2021

LAPORAN

HASIL PENILAIAN

CYBER SECURITY MATURITY (CSM)

DINAS KOMUNIKASI DAN INFORMATIKA
PROVINSI JAMBI

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 Jambi. 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:

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 Oktober – November 2021.

2. Validasi Penilaian CSM

   BSSN melakukan validasi pengisian instrumen CSM pada tanggal 24 dan 25 November 2021, dengan cara diskusi dengan perwakilan tim Diskominfo Provinsi Jambi. Tim BSSN yang terlibat:

   1) Marcelina Tri Nasiti Widayatmi, S.Sos.,M.Si (Han).
   2) Irma Nurfitri Handayani, S.ST.
   3) Diah Sulistyowati, S.Kom.
   4) Mochamad Jazuly, S.S.T.TP.

HASIL KEGIATAN

I. Informasi *Stakeholder*

Nama Instansi/Lembaga : Dinas Komunikasi dan Informatika Provinsi Jambi
Alamat : Jl. A Yani No.1, Telanaipura, Jambi
Nomor Telp./Fax. : (0741) 66269
Email : diskominfo@jambiprov.go.id
Narasumber Instansi/Lembaga :

1. Moch. Mawardi, S.I.P. (Kasi Pengawasan dan Evaluasi Penyelenggaraan Persandian)
2. Epa Susanti, S.E. (Kasi Tata Kelola Operasional Persandian)
3. Fransisco (Analis Deteksi Kerentanan Siber)
4. Dika Heraditama, S.Kom (Tenaga Ahli IT)
5. Nur Hamid, S.Kom (Tenaga Ahli IT)

