
Email : diskominfotik@bengkuluprov.go.id
Narasumber Instansi/Lembaga :

1. Tanti Nasilva, S.Sos (Kepala Bidang Statistik dan Persandian)
2. Isweldi, S.Sos (Sub Koordinator Tata Kelola Persandian)
3. Mukhlis S, S.Sos (Sub Koordinator Operasional Pengamanan Persandian)
4. M. Iqbal, S.T., M.E. (Sub Koordinator Tata Kelola E-Government)
5. Hijrah Saputra, S.Kom., M.E. (Sub Koordinator Data dan Informasi BKD)
6. Febriyanda Ardita Putra, S.Kom (Pranata Komputer Ahli Pertama)
7. Ferdi Septianda, S.T. (Pranata Komputer Ahli Pertama)
8. Adio Gustiansyah, S.T. (Pranata Komputer Ahli Pertama)
9. Hendy Dwiyanayah, S.Kom. (Analisis Persandian)

II. Deskripsi Ruang Lingkup Penilaian

1. Ruang Lingkup Penilaian :
☐ Organisasi Keseluruhan ☐ Regional, Kanwil, Cabang ☒ Unit Kerja ☐ Lainnya
2. Instansi/Unit Kerja : Dinas Komunikasi dan Informatika Provinsi Bengkulu



Gambar 2. Capaian Level Kematangan

Level Kematangan 3:

Level kematangan 3 menunjukkan bahwa pengelolaan keamanan siber di Dinas Komunikasi dan Informatika Provinsi Bengkulu sudah terorganisasi dengan jelas, bersifat formal, dilakukan secara berulang, dilakukan reviu berkala, dan konsisten. Namun penerapan perubahan belum dilakukan secara berkelanjutan.

IV. Kekuatan/Kematangan

Tata Kelola

1. Organisasi sudah membuat program pemahaman kesadaran keamanan informasi untuk semua karyawan namun belum berkelanjutan.
2. Setiap karyawan sudah mendapatkan pengarahan mengenai Keamanan Informasi namun hanya sebagian kecil pegawai yang menerapkan kebijakan keamanan informasi, meskipun belum semuanya berkontribusi terhadap efektivitas sistem manajemen keamanan informasi.
3. Organisasi sudah melatih staf secara khusus tentang kewajiban menjaga data privasi namun organisasi jarang melakukan manajemen kerentanan siber dan mitigasi kerentanan serta belum melakukan simulasi secara rutin.
4. Telah memiliki kebijakan terkait keamanan informasi, diantaranya Peraturan Gubernur Bengkulu Nomor 36 Tahun 2020 tentang Penyelenggaraan Persandian untuk Pengamanan Informasi dan Peraturan Gubernur Bengkulu Nomor 37 Tahun 2021 tentang Tata Kelola SPBE, namun belum dilaksanakan secara menyeluruh dan belum terdapat turunan kebijakannya baik berupa Juknis maupun SOP.
5. Telah melakukan reviu security risk assessment dan risk treatment, namun belum dilakukan secara berkala dan berkelanjutan.
6. Telah memiliki kebijakan terkait dengan audit Keamanan SPBE, diantaranya Peraturan Gubernur Bengkulu Nomor 9 Tahun 2022 tentang Sistem Pemerintahan Berbasis Elektronik Pemerintah Provinsi Bengkulu, namun belum dilaksanakan secara berkala.
7. Menerapkan standar konfigurasi (port, protokol, service) untuk semua sistem, seperti operating system, software/aplikasi, dan lain-lain, namun belum semuanya terdokumentasi.
8. Telah melindungi aplikasi web organisasi menggunakan firewall aplikasi web (WAFs).
9. Telah menyusun risk register beserta analisis dampaknya sesuai dengan probabilitas yang ada.

10. Telah melakukan manajemen kerentanan siber dan mitigasi terhadap kerentanan, namun belum secara berkala.
11. Telah melakukan penetrating testing menggunakan pihak eksternal (BSSN).
12. Konfigurasi dan akun default selalu diubah sebelum digunakan, namun belum terdokumentasi.

