2022

LAPORAN

HASIL PENILAIAN

CYBER SECURITY MATURITY (CSM)

DINAS KOMUNIKASI INFORMATIKA PERSANDIAN DAN STATISTIK PROVINSI KALIMANTAN TENGAH

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, Informatika, Persandian dan Statistik Provinsi Kalimantan Tengah. 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:

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

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 25 Juli 2022.

2. Validasi Penilaian CSM

   BSSN melakukan validasi pengisian instrumen CSM pada tanggal 1 s.d. 3 Agustus 2022, dengan cara diskusi dengan perwakilan tim Diskominfosantik Provinsi Kalimantan Tengah. Tim BSSN yang terlibat:

   1) Nurchaerani, S.E.
   2) Irma Nurfitri Handayani, S.ST.
   3) Ikrima Galuh Nasucha, S.Tr.Tp.
   4) Ni Putu Ayu Lhaksmi Wulansari, S.Tr.TP.

HASIL KEGIATAN

I. Informasi *Stakeholder*

Nama Instansi/Lembaga : Dinas Komunikasi Informatika Persandian dan Statistik Provinsi Kalimantan Tengah

Alamat : Jl. Tjilik Riwut KM 3,5 No.18 A, Palangkaraya, Kalteng

Nomor Telp./Fax. : -

Email : diskominfo@kalteng.go.id

Narasumber Instansi/Lembaga :

1. Billy Bareto, S.T.
2. Nursinta Uli Situmorang, S.H.
3. Marlin Pakondo, S.E., M.Si.
4. Ashadi Noor, S.Kom.
5. Gayus Zuarin, S.H.
6. Ari Gunadi Palilu, S.Kom., M.T.
7. Restiasih Pratiwi, S.T.
8. Ivan Oktobrian, S.Kom.