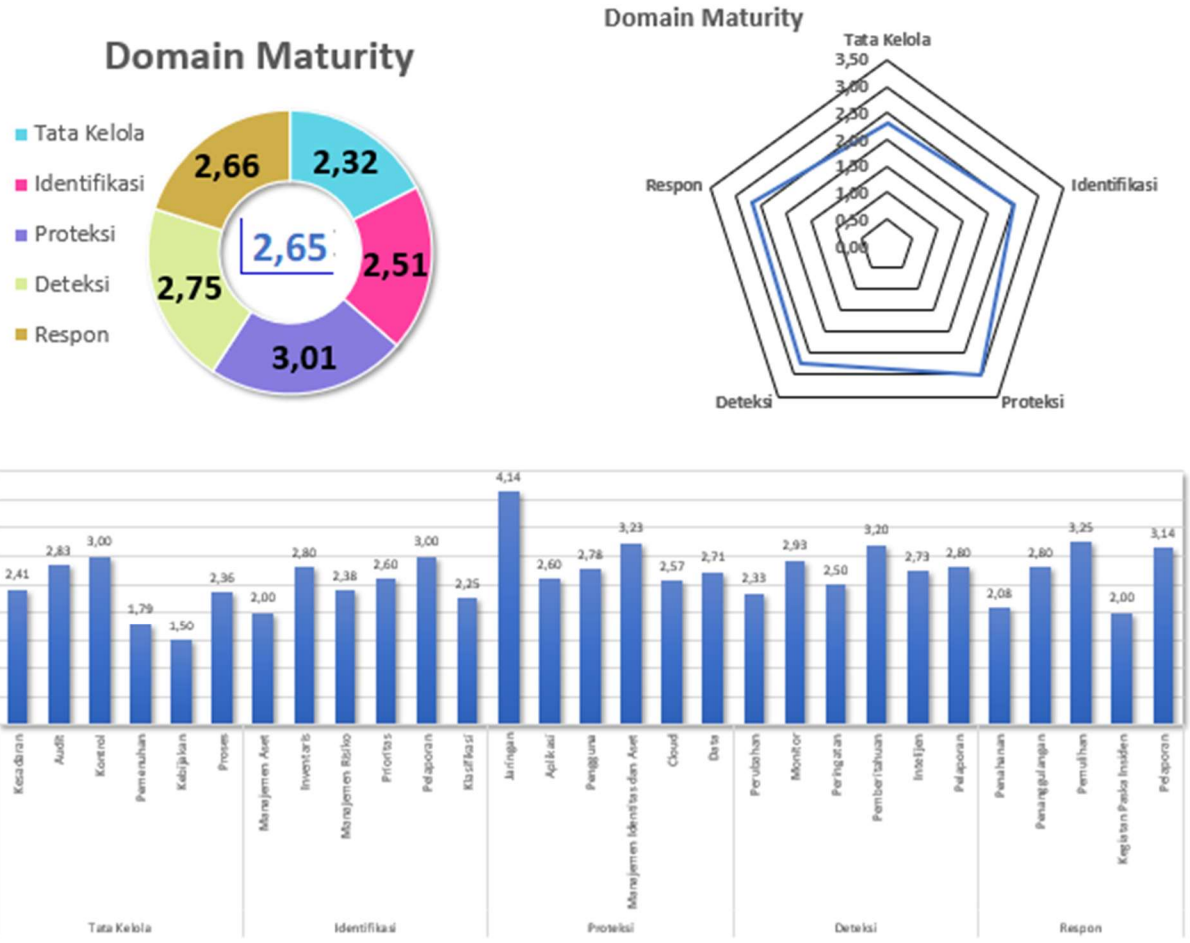
II. Deskripsi Ruang Lingkup Penilaian

1. Ruang Lingkup Penilaian :

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

2. Instansi/Unit Kerja* : Dinas Komunikasi dan Informatika Provinsi Jambi

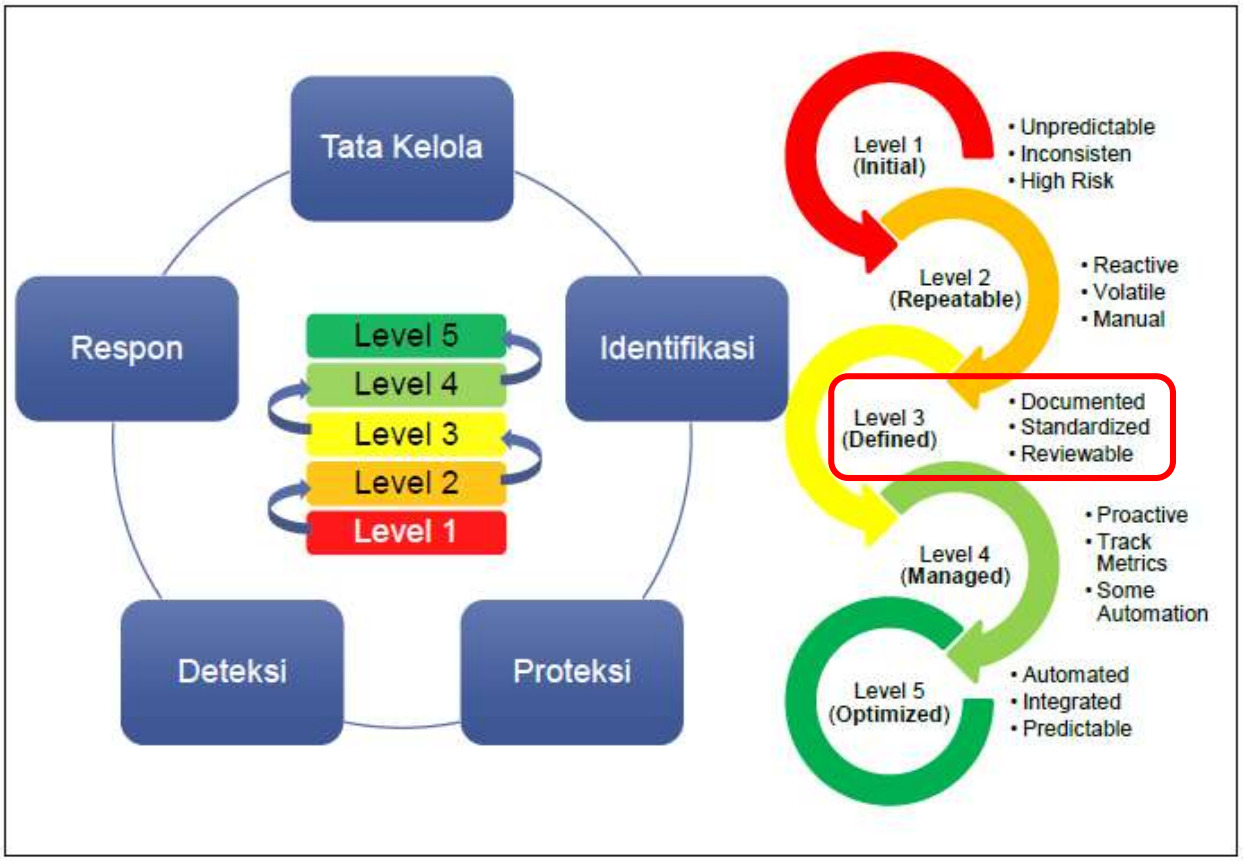
III. Hasil Penilaian CSM



Gambar 1. Hasil Penilaian CSM

Berdasarkan hasil penilaian instrumen CSM, diperoleh hasil sebagai berikut **Total Score Indeks Kematangan : 2,68,** 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 dan Informatika Provinsi Jambi sudah sudah terorganisir 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. Melakukan internal audit keamanan informasi setiap 1 tahun sekali.
2. Adanya prosedur untuk menambah / mengubah / menghapus hak akses ketika terjadi perpindahan pegawai, meskipun masih atas permintaan atasan/ lainnya.
3. Melindungi aplikasi web organisasi menggunakan *firewall* aplikasi web (WAFs).
4. Mengaktifkan secara *default firewall* atau perlindungan yang sejenis berjalan di semua perangkat komputasi *end user*, meskipun pengguna dapat mengonfigurasi, mengaktifkan dan menonaktifkan aplikasi.
5. Seluruh alamat IP internal dilindungi oleh NAT (Network Addresss Translation).
6. Jaringan internal dan jaringan perimeter, diperbarui secara regular dengan *threat intelligence*.
7. Menggunakan DLP (Data Loss Prevention) atau NAC (Network Access Control).
8. Menerapkan dan mendokumentasikan standar konfigurasi (*port, protokol, service*) untuk semua sistem, seperti *operating system, software*/aplikasi, meskipun belum terdokumentasi seluruhnya.
9. Konfigurasi dan akun *default* selalu diubah sebelum digunakan, meskipun belum terdokumentasi seluruhnya.
10. Telah menggunakan algoritma enkripsi dalam pengembangan *software*/aplikasi, meskipun belum direviu secara berkala.
11. Telah melakukan pemeriksaan latar belakang dilakukan untuk semua pegawai baru.
12. Dalam pengembangan *software*/aplikasi, personel yang terlibat dalam pengembangan *software*/aplikasi telah mendapatkan pelatihan dalam membuat *secure code* yang baik.