Identifikasi

1. Telah melakukan perencanaan kapasitas secara berkala untuk memastikan bahwa semua aset perangkat dan aplikasi sesuai dengan kebutuhan namun belum dilakukan secara berkala.
2. Menerapkan keamanan pada sebagian perangkat keras dan perangkat lunak saat ada *update patch* yang sudah dirilis, namun belum ada pengelolaan *patch*.
3. Telah mengidentifikasi perangkat yang tidak diizinkan oleh organisasi, namun belum dilakukan pembatasan aksesnya.
4. Organisasi sudah melakukan klasifikasi informasi, namun belum terinventarisasi.
5. Aspek keamanan menjadi pertimbangan dan diprioritaskan dalam semua pengambilan keputusan TI, kapasitas server dan perangkat jaringan.
6. Telah memiliki metode atau standar untuk klasifikasi data yang mengacu pada KIP dan PPID.
7. Menerapkan *patch* keamanan pada semua perangkat keras dan perangkat lunak saat ada *update patch* yang sudah dirilis.

Proteksi

1. Telah memiliki firewall dan IPS namun belum diupdate secara rutin.
2. Firewall atau ACL menerapkan *implicit or explicit deny any/any rule*.
3. *Inbound* dan *outbond network traffic* hanya mengizinkan *traffic* yang dibutuhkan oleh organisasi, meskipun hanya dari sisi server.

4. *Inbound network traffic* difilter untuk memeriksa malware dan mencegah eksploitasi terhadap kerentanan, namun masih terkendala pembaharuan lisensi untuk implementasinya.
5. Sebagian aplikasi yang menggunakan server terpisah baik fisik maupun virtual.
6. Email system telah melakukan pengecekan otomatis terhadap spam/phishing/malware.
7. Master images tersimpan pada server yang dikonfigurasi secara aman
8. Sebagian perangkat dilakukan enkripsi dan *time-based authentication*.
9. Telah menggunakan informasi identitas dan akses pengguna digunakan untuk membatasi hak akses dari dalam jaringan.
10. Telah mengimplementasikan Multi-Factor Authentication (MFA) digunakan untuk mengakses data sensitif.
11. Semua data penting di organisasi di-*backup* secara berkala dan disimpan di tempat yang aman, meskipun dilakukan secara manual, belum dilakukan pengujian integritas data dan tidak diamankan dengan enkripsi.
12. Log telah disimpan sehingga mempermudah untuk dilakukan audit dan forensik.
13. Sebagian aplikasi telah menerapkan *whitelists* aplikasi di organisasi juga memastikan bahwa hanya *authorized software library* dan *signed script*.
14. Semua *critical system clocks* telah disinkronkan dengan metode otomatis seperti Network Time Protocol.

Deteksi

1. Terdapat Change Advisory Board (CAB) yang meninjau dan menyetujui semua perubahan konfigurasi, namun belum dilakukan dengan jadwal tertentu hanya sesuai dengan kebutuhan.
2. Sudah menerapkan monitoring (pemantauan dan notifikasi) terhadap aktivitas lalu lintas jaringan walaupun masih secara manual.
3. Telah melakukan *monitoring* terhadap log dari perangkat *security control*, jaringan, dan aplikasi pada saat diketahui masalah.

4. Sebagian aplikasi telah mengaktifkan Enable Detailed Logging yang mencakup informasi terperinci seperti *event source*, tanggal, *user*, *timestamp*, *source addresses*, *destination addresses*, dan komponen lainnya.
5. Memonitor aktivitas fisik dan juga pihak ketiga untuk mendeteksi adanya potensi kejadian keamanan siber.
6. Dapat mendeteksi aktivitas anomali login seperti waktu, lokasi, durasi, dan sebagainya meskipun secara manual.
7. Memiliki SOC bayangan atau manajemen teknis yang dapat dihubungi setiap saat untuk menangani kejadian dengan prioritas tinggi dan kritis sesuai dengan tupoksi yang ada.
8. Memiliki *contact tree* untuk mengeskalasi dalam merespon suatu kejadian.
9. Memiliki mekanisme *sharing* informasi hasil deteksi meskipun hanya lingkup internal.
10. Top Level Management telah menerima *briefing* tentang kondisi keamanan siber terkini, minimal 1 tahun sekali dan perlu ditingkatkan.