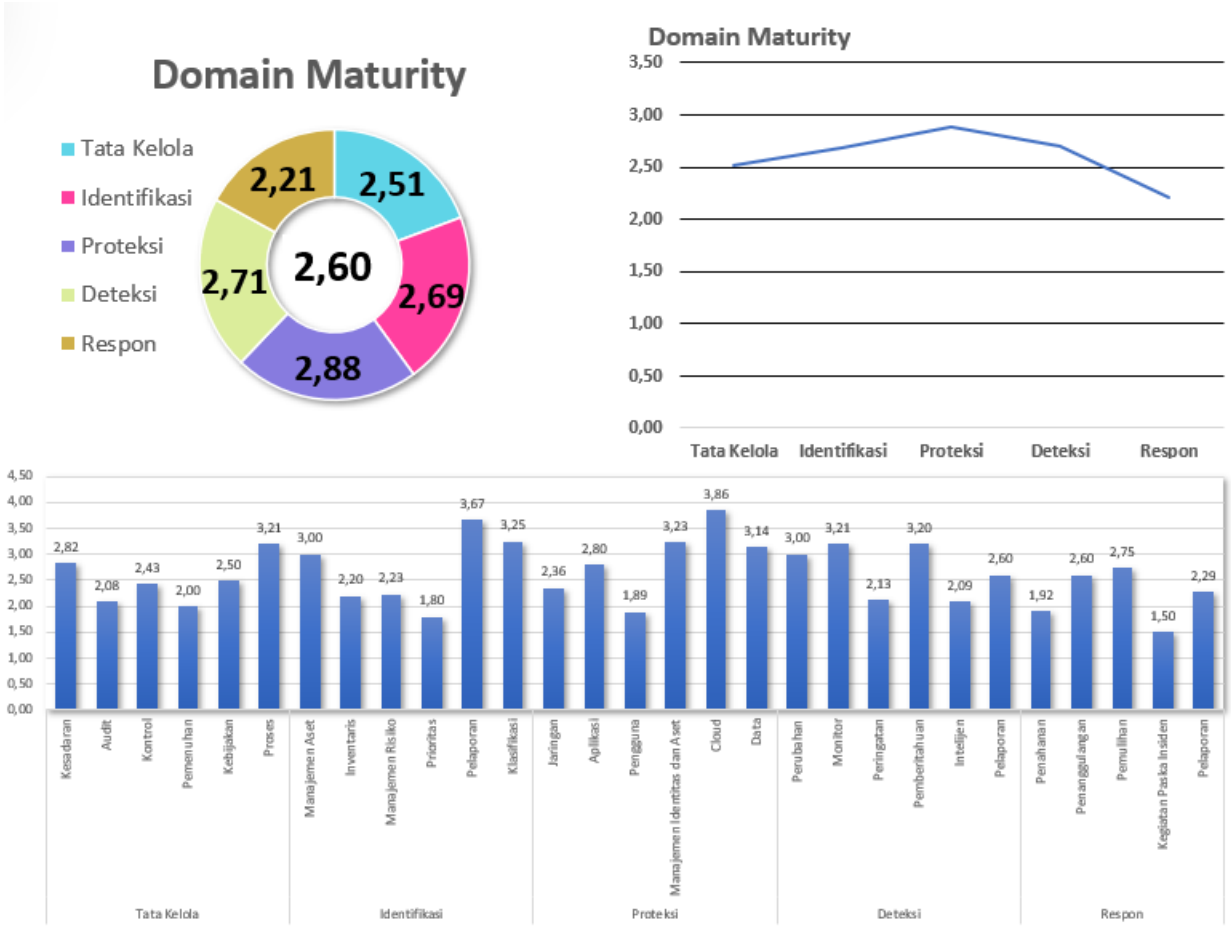
II. Deskripsi Ruang Lingkup Penilaian

1. Ruang Lingkup Penilaian :

   ☐ Organisasi Keseluruhan ☐ Regional, Kanwil, Cabang √ Unit Kerja ☐ Lainnya

2. Instansi/Unit Kerja : Dinas Komunikasi Informatika Persandian dan Statistik Provinsi Kalimantan Tengah

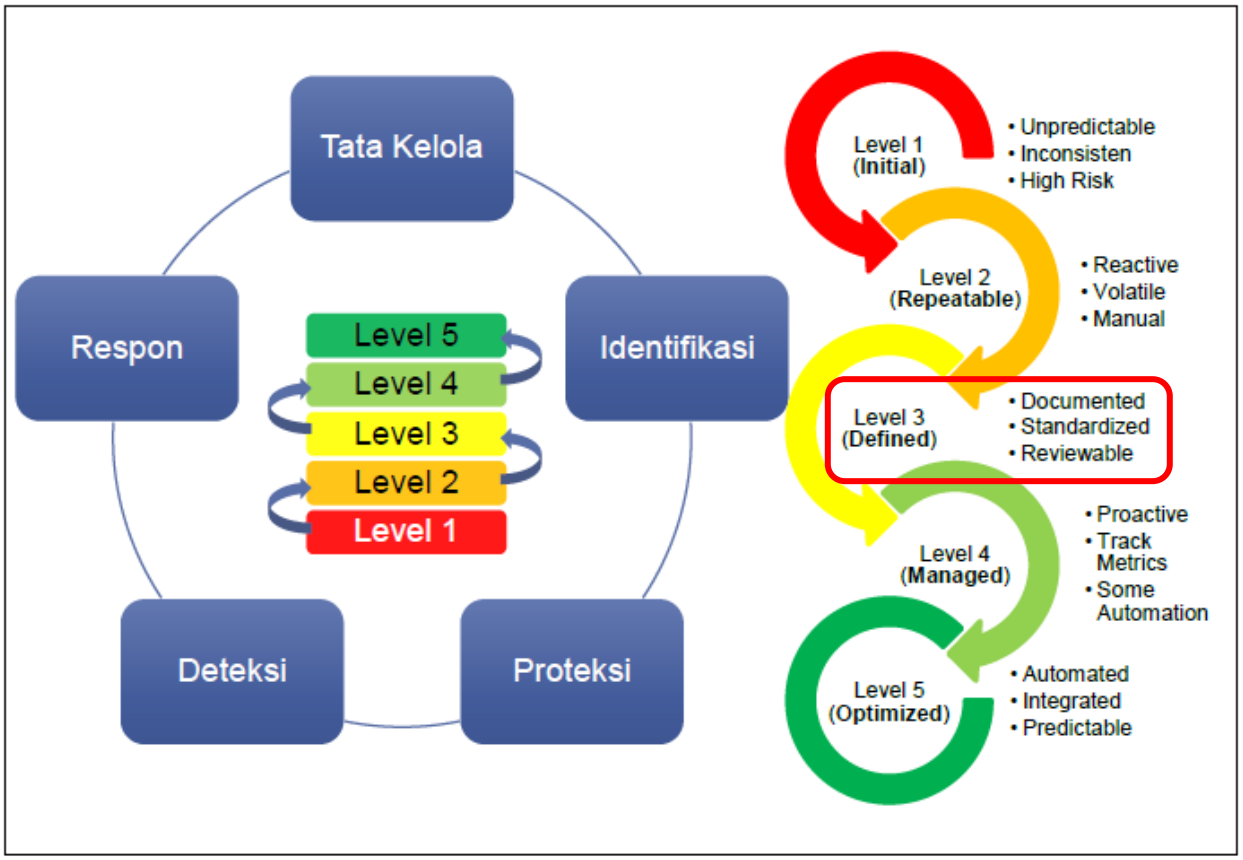
III. Hasil Penilaian CSM



Gambar 1. Hasil Penilaian CSM

Berdasarkan hasil penilaian instrumen CSM, diperoleh hasil sebagai berikut **Total Score Indeks Kematangan : 2,60,** sehingga perhitungan penentuan Level Kematangan didapatkan level kematangan sebagai berikut:

Level Kematangan Tingkat 3



Gambar 2. Capaian Level Kematangan

Level Kematangan 3:

Level kematangan 3 menunjukkan bahwa pengelolaan keamanan siber di Dinas Komunikasi Informatika Persandian dan Statistik Provinsi Kalimantan Tengah 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. Telah menjalankan program pemahaman kesadaran keamanan informasi bagi karyawan dan juga stakeholder yang dipublikasikan melalui media sosial.
2. Melakukan pemeriksaan *background* untuk semua karyawan baru.
3. Menerapkan kontrol kriptografi sesuai dengan peraturan yang berlaku.
4. Menerapkan perlindungan sesuai dengan persyaratan dan peraturan terhadap dokumentasi yang dimiliki organisasi.
5. Menerapkan filterisasi pada email dinas.
6. Konfigurasi dan akun default selalu diubah sebelum digunakan, namun belum terdokumentasi.