13. Seluruh dokumentasi yang dimiliki organisasi dilindungi dan dijaga agar tidak hilang, hancur, dipalsukan, diakses oleh pihak yang tidak sah sesuai dengan persyaratan perundang-undangan, peraturan, dan kontrak.
14. Memiliki program pemahaman kesadaran keamanan informasi untuk semua pegawai dalam rangka memastikan mereka memahami serta menunjukkan *behavior* dan *skill*

yang diperlukan untuk memastikan keamanan informasi, meskipun belum dilakukan secara berkelanjutan.

15. Telah melakukan proses *security risk assessment*, namun belum secara berkala dan berkelanjutan.
16. Memiliki dokumentasi/diagram yang menggambarkan semua aliran data di seluruh sistem dan jaringan serta diperbaharui setiap tahunnya.
17. Melakukan manajemen kerentanan siber dan mitigasi terhadap kerentanan, meskipun belum secara konsisten dilakukan.
18. Dapat menggunakan *tool vulnerability scanning* secara mandiri, yang mana hasil *vulnerability assessment* digunakan sebagai titik awal dalam melakukan *penetrating testing*.
19. Menetapkan program untuk *vulnerability assessment* atau *penetrating testing* secara berkala kepada aplikasi web, aplikasi *client-based*, aplikasi mobile, *wireless*, server dan perangkat jaringan.

Identifikasi

1. Aspek keamanan menjadi pertimbangan dan diprioritaskan dalam semua pengambilan keputusan TI, kapasitas server dan perangkat jaringan.
2. Melakukan inventarisasi data aset (perangkat keras maupun lunak), disusun berdasarkan klasifikasi kritikalitas, memiliki penanggung jawab aset, meskipun belum secara konsisten dilakukan.
3. Melakukan identifikasi dan membatasi akses perangkat yang tidak diizinkan, meskipun belum melakukan pembatasan akses
4. Pihak ketiga tidak diizinkan untuk menggunakan aset mereka pada jaringan dan dikontrol dengan menggunakan NAC (network access control).
5. Memiliki metode/ standar untuk klasifikasi data dan aset TI, namun belum direviu secara berkala.