Respon

1. Memiliki kebijakan penanganan insiden namun tidak selaras dengan kebijakan pengaturan kesinambungan organisasi atau business continuity planning (BCP).
2. Memiliki standar operasional prosedur (SOP) dan form pelaporan penanganan insiden yang diketahui oleh pihak terkait.
3. Memiliki Rencana Respon insiden atau Disaster Recovery Plan (DRP) dan Standard Operasional Prosedur (SOP) penanganan insiden namun belum direviu secara berkala.
4. Telah memiliki kontak tim penanganan insiden internal dan eksternal dan selalu diperbarui.
5. Telah mendokumentasikan rencana respon insiden, mendefinisikan peran personel pada fase penanganan/managemen insiden serta pembagian peran kepada pihak eksternal dalam eskalasi permasalahan.

6. Desain jaringan dapat memastikan apabila server DMZ terkena serangan siber, penyerang tidak dapat mengakses server yang lain, karena secara fisik server terpisah.
7. Tim respons insiden memiliki kemampuan mendeteksi insiden, melakukan analisis, dan rekomendasi solusi.
8. Tim melakukan scanning ulang untuk memastikan bahwa pada suatu kerentanan yang ditangani sudah ditutup.
9. Ketika mengalami insiden siber, tim respons insiden dapat dengan cepat mendapat bantuan dari tim manajemen krisis namun sulit mendapatkan informasi dari pihak ketiga.
10. Tim respons insiden di organisasi mencatat setiap langkah yang dilakukan dalam rangka penanggulangan insiden menggunakan format yang baku.
11. Mempublikasikan informasi untuk semua pegawai dan *stakeholder*/klien/konsumen/pelanggan mengenai mekanisme pelaporan anomali dan insiden siber kepada tim penanganan insiden siber organisasi namun tidak dimasukkan dalam kegiatan rutin.
12. Laporan insiden di organisasi dilaporkan ke *middle management* dan ke pihak eksternal yang berkepentingan/wajib dilaporkan sesuai regulasi.

V. Kelemahan/Kekurangan

Tata Kelola

1. Belum dilakukan secara berkelanjutan kegiatan program pemahaman kesadaran keamanan informasi dengan fokus/isu baik terkait dengan kebijakan yang telah ditetapkan maupun permasalahan keamanan informasi.
2. Belum melakukan internal audit keamanan informasi secara berkala.
3. Organisasi belum melakukan gap analisis untuk memahami skill dan behavior yang tidak dimiliki oleh karyawan untuk membuat roadmap terkait baseline Pendidikan dan pelatihan keamanan informasi dan belum melakukan simulasi secara rutin.

4. Personel yang terlibat dalam pengembangan software/aplikasi belum mendapatkan pelatihan secure coding.
5. Belum melakukan reviu izin akses dari akun pengguna secara berkala.
6. Konfigurasi firewall belum terdokumentasi dengan baik dan dilakukan reviu terhadap konfigurasi router dan switch bila dianggap perlu saja.
7. Belum membentuk Red Team dan Blue Team serta melakukan pengujian secara berkala dalam mengukur kesiapan organisasi untuk mengidentifikasi dan menghentikan serangan atau merespon dengan cepat dan efektif dari insiden keamanan yang terjadi.
8. Belum melakukan pemisahan environment antara sistem production dan development, dan mengizinkan akses kepada pengembang tanpa pengawasan dari bagian keamanan organisasi.
9. Belum menggunakan standar hardening configuration template pada database dan belum dilakukan pengujian pada semua sistem (software) yang menjadi bagian penting dari proses bisnis organisasi.
10. Belum mengimplementasikan software anti virus dan anti malware secara terpusat dan selalu update terhadap perangkat endpoint.
11. Belum melakukan filterisasi terhadap seluruh jenis file lampiran email dan penerapan sandbox.
12. Belum memiliki Business Continuity Plan dan Disaster Recovery Plan yang mencakup backup dan restoration dari data pribadi.
13. Belum memiliki kebijakan metode penghapusan data.
14. Belum memiliki kebijakan terkait perlindungan data pribadi.
15. Belum melakukan analisis statis dan/atau dinamis untuk memverifikasi bahwa praktik secure coding benar-benar diterapkan pada software yang dikembangkan secara internal.
16. Belum ada kebijakan yang mengatur single ID untuk otentikasi.