Identifikasi

1. Melakukan perencanaan kapasitas secara berkala untuk memastikan bahwa pengadaan semua aset perangkat dan aplikasi dilakukan sesuai dengan kebutuhan melalui perencanaan pengadaan setiap tahun.
2. Menerapkan segmentasi jaringan berdasarkan fungsionalitas.
3. Melakukan inventarisasi data aset perangkat keras.
4. Menerapkan patch keamanan pada semua perangkat keras dan perangkat lunak saat ada update patch yang sudah dirilis.
5. Organisasi sudah memiliki metode atau standar untuk klasifikasi informasi, namun belum terinventarisasi.
6. Aspek keamanan menjadi pertimbangan dan diprioritaskan dalam semua pengambilan keputusan TI, kapasitas server dan perangkat jaringan.

Proteksi

1. Memiliki Next Generation Firewall (Fortigate).
2. Menerapkan sistem enkripsi pada akses nirkabel.
3. Melakukan backup data dan log secara berkala.

4. Email system memiliki pengecekan otomatis terhadap spam/phising/malware.
5. Master images tersimpan pada server yang dikonfigurasi secara aman.

Deteksi

1. Mengaktifkan Enable Detailed Logging yang mencakup informasi terperinci.
2. Organisasi menjamin alokasi kapasitas penyimpanan log sesuai kebutuhan.
3. Melakukan pemantauan akses fisik terhadap perangkat yang berada di dalam ruangan data center.
4. Memiliki ticketing system.
5. Memiliki contact tree untuk mengeskalasi dalam merespon suatu kejadian.