6. Melakukan perencanaan kapasitas secara berkala untuk memastikan bahwa semua aset perangkat dan aplikasi sesuai dengan kebutuhan, meskipun belum secara berkala.
7. Menerapkan *patch* keamanan secara manual pada semua perangkat keras dan perangkat lunak saat ada *update patch* yang sudah dirilis, meskipun belum secara konsisten dilakukan.

Proteksi

1. Semua data penting di-*backup* secara berkala dan dilakukan secara otomatis.
2. Melakukan pengujian data *integrity* secara berkala terhadap data yang di *backup* dengan melakukan *restore* data, meskipun tidak konsisten dan dalam kondisi tertentu.
3. Menyimpan data *backup* telah dilindungi secara tepat, baik secara fisik maupun non fisik pada lokasi yang aman, meskipun belum dienkripsi.
4. Menerapkan pembatasan akun pada laptop/PC milik organisasi yang digunakan untuk aktivitas tertentu seperti: *browsing* internet, email, akses ke sosial media, transfer *file* via media eksternal.
5. *Identity and access management systems* digunakan untuk seluruh *operating system*.
6. Menerapkan pengguna selain admin *database* hanya memiliki akses *read-only* pada akses ke *database*.
7. Telah menggunakan informasi identitas dan akses pengguna untuk membatasi hak akses dari dalam jaringan.
8. Menerapkan metode otentikasi melalui saluran terenkripsi.
9. Menerapkan *whitelist* aplikasi untuk memastikan bahwa hanya *authorized software library* dan *signed script* yang dapat dijalankan oleh sistem.
10. Menggunakan Next Generation Endpoint Protection.

11. Setiap koneksi ke perangkat server dan jaringan telah menggunakan protokol terenkripsi seperti SSH, *secure* RDP, dll dan menerapkan otentikasi terpusat pada seluruh perangkat jaringan.
12. Mengaktifkan *firewall* atau ACL untuk mengimplementasikan *implicit or explicit deny any/any rule*.
13. Seluruh *traffic outbond* hanya diizinkan sesuai dengan kebutuhan organisasi.
14. Firewall, IPS dan IDS secara umum telah dikonfigurasi semaksimal mungkin untuk memblokade ancaman dari dalam maupun dari luar jaringan.
15. Memiliki kemampuan untuk melacak dan dapat mendeteksi perilaku anomali transaksi dan melakukan identifikasi perangkat yang digunakan.
16. Akses nirkabel telah dikonfigurasikan dengan menggunakan sistem enkripsi.

Deteksi

1. Memiliki perangkat *anti-malware* yang secara otomatis melakukan *scanning* terhadap removable media yang terhubung ke perangkat.
2. Dapat mendeteksi Wireless Access Point yang terhubung ke jaringan LAN (ethernet).
3. Setiap perubahan konfigurasi pada peralatan jaringan terdeteksi secara otomatis.
4. Memiliki *contact tree* untuk mengeskalasi dalam merespons suatu kejadian.
5. Telah menerapkan dan pengelolaan sistem *loging*, namun belum terpusat.
6. Dapat mendeteksi aktivitas anomali login seperti waktu, lokasi, durasi, dan sebagainya, namun belum ter notifikasi.
7. Memperoleh informasi dari *multiple threat intelligence feeds* untuk mendeteksi serangan siber.