17. Dalam pengembangan software belum menggunakan Praktik secure coding, algoritma enkripsi dan direviu secara berkala, serta belum menerapkan kontrol kriptografi.
18. Belum ada prosedur untuk menambah/mengubah/menghapus hak akses ketika terjadi perpindahan karyawan.

Identifikasi

1. Organisasi belum membuat/memperbarui *roadmap* keamanan TI organisasi dalam jangka waktu tertentu.
2. Belum memiliki system configuration management tools untuk otomatisasi konfigurasi perangkat keras dan perangkat lunak.
3. Belum memiliki metode/standar untuk klasifikasi aset TI.
4. Belum dilakukan inventaris data yang ada pada aset perangkat lunak secara rutin.
5. Organisasi belum melakukan Analisa Keterkaitan antara keamanan dan kenyamanan dari pengguna asset dalam rangka penyusunan standar keamanan informasi.
6. Belum ada dokumentasi mengenai alur informasi yang memproses data stakeholder yang sesuai dengan kebijakan regulasi dan kebutuhan bisnis.
7. Belum ada reviu yang berkaitan dengan pemrosesan data sensitive termasuk data stakeholder sesuai dengan kebijakan dan regulasi.
8. Belum adanya kebijakan dan implementasi mengenai retensi data.
9. Belum dilakukan pemeringkatan pada kerentanan yang ditemukan berdasarkan pedoman/standart organisasi.
10. Belum memiliki Bisnis Impact Analysis terhadap perangkat dan aplikasi TI.
11. Belum menjadikan prioritas terkait dengan langkah proteksi keamanan siber termasuk memprioritaskan perlindungan data dan aset kritis.
12. Belum tercantum pada risk register untuk semua aplikasi yang memproses data stakeholder/klien/konsumen/pelanggan.
13. Belum memiliki *system configuration management tools* otomatisasi konfigurasi perangkat keras dan perangkat lunak.

14. Belum memiliki metode/standar untuk klasifikasi aset IT.
15. Belum melakukan klasifikasi terhadap cyber threats yang ditemukan.
16. Belum melakukan vulnerability scanning dan/atau penetration testing terhadap semua aset perangkat dan aplikasi.

Proteksi

1. Belum memiliki perangkat jaringan menggunakan otentikasi terpusat.
2. Belum menerapkan firewall filtering antar segmen pada jaringan lokal.
3. Belum menonaktifkan komunikasi antar workstation.
4. Belum melakukan disable peer-to-peer pada wireless client di perangkat endpoint.
5. Belum memiliki pengaturan terkait pembatasan aplikasi yang dapat diunduh, diinstall dan dioperasikan pada perangkat milik organisasi.
6. Belum menerapkan DNS Filtering Services.
7. Belum ada pembatasan dalam penggunaan scripting tools.
8. Organisasi belum memastikan web browser, email client yang digunakan pada perangkat milik organisasi apakah masih mendapatkan update support dan juga dalam penggunaan add-on dan plugin.
9. Belum melakukan implementasi URL filtering, device control dan application control pada semua perangkat endpoint
10. Belum ada pengaturan akses terhadap perangkat USB/penyimpanan eksternal.
11. Belum menerapkan *Multi-Factor Authentication* (MFA) untuk mengakses data sensitif dan akses jaringan.
12. Belum menerapkan IP reputation untuk memverifikasi alamat IP yang diizinkan dalam proses transaksi.
13. Belum dapat melacak dan mendeteksi perilaku anomali transaksi yang dilakukan oleh karyawan maupun stakeholder/klien/konsumen/pelanggan serta mengidentifikasi perangkat yang digunakannya.
14. Belum melakukan disable peer-to-peer pada wireless client di perangkat endpoint.