Respon

1. Tim respon insiden memiliki kemampuan dalam mendeteksi insiden, analisis dan memberikan rekomendasi penanganan.
2. Memiliki form pelaporan insiden.
3. Memiliki daftar kontak tim penanganan insiden internal dan eksternal.
4. Ketika mengalami insiden siber, tim respons insiden dapat dengan cepat mendapat bantuan dari tim manajemen krisis namun sulit mendapatkan informasi dari pihak ketiga.
5. Laporan insiden di organisasi dilaporkan ke pimpinan dan ke pihak eksternal yang berkepentingan/wajib dilaporkan sesuai regulasi.

V. Kelemahan/Kekurangan

Tata Kelola

1. Belum seluruh karyawan mengetahui dan menerapkan kebijakan keamanan informasi.
2. Belum melakukan internal audit keamanan informasi secara berkala.
3. Belum melakukan gap analisis terkait skill dan behavior karyawan.

4. Belum membuat roadmap baseline pendidikan dan pelatihan terkait keamanan informasi.
5. Karyawan belum mendapat pelatihan mengenai kewajiban menjaga data privasi dan melindungi data sensitif stakeholder.
6. Belum pernah melakukan simulasi phishing.
7. Personil yang terlibat dalam pengembangan software belum mendapatkan pelatihan mengenai secure coding.
8. Belum memiliki kebijakan perlindungan data pribadi.
9. Belum melakukan security risk assessment serta reviu.
10. Belum menyusun risk treatment dan melakukan reviu terhadap risk treatment secara berkelanjutan.
11. Belum melakukan reviu izin akses dari akun pengguna secara periodik (setiap tiga bulan).
12. Belum membuat persyaratan keamanan informasi terkait akses supplier terhadap aset organisasi.
13. Belum menetapkan program untuk vulnerability assessment secara berkala.
14. Belum melakukan vulnerability assessment secara mandiri.
15. Belum memiliki Red Team dan Blue Team.
16. Belum menerapkan firewall aplikasi web (WAFs).
17. Belum menerapkan metode sandbox terhadap seluruh lampiran email.
18. Belum memiliki BCP (Business Continuity Plan) dan DRP (Disaster Recovery Plan).
19. Otentikasi menggunakan single ID unik belum diatur.
20. Belum melakukan pemisahan environment antara sistem production dan development.
21. Belum mengimplementasikan software anti virus dan anti malware secara terpusat dan selalu update terhadap perangkat endpoint.

Identifikasi

1. Belum mendokumentasikan proses dan prosedur untuk manajemen patch semua aset perangkat dan aplikasi.
2. Belum memiliki system configuration management tools otomatisasi konfigurasi perangkat keras dan perangkat lunak.
3. Belum menyusun risk register untuk seluruh aset.
4. Business Impact Analysis terhadap perangkat dan aplikasi TI belum disusun.
5. Identifikasi aset belum disusun berdasarkan klasifikasi kritikalitas dan belum ada penetapan terkait penanggungjawab untuk setiap aset tersebut.
6. Belum ada dokumentasi mengenai alur informasi yang memproses data stakeholder termasuk yang dikelola oleh pihak ketiga.
7. Standar terkait klasifikasi aset TI dan klasifikasi terhadap cyber threat belum disusun.
8. Belum dilakukan identifikasi dan pembatasan akses perangkat yang tidak diizinkan oleh organisasi.
9. Belum ada kebijakan pembatasan penggunaan aset organisasi untuk kepentingan pribadi.
10. Dokumentasi mengenai alur informasi yang memproses data stakeholder termasuk yang dikelola oleh pihak ketiga belum ada.
11. Roadmap keamanan TI organisasi belum ada.

Proteksi

1. Belum menerapkan Multi-Factor Authentication (MFA) untuk mengakses data sensitif dan akses jaringan.
2. Perangkat jaringan belum menerapkan otentikasi terpusat.
3. Organisasi belum menerapkan port access control sebagai pengendalian terhadap otentikasi perangkat yang dapat terhubung ke jaringan.
4. Organisasi belum mengatur terkait pembatasan fitur wireless, penerapan disable peer-to-peer pada wireless client, penerapan DNS filtering services dan belum ada

pembatasan terkait aplikasi yang diperbolehkan untuk diunduh, diinstal dan dioperasikan.