Respon

1. Terdapat standar operasional prosedur (SOP) dan form pelaporan penanganan insiden yang diketahui oleh pihak terkait.
2. Sebagian pegawai telah melakukan pelatihan tentang cara mengidentifikasi, penanganan, dan pelaporan suatu insiden keamanan informasi.
3. Ketika terdapat laporan terjadinya infeksi *malware*, membutuhkan 30 menit dibutuhkan untuk melakukan diskoneksi segmen jaringan untuk mencegah penyebaran *malware*.
4. Tim respon insiden siber memiliki peralatan sumber daya analisis insiden (misalnya daftar *host, packet snifer*, analisis protokol, dokumentasi protokol keamanan, diagram jaringan, daftar aset penting, alat digital *forensic*, dan sebagainya).
5. Tim respon insiden memiliki kemampuan mendeteksi insiden.
6. Ketika mengalami insiden siber tim respon insiden dapat dengan cepat mendapat bantuan dari tim manajemen krisis, namun sulit mendapatkan informasi dari pihak ketiga.
7. Memastikan pencapaian SLA dalam penanganan insiden.
8. Laporan insiden dilaporkan ke top manajemen dan ke pihak eksternal yang berkepentingan/ wajib dilaporkan sesuai regulasi.

V. Kelemahan/Kekurangan

Tata Kelola

1. Meningkatkan 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.
2. Belum terdapat *Business Continuity Plan* dan *Disaster Recovery Plan* yang mencakup *backup* dan *restoration* dari data pribadi.
3. Belum adanya kebijakan dan implementasi dalam pelaksanaan reviu izin akses dari akun pengguna dan menerapkan *single* ID untuk otentikasi.

4. Karena masih menggunakan layanan email dari Kemenkominfo, maka belum dapat dipastikan apakah mengimplementasikan kebijakan Domain-based Message Authentication Reporting and Conformance (DMARC) atau protokol otentikasi email untuk melindungi domain dari penggunaan yang tidak sah agar tidak digunakan dalam serangan penyusupan email bisnis, email *phishing*, penipuan email, email palsu dan aktivitas ancaman *cyber*.
5. Belum mengimplementasikan *software* anti virus dan anti *malware* secara terpusat dan selalu *update* terhadap perangkat *endpoint*.
6. Belum adanya proses formal yang dilakukan dalam manajemen terhadap perubahan dan pengujian semua perubahan konfigurasi *router, switch*, dan *firewall*.
7. Masih sebagian kecil pegawai yang mengetahui dan menerapkan kebijakan keamanan informasi di lingkungan kerja, serta memberikan kontribusi terhadap efektivitas sistem manajemen keamanan informasi.
8. Setiap pegawai baru belum mendapatkan pengarahan mengenai keamanan informasi.
9. Belum memiliki kebijakan terkait SMKI.
10. Belum 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.
11. Belum melakukan pelatihan keamanan informasi secara terjadwal untuk semua pegawai. Setidaknya untuk *sharing* secara menyeluruh terkait keamanan informasi kepada seluruh pegawai.
12. Belum adanya kebijakan dalam pengelolaan data stakeholder/ pegawai/ masyarakat/ pribadi.
13. Belum adanya kebijakan atau prosedur SDLC yang dapat dijadikan acuan dalam pengembangan aplikasi.
14. Belum adanya pengaturan terhadap 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.

15. 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.
16. Belum melakukan *threat hunting* secara berkala.

Identifikasi

1. Organisasi belum membuat/ memperbaharui *roadmap* keamanan TI organisasi dalam jangka waktu tertentu.
2. Belum tercantum pada risk register untuk semua aplikasi yang memproses data stakeholder / klien / konsumen / pelanggan.
3. Pegawai masih diizinkan memiliki akses sebagai administrator pada perangkat (terutama pada perangkat BMN).
4. Belum melakukan segmentasi jaringan berdasarkan fungsionalitas.
5. Belum memiliki *system configuration management tools* untuk otomatisasi konfigurasi perangkat keras dan perangkat lunak.
6. Belum melakukan prioritasi terkait langkah proteksi keamanan siber termasuk strategi untuk memprioritaskan perlindungan data dan aset kritis.
7. Belum melakukan analisa keterkaitan antara keamanan dan kenyamanan dari penggunaan aset perangkat dan aplikasi dalam rangka penyusunan standar keamanan informasi.
8. Belum dilakukan pemeringkatan pada kerentanan yang teridentifikasi berdasarkan pedoman/standar / acuan organisasi.
9. Belum maksimalnya pengelolaan data log keamanan informasi.
10. Belum melakukan klasifikasi terhadap *cyber threats* yang ditemukan.