15. Tidak ada data stakeholder/klien/konsumen/pelanggan dienkripsi saat disimpan, namun dienkripsi saat proses transmisi.
16. Belum melakukan pengujian data integrity secara berkala terhadap data yang dibackup.
17. Belum menerapkan enkripsi untuk data stakeholder/pengguna yang disimpan oleh organisasi dan enkripsi pada media penyimpanan eksternal.

Deteksi

1. Belum dilakukan reviu terhadap semua perubahan konfigurasi melalui Change Management system.
2. Perubahan konfigurasi pada peralatan jaringan belum terdeteksi secara otomatis.
3. Belum melakukan pemantauan akses fisik terhadap perangkat yang berada di dalam ruangan data center.
4. Belum memiliki sistem untuk memonitoring dan mencegah kehilangan data sensitif termasuk data stakeholder/klien/konsumen/pelanggan.
5. Belum dapat mendeteksi Wireless Access Point yang terhubung ke jaringan LAN (ethernet) karena masih menggunakan ISP secara langsung.
6. Perubahan konfigurasi pada peralatan jaringan belum terdeteksi secara otomatis.
7. Belum mengimplementasikan SIEM untuk monitoring secara maksimal untuk monitoring anomali pada jaringan, server dan aplikasi.
8. Belum menerapkan automated port scan secara berkala terhadap semua sistem dan memberikan alert jika terdapat port yang tidak sah terdeteksi pada suatu sistem.
9. Belum memiliki sistem untuk mendeteksi ancaman siber sehingga dapat memberikan input/feed bagi threat intelligence seperti penggunaan deception technology.
10. Belum memiliki sistem untuk melakukan Malicious Code Detection guna mendeteksi, menghapus, dan melindungi dari malicious code.
11. Tidak menyimpan semua log terhadap URL yang diakses oleh pegawai.

12. Belum secara aktif melakukan threat hunting untuk mengetahui secara dini apakah sistem telah disusupi malicious file.
13. Belum mengimplementasikan vulnerability scanning tools secara otomatis untuk mendeteksi kerentanan siber.
14. Belum secara aktif melakukan threat hunting untuk mengetahui secara dini apakah sistem telah disusupi malicious file.
15. Belum mengimplementasikan vulnerability scanning tools secara otomatis untuk mendeteksi kerentanan siber.

Respon

1. Belum memiliki kebijakan penanganan insiden dan selaras dengan kebijakan pengaturan kesinambungan organisasi atau business continuity planning (BCP).
2. Belum merencanakan skenario insiden dan melakukan latihan respon insiden secara rutin untuk pegawai yang terlibat dalam respon insiden.
3. Belum melaksanakan pelatihan untuk pegawai tentang cara mengidentifikasi, penanganan, dan pelaporan suatu insiden keamanan informasi.
4. Belum memiliki sumber daya redundan yang dapat langsung digunakan ketika sistem penting/kritikal yang down karena insiden siber.
5. Waktu yang dibutuhkan untuk melakukan diskoneksi segmen jaringan untuk mencegah penyebaran malware masih terlalu lama (lebih dari 3 jam).
6. Tim respon insiden memiliki sedikit peralatan sumber daya analisis insiden.
7. Hasil revidu terhadap rekap laporan insiden siber belum dilaporkan ke *top management* dan didistribusikan kepada para pemangku kepentingan serta digunakan dalam rangka merevidu kontrol yang ada untuk perbaikan respon penanganan insiden siber selanjutnya.
8. Rekaman insiden dan pelanggaran tidak disimpan dan dilaporkan berdasarkan *trends* insiden dalam jangka waktu tertentu.
9. Belum menerapkan mekanisme backup data karyawan ke cloud organisasi.