5. Belum ada kebijakan terkait pembatasan penggunaan scripting tools.
6. Belum memanfaatkan metode otentikasi pada saluran yang terenkripsi dan juga penambahan OTP.

Deteksi

1. Perubahan konfigurasi pada peralatan jaringan belum terdeteksi secara otomatis.
2. Belum memiliki mekanisme monitoring terhadap akses pengguna, koneksi jaringan, perangkat keras dan perangkat lunak, akses dan perubahan pada data sensitive, monitoring dan deteksi terhadap penggunaan enkripsi yang tidak sah.
3. Belum memiliki sistem untuk monitoring dan mencegah kehilangan data sensitif.
4. Belum ada mekanisme monitoring aktivitas pihak ketiga yang dilakukan di organisasi.
5. Belum memiliki SOC atau manajemen teknis yang dapat dihubungi setiap saat (24x7) untuk menangani kejadian dengan prioritas tinggi dan kritikal.
6. Organisasi belum menjalankan vulnerability scanning tools secara otomatis menggunakan agent/aplikasi yang diinstal pada endpoint.
7. Belum melakukan *record* seperti Change Advisory Board (CAB) yang meninjau dan menyetujui semua perubahan konfigurasi.
8. Belum memiliki mekanisme *monitoring* terhadap akses dan perubahan pada data *sensitive*.
9. Unit dalam organisasi belum menjalankan fungsi Cyber Threat Intelligence (CTI).
10. Organisasi belum memiliki Metrik Security Event.
11. Belum mengoperasionalkan SIEM atau Log Analytics Tools.
12. Belum memiliki perangkat anti malware yang secara otomatis melakukan scanning terhadap removable media yang terhubung ke perangkat.
13. Belum membuat escalation profile untuk setiap security event yang ditemukan.

14. Belum memiliki sistem untuk melakukan Malicious Code Detection untuk melindungi dari malicious code.
15. Mekanisme sharing informasi hasil deteksi belum ada.

Respon

1. Belum memiliki kebijakan penanganan insiden dan selaras dengan kebijakan pengaturan kesinambungan organisasi atau business continuity planning (BCP).
2. Belum memiliki dokumen rencana respon insiden atau disaster recovery plan (DRP) dan standar operasional prosedur (SOP) terkait pelaporan hingga paska penanganan insiden.
3. Belum merencanakan skenario insiden dan melakukan latihan respon insiden secara rutin untuk pegawai yang terlibat dalam respon insiden.
4. Tim respon insiden belum melakukan pencatatan langkah-langkah penanggulangan insiden menggunakan format baku.
5. Belum mendesain jaringan terlindungi dari akses tidak sah penyerang apabila server DMZ terkena serangan.
6. Belum menerapkan mekanisme backup data karyawan ke cloud organisasi.
7. Belum memiliki sumber daya redundan yang dapat langsung digunakan dan menjadi cadangan apabila sumber daya utama sedang tidak dapat beroperasi atau terkena serangan.
8. Belum memiliki SLA (Service Level Agreement) dalam penanganan insiden.
9. Belum memiliki mekanisme pelaporan anomali atau insiden siber dari karyawan maupun stakeholder kepada tim penanganan insiden siber organisasi.

VI. Rekomendasi

1. Untuk meningkatkan aspek tata kelola di lingkungan Diskominfosantik Provinsi Kalteng maka dapat dilakukan hal-hal sebagai berikut:
   a. Meningkatkan kegiatan program pemahaman kesadaran keamanan informasi dengan fokus/isu baik terkait dengan kebijakan yang telah ditetapkan

(kebijakan keamanan informasi atau kebijakan mengenai data pribadi) maupun permasalahan keamanan informasi yang perlu dilakukan secara berkelanjutan.