Proteksi

1. Log disimpan kurang dari 1 tahun sehingga akan mempersulit ketika dilakukan audit dan forensik.
2. Belum menggunakan penyedia *cloud* atau menerapkan *cloud system*.
3. Belum menerapkan Multi-Factor Authentication (MFA) untuk mengakses data sensitif dan akses jaringan.
4. Belum menerapkan IP *reputation* untuk memverifikasi alamat IP yang diizinkan dalam proses transaksi.
5. Belum melakukan pembatasan aplikasi yang diunduh, di-*install* dan dioperasikan, serta penggunaan *scripting tools*, penggunaan *add-on* dan *plugin*.
6. Belum seluruh perangkat *endpoints* menggunakan antivirus, menerapkan web URL *filtering*, *device control*, *application control*, enkripsi dan membatasi fitur *autorun content*.
7. Sebagian *traffic* diatur untuk *inbound* yang dibutuhkan oleh organisasi.
8. Data master *images* belum tersimpan pada server yang dikonfigurasi secara aman.
9. Seluruh data stakeholder / klien / konsumen / pelanggan belum dienkripsi saat disimpan.
10. Belum memiliki BCP dan DRP.
11. Belum memiliki kebijakan untuk memastikan penggunaan *password* yang kompleks untuk semua akses *login*, pergantian *password* secara berkala dan menggunakan/ menambahkan verifikasi OTP.

Deteksi

1. Belum melaksanakan pemantauan akses fisik terhadap perangkat yang berada di dalam ruangan data center untuk mendeteksi potensi kejadian keamanan siber.
2. Belum melakukan *record* seperti Change Advisory Board (CAB) yang meninjau dan menyetujui semua perubahan konfigurasi.

3. Belum memiliki mekanisme *monitoring* terhadap akses dan perubahan pada data *sensitive*.
4. Escalation profile belum dibuat untuk setiap *security event* yang ditemukan, kemudian disimpan sebagai panduan untuk digunakan di masa mendatang.
5. Belum memiliki SOC atau manajemen teknis yang dapat dihubungi setiap saat (24x7) untuk menangani kejadian dengan prioritas tinggi dan kritikal.
6. Belum memiliki *ticketing system* yang digunakan untuk melacak progres dari *events post-notification*, kejadian berdasarkan tingkat keparahan / prioritas / dampak, kategori keamanan, dan jenis log yang berkorelasi untuk suatu kejadian.
7. Belum melakukan *vulnerability scanning* secara otomatis menggunakan *agent*/aplikasi yang di-*install* pada endpoint.

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 memiliki daftar kontak tim penanganan insiden internal dan eksternal (misalnya penegak hukum, *ambulance*, pemadam kebakaran, dll) yang dapat dihubungi pada saat terjadi insiden.
4. Belum mengimplementasikan rencana respon insiden secara terdokumentasi dan dapat mendefinisikan peran personel pada fase penanganan/ manajemen insiden serta pembagian peran ke pihak eksternal termasuk eskalasi permasalahan.
5. Belum menerapkan *backup* data yang ada di pc/laptop pegawai ke *cloud* organisasi.
6. Dari desain jaringan eksisting belum dapat memastikan apabila server DMZ terkena serangan siber, penyerang tidak dapat mengakses server yang lain.

7. Belum melakukan *scanning* ulang untuk memastikan bahwa kerentanan tersebut sudah ditutup ketika ditemukan kerentanan yang menyebabkan pelanggaran dan telah dilakukan *patching*.
8. Belum adanya format yang baku dalam pencatatan setiap langkah yang dilakukan dalam rangka penanggulangan insiden.
9. Belum melakukan reviu terhadap rekap laporan insiden siber yang pernah terjadi untuk melihat apakah prosedur insiden respon sudah sesuai dengan standar yang ditetapkan.
10. Belum semua rekaman insiden dan pelanggaran disimpan dan dilaporkan berdasarkan *trends* insiden dalam jangka waktu tertentu.