10. Belum memiliki SLA (*Service Level Agreement*) dalam penanganan insiden.
11. Belum melakukan revidir rekap laporan insiden.

VI. Rekomendasi

1. Untuk meningkatkan aspek tata kelola di lingkungan Diskominfotik Pemrov Bengkulu maka dapat dilakukan hal-hal sebagai berikut:
 - a. Mengimplementasikan Pergub Bengkulu Nomor 36 dan 37 Tahun 2020.
 - b. Mengimplementasikan Pergub Bengkulu Nomor 9 Tahun 2022.
 - c. Perlu menyelenggarakan kegiatan program pemahaman kesadaran keamanan informasi dengan fokus/isu baik terkait dengan kebijakan yang telah ditetapkan maupun permasalahan keamanan informasi yang perlu dilakukan secara berkelanjutan.
 - d. Perlu adanya pelatihan Secure Coding untuk personel yang terlihat dalam pengembangan software/aplikasi.
 - e. Menyusun kebijakan dan implementasi dalam pelaksanaan revidir izin akses dari akun pengguna dan menerapkan *single* ID untuk otentikasi.
 - f. Menerapkan dan mendokumentasikan standar konfigurasi (*port*, protokol, *service*) untuk semua sistem, seperti *operating system*, *software*/aplikasi.
 - g. Konfigurasi dan akun *default* selalu diubah sebelum digunakan secara menyeluruh dan terdokumentasi.
 - h. Membentuk Red Team dan Blue Team serta melakukan pengujian secara berkala dalam mengukur kesiapan organisasi untuk mengidentifikasi dan menghentikan serangan atau merespon dengan cepat dan efektif dari insiden keamanan yang terjadi.
 - i. Melakukan pemisahan environment antara sistem production dan development dan mengizinkan akses kepada pengembang dengan pengawasan.
 - j. Mengimplementasikan *software* anti virus dan anti *malware* secara terpusat dan selalu *update* terhadap perangkat *endpoint*.

- k. Menggunakan standar hardening configuration template pada database dan melakukan pengujian pada semua sistem (software) yang menjadi bagian penting dari proses bisnis organisasi.
- l. Membuat BCP dan DRP serta Kebijakan metode penghapusan data, Perlindungan data Pribadi dan kebijakan SMKI.
- m. Melakukan filterisasi lampiran pada aplikasi email dan menerapkan metode sandbox.
- n. Menerapkan dan mereviu secara berkala algoritma enkripsi dalam pengembangan *software*/aplikasi.
- o. Melakukan pelatihan keamanan informasi secara terjadwal untuk semua pegawai. Setidaknya untuk *sharing* secara menyeluruh terkait keamanan informasi kepada seluruh pegawai.
- p. Menyusun dan melaksanakan secara konsisten dan berkelanjutan program pemahaman kesadaran keamanan informasi untuk semua pegawai.
- q. Dokumentasi/diagram yang menggambarkan semua aliran data di seluruh sistem dan jaringan serta diperbaharui setiap ada aset baru.
- r. Menyusun proses formal yang dilakukan dalam manajemen terhadap perubahan dan pengujian semua perubahan konfigurasi *router*, *switch*, dan *firewall*.
- s. Seluruh pegawai agar mengetahui dan menerapkan kebijakan keamanan informasi di lingkungan kerja, serta memberikan kontribusi terhadap efektivitas sistem manajemen keamanan informasi.
- t. Melakukan gap analisis untuk memahami *skill* dan *behavior* yang tidak dimiliki oleh pegawai, dan menggunakan informasi tersebut untuk membuat roadmap terkait *baseline* pendidikan dan pelatihan terkait keamanan informasi.
- u. Menyusun kebijakan atau prosedur SDLC yang dapat dijadikan acuan dalam pengembangan aplikasi.
- v. Mengatur setiap akun pengguna atau sistem yang digunakan dalam melakukan *penetrating testing* dikontrol dan dipantau untuk memastikan bahwa akun

tersebut hanya digunakan untuk tujuan yang sah, dan dihapus atau dikembalikan ke fungsi normal setelah pengujian selesai dilakukan.