b. Mendokumentasikan standar konfigurasi (*port*, protokol, *service*) untuk semua sistem, seperti *operating system, software*/aplikasi.
c. Melakukan dan menyusun gap analisis terkait skill dan behavior karyawan yang nantinya dijadikan roadmap baseline pendidikan dan pelatihan terkait keamanan informasi.
d. Mengadakan atau mengalokasikan kegiatan latihan respon insiden, simulasi phising dan pelatihan secure coding untuk personil yang terlibat dalam pengembangan software.
e. Menyusun kebijakan perlindungan data pribadi.
f. Melaksanakan risk assessment secara berkala.
g. Menyusun risk treatment dan melakukan reviu terhadap risk treatment secara berkelanjutan.
h. Menerapkan mekanisme reviu izin akses dari akun pengguna secara periodik (setiap tiga bulan).
i. Menyusun persyaratan keamanan informasi terkait akses supplier terhadap aset organisasi.
j. Melaksanakan kegiatan vulnerability scanning secara berkala terhadap sistem/aplikasi yang dikelola.
k. Membentuk Red Team dan Blue Team.
l. Menerapkan firewall aplikasi web (WAFs).
m. Menerapkan metode sandbox terhadap seluruh lampiran email.
n. Menyusun BCP (Business Continuity Plan) dan DRP (Disaster Recovery Plan).
o. Menyusun kebijakan terkait otentikasi menggunakan single ID unik.

2. Untuk meningkatkan aspek identifikasi, dapat dilakukan hal-hal sebagai berikut:
    a. Melakukan identifikasi aset (perangkat keras, perangkat lunak) dan di inventaris yang disusun berdasarkan klasifikasi kritikalitas dan mencantumkan penanggungjawab untuk setiap aset yang diinventaris.
    b. Menyusun proses dan prosedur untuk *manajemen patch* semua aset perangkat dan aplikasi.
    c. Menerapkan system configuration management tools untuk otomatisasi konfigurasi perangkat keras dan perangkat lunak.
    d. Melakukan risk assessment secara berkala, mereviu dan menyusun risk register untuk seluruh aset yang dikelola.
    e. Menyusun Business Impact Analysis terhadap perangkat dan aplikasi TI.
    f. Menyusun alur informasi yang memproses data stakeholder termasuk yang dikelola oleh pihak ketiga.
    g. Menyusun standar terkait klasifikasi aset TI dan klasifikasi terhadap cyber threat.
    h. Melakukan identifikasi dan membuat mekanisme atau kebijakan terkait pembatasan akses perangkat yang tidak diizinkan oleh organisasi.
    i. Menyusun roadmap keamanan TI organisasi.

3. Untuk meningkatkan aspek proteksi, dapat dilakukan hal-hal sebagai berikut:
    a. Mengatur dan membuat kebijakan terkait retensi log.
    b. Menerapkan Multi-Factor Authentication (MFA) untuk mengakses data sensitif dan akses jaringan serta penambahan OTP untuk otentikasi.
    c. Menerapkan otentikasi terpusat, menerapkan port access control sebagai pengendalian terhadap otentikasi perangkat yang dapat terhubung ke jaringan.
    d. Membuat pengaturan terkait pembatasan fitur wireless, penerapan disable peer-to-peer pada wireless client, penerapan DNS filtering services dan pembatasan terkait aplikasi yang diperbolehkan untuk diunduh, diinstal dan dioperasikan.

e. Menyusun kebijakan terkait pembatasan penggunaan scripting tools.
f. Menerapkan IP reputation untuk memverifikasi alamat IP yang diizinkan dalam proses transaksi.
g. Mempertimbangkan faktor keamanan pada data stakeholder / klien / konsumen / pelanggan yang dikirim yaitu dengan menerapkan enkripsi saat dikirim.