VI. Rekomendasi

1. Untuk meningkatkan aspek tata kelola di lingkungan Diskominfo Pemprov Jambi 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 maupun permasalahan keamanan informasi yang perlu dilakukan secara berkelanjutan.
   b. Menerapkan dan mendokumentasikan standar konfigurasi (*port*, protokol, *service*) untuk semua sistem, seperti *operating system, software*/aplikasi.
   c. Konfigurasi dan akun *default* selalu diubah sebelum digunakan secara menyeluruh dan terdokumentasi.
   d. Menerapkan dan mereviu secara berkala algoritma enkripsi dalam pengembangan *software*/aplikasi.
   e. Menyusun dan melaksanakan secara konsisten dan berkelanjutan program pemahaman kesadaran keamanan informasi untuk semua pegawai.
   f. Dokumentasi/diagram yang menggambarkan semua aliran data di seluruh sistem dan jaringan serta diperbaharui setiap ada aset baru.
   g. Menyusun BCP dan DRP.

h. Menyusun kebijakan dan implementasi dalam pelaksanaan reviu izin akses dari akun pengguna dan menerapkan *single* ID untuk otentikasi.
i. Berkoordinasi dengan Kemenkominfo untuk dapat memastikan keamanan email *client* yang digunakan dan memperkuatnya jika diperlukan.
j. Mengimplementasikan *software* anti virus dan anti *malware* secara terpusat dan selalu *update* terhadap perangkat *endpoint*.
k. Menyusun proses formal yang dilakukan dalam manajemen terhadap perubahan dan pengujian semua perubahan konfigurasi *router, switch,* dan *firewall*.
l. Seluruh pegawai agar mengetahui dan menerapkan kebijakan keamanan informasi di lingkungan kerja, serta memberikan kontribusi terhadap efektivitas sistem manajemen keamanan informasi.
m. Menyusun kebijakan SMKI.
n. 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.
o. Melakukan pelatihan keamanan informasi secara terjadwal untuk semua pegawai. Setidaknya untuk *sharing* secara menyeluruh terkait keamanan informasi kepada seluruh pegawai.
p. Menyusun kebijakan atau prosedur SDLC yang dapat dijadikan acuan dalam pengembangan aplikasi.
q. 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.
r. 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.
s. Melakukan *threat hunting* secara berkala.

2. Untuk meningkatkan aspek identifikasi, dapat dilakukan hal-hal sebagai berikut:
   a. Melakukan pembaharuan secara berkala dalam inventarisasi data asset (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 pemeringkatan pada kerentanan yang teridentifikasi berdasarkan pedoman/standar / acuan organisasi.
   f. Mencantumkan pada *risk register* untuk semua aplikasi yang memproses data stakeholder / klien / konsumen / pelanggan.
   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

3. Untuk meningkatkan aspek proteksi, dapat dilakukan hal-hal sebagai berikut:
   a. Menyimpan data *backup* telah dilindungi secara tepat, baik secara fisik maupun non fisik pada lokasi yang aman dan terenkripsi.
   b. Log dapat disimpan minimal 1 tahun sehingga akan mempermudah ketika dilakukan audit dan forensik.
   c. Menerapkan Multi-Factor Authentication (MFA).

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.

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. Menerapkan *Change Management System* untuk melakukan perubahan konfigurasi.
   c. Menyusun *escalation profile* untuk setiap *security event* yang ditemukan.
   d. Menyusun Metrik *Security Event*.
   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 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. Memberikan pelatihan untuk pegawai tentang cara mengidentifikasi, penanganan, dan pelaporan suatu insiden keamanan informasi.
e. Menyusun daftar kontak tim penanganan insiden internal dan eksternal.
f. Mengadakan sumber daya redundan yang dapat langsung digunakan saat sistem penting/kritikal mengalami *down* karena insiden siber.
g. Melakukan reviu terhadap *root cause* dari suatu insiden siber serta rekap laporan insiden siber yang pernah terjadi.
h. Melakukan *scanning* ulang untuk memastikan bahwa kerentanan tersebut sudah ditutup ketika ditemukan kerentanan yang menyebabkan pelanggaran dan telah dilakukan *patching*.
i. Menyusun format yang baku dalam pencatatan setiap langkah yang dilakukan dalam rangka penanggulangan insiden.
j. 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 disampaikan laporan kegiatan penilaian CSM pada Dinas Komunikasi dan Informatika Provinsi Jambi, sebagai bahan masukkan bagi pimpinan dalam menentukan kebijakan lebih lanjut.

Jambi, 25 November 2021

Kasi Pengawasan dan Evaluasi Penyelenggaraan Persandian	Koordinator Kelompok Pengembangan Ekosistem PTK KSS Pemda
(Moch. Mawardi