- w. Melakukan *threat hunting* secara berkala.
 - x. Membuat dokumentasi seluruh sistem dan jaringan.
2. Untuk meningkatkan aspek identifikasi, dapat dilakukan hal-hal sebagai berikut:
- a. Melakukan pembaharuan secara berkala dalam inventarisasi data aset (perangkat keras maupun lunak), disusun berdasarkan klasifikasi kritikalitas, memiliki penanggung jawab aset.
 - b. Melakukan secara berkala dalam perencanaan kapasitas secara berkala untuk memastikan bahwa semua aset perangkat dan aplikasi sesuai dengan kebutuhan.
 - c. Menerapkan *patch* keamanan pada semua perangkat keras dan perangkat lunak saat ada *update patch* yang sudah dirilis.
 - d. Membuat/memperbaharui *roadmap* keamanan TI organisasi dalam jangka waktu tertentu
 - e. Membuat Bisnis Impact Analysis terhadap perangkat dan aplikasi TI
 - f. Membuat pemeringkatan pada kerentanan yang teridentifikasi berdasarkan pedoman/standar/acuan organisasi.
 - g. Melakukan segmentasi jaringan berdasarkan fungsionalitas.
 - h. Melakukan analisa keterkaitan antara keamanan dan kenyamanan dari penggunaan aset perangkat dan aplikasi dalam rangka penyusunan standar keamanan informasi.
 - i. Melakukan pengelolaan data log keamanan informasi.
 - j. Melakukan klasifikasi terhadap *cyber threats* yang ditemukan.
 - k. Memastikan pegawai tidak menyimpan credentials di browser.
 - l. Melakukan vulnerability scanning dan/atau penetration testing terhadap semua aset perangkat dan aplikasi secara berkala.

3. Untuk meningkatkan aspek proteksi, dapat dilakukan hal-hal sebagai berikut:
 - a. Memiliki perangkat jaringan menggunakan otentikasi terpusat dan menerapkan DNS Filtering Services.
 - b. Menyimpan data *backup* telah dilindungi secara tepat, baik secara fisik maupun non fisik pada lokasi yang aman dan terenkripsi.
 - c. Log disimpan minimal 1 tahun sehingga akan mempermudah ketika dilakukan audit dan forensik.
 - d. Seluruh perangkat *endpoints* menggunakan antivirus, menerapkan web URL *filtering*, *device control*, *application control*, enkripsi dan membatasi fitur *autorun content*.
 - e. Menyusun kebijakan untuk memastikan penggunaan *password* yang kompleks untuk semua akses *login*, pergantian *password* secara berkala dan menggunakan/menambahkan verifikasi OTP.
 - f. Menerapkan IP *reputation* untuk memverifikasi alamat IP yang diizinkan dalam proses transaksi.
 - g. Menerapkan enkripsi pada media penyimpanan eksternal, dapat menggunakan software open source atau menggunakan aplikasi dari BSSN.
 - h. Melakukan enkripsi data pada saat disimpan.
 - i. Membatasi aplikasi yang diunduh, diinstal, dan dioperasikan oleh pegawai serta membatasi penggunaan scripting tools pada aplikasi.
4. Untuk meningkatkan aspek deteksi, dapat dilakukan hal-hal sebagai berikut:
 - a. Melaksanakan pemantauan akses fisik terhadap perangkat yang berada di dalam ruangan data *center*.
 - b. Menyusun *escalation profile* untuk setiap *security event* yang ditemukan.
 - c. Menyusun Metrik *Security Event*.
 - d. Mengimplementasikan SIEM, dapat menggunakan opensource seperti WAZUH (instalasi dapat dilihat pada website Gov-CSIRT).
 - e. Menerapkan *vulnerability scanning tools* secara otomatis menggunakan *agent*/aplikasi dan diinstal pada *endpoint*.