4. Untuk meningkatkan aspek deteksi, dapat dilakukan hal-hal sebagai berikut:
   a. Menerapkan deteksi secara otomatis terhadap perubahan konfigurasi pada peralatan jaringan.
   b. Menyusun mekanisme monitoring terhadap akses pengguna, koneksi jaringan, perangkat keras dan perangkat lunak, akses dan perubahan pada data sensitive, monitoring dan deteksi terhadap penggunaan enkripsi yang tidak sah.
   c. Menerapkan sistem untuk monitoring dan mencegah kehilangan data sensitif.
   d. Menyusun mekanisme monitoring aktivitas pihak ketiga yang dilakukan di organisasi.
   e. Menerapkan SOC atau manajemen teknis yang dapat dihubungi setiap saat (24x7) untuk menangani kejadian dengan prioritas tinggi dan kritikal.
   f. Menerapkan vulnerability scanning tools secara otomatis menggunakan agent/aplikasi yang diinstal pada endpoint.
   g. Menyusun *escalation profile* untuk setiap *security event* yang ditemukan.
   h. Menjalankan fungsi Cyber Threat Intelligence (CTI).
   i. Menyusun metrik security event.
   j. Mengimplementasikan SIEM, dapat menggunakan opensource seperti WAZUH (instalasi dapat dilihat pada website Gov-CSIRT).
   k. Menerapkan perangkat anti malware yang secara otomatis melakukan scanning terhadap removable media yang terhubung ke perangkat.
   l. Menerapkan sistem untuk melakukan Malicious Code Detection untuk melindungi dari malicious code.

m. Menyusun mekanisme untuk sharing informasi hasil deteksi ke karyawan ataupun stakeholder.
n. Menyusun laporan periodik terkait kondisi keamanan siber terkini dan melaporkan atau menyampaikan ke top level management.

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 reviu secara berkala.
   c. Melakukan latihan respon insiden dan memberikan pelatihan kepada para personil tentang cara penanganan suatu insiden.
   d. Tim respon insiden selalu melakukan pencatatan langkah-langkah penanggulangan insiden menggunakan format baku.
   e. Mendesain jaringan terlindungi dari akses tidak sah penyerang apabila server DMZ terkena serangan.
   f. Menerapkan cloud organisasi dan karyawan melakukan backup data dari perangkat yang digunakan ke cloud organisasi.
   g. Menerapkan sumber daya redundan yang dapat langsung digunakan dan menjadi cadangan apabila sumber daya utama sedang tidak dapat beroperasi atau terkena serangan.
   h. Melakukan *scanning* ulang untuk memastikan bahwa kerentanan tersebut sudah ditutup ketika ditemukan kerentanan yang menyebabkan pelanggaran dan telah dilakukan *patching*.
   i. Menyusun SLA (Service Level Agreement) dalam penanganan insiden.
   j. Menyusun mekanisme pelaporan anomali atau insiden siber dari karyawan maupun stakeholder kepada tim penanganan insiden siber organisasi.

k. Rekaman insiden dan pelanggaran disimpan dan dilaporkan berdasarkan *trends* insiden dalam jangka waktu tertentu, dapat dalam bentuk laporan bulanan, triwulanan, semester maupun tahunan.

PENUTUP

Demikian Laporan Penilaian CSM pada Dinas Komunikasi Informatika Persandian dan Statistik Provinsi Kalimantan Tengah ini disusun, sebagai bahan pengambilan keputusan pimpinan dalam pelaksanaan pengamanan siber pada Pemprov Kalimantan Tengah. Agar Pemprov Kalimantan Tengah 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 3 (tiga) untuk disampaikan kepada:

1. Kepala Badan Siber dan Sandi Negara;
2. Gubernur Provinsi Kalimantan Tengah;
3. Sekretaris Daerah Provinsi Kalimantan Tengah.

Palangkaraya, 3 Agustus 2022

Kepala Bidang Persandian	Sandiman Madya pada Direktorat Keamanan Siber dan Sandi Pemerintah Daerah
Telah ditandatangani secara elektronik oleh : BILLY BARETO, ST Penata Tingkat I NIP. 197611232006041005	Ditandatangani secara elektronik oleh: Nurchaerani NIP. 196507081987102003 Sandiman Madya pada Direktorat Keamanan Siber dan Sandi Pemda
Billy Bareto, S.T.	Nurchaerani, S.E.
NIP. 19761123 200604 1 006	NIP. 19650708 198710 2 003

Mengetahui,

Kepala Dinas Komunikasi Informatika

Persandian dan Statistik Provinsi Kalimantan Tengah

Telah ditandatangani secara elektronik oleh :

AGUS SISWADI
Pembina Tingkat I
NIP. 196802041999031007

Agus Siswadi

NIP. 19680204 199903 1 007