- f. Menerapkan *ticketing system* melacak kejadian berdasarkan tingkat keparahan/prioritas/dampak, kategori keamanan, dan jenis log yang berkorelasi untuk suatu kejadian.
 - g. Menerapkan *automated port scan* secara berkala terhadap semua sistem dan memberikan *alert*.
 - h. Mengadakan atau menganggarkan pelatihan terkait Cyber Threat Intelligence kepada personil untuk menjalankan fungsi CTI.
 - i. Menggunakan aplikasi maupun OS dengan lisensi yang *original* (tidak bajakan) dalam rangka menghindari kerentanan yang timbul pada aplikasi tidak berlisensi.
5. Untuk meningkatkan aspek respon, dapat dilakukan hal-hal sebagai berikut:
- a. Merencanakan skenario insiden dan melakukan latihan respon insiden secara rutin untuk pegawai yang terlibat dalam respon insiden.
 - b. Menyusun dokumen rencana respon insiden atau disaster recovery plan (DRP) dan standar operasional prosedur (SOP) penanganan insiden dan menjadwalkan revidi secara berkala.
 - c. Melakukan latihan respon insiden dan memberikan pelatihan kepada para personil tentang cara penanganan suatu insiden.
 - d. Memberikan pelatihan untuk pegawai tentang cara mengidentifikasi, penanganan, dan pelaporan suatu insiden keamanan informasi.
 - e. Mengadakan sumber daya redundan yang dapat langsung digunakan saat sistem penting/kritikal mengalami *down* karena insiden siber.
 - f. Melakukan revidi terhadap *root cause* dari suatu insiden siber serta rekap laporan insiden siber yang pernah terjadi.
 - g. Melakukan *scanning* ulang untuk memastikan bahwa kerentanan tersebut sudah ditutup ketika ditemukan kerentanan yang menyebabkan pelanggaran dan telah dilakukan *patching*.



- h. Rekaman insiden dan pelanggaran disimpan dan dilaporkan berdasarkan *trends* insiden dalam jangka waktu tertentu, dapat dalam bentuk laporan bulanan, triwulanan, semester maupun tahunan.
- i. Menyusun SLA (Service Level Agreement) dalam penanganan insiden.
- j. Hasil revidu terhadap rekap laporan insiden siber dapat dilaporkan ke top management.

PENUTUP

Demikian Laporan Penilaian CSM pada Dinas Komunikasi dan Informatika Provinsi Bengkulu ini disusun, sebagai bahan pengambilan keputusan pimpinan dalam pelaksanaan pengamanan siber pada Pemprov Bengkulu. Agar Pemprov Bengkulu melaksanakan tindak lanjut atas hasil observasi dan rekomendasi yang disampaikan pada Laporan Penilaian CSM ini dan melaporkan tindak lanjutnya kepada BSSN.

Laporan Penilaian CSM ini disusun rangkap 4 (empat) untuk disampaikan kepada :

1. Kepala Badan Siber dan Sandi Negara;
2. Gubernur Provinsi Bengkulu; dan
3. Sekretaris Daerah Provinsi Bengkulu; dan
4. Kepala Dinas Komunikasi dan Informatika Provinsi Bengkulu.

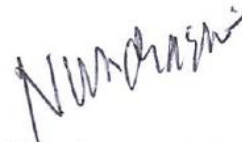
Bengkulu, 14 Juli 2022

Sandiman Madya pada Direktorat Keamanan
Siber dan Sandi Pemerintah Daerah

Sub Koordinator
Tata Kelola Persandian



Isweldi, S.Sos
NIP. 19750511 200502 1 003



Nurchaerani, S.E.
NIP. 19650708 198710 2 003

Mengetahui,

Kepala Bidang Statistik dan Persandian
Dinas Komunikasi, Informatika dan Statistik
Provinsi Bengkulu



Tanti Nasilva, S.Sos.
NIP. 19701115 199203 2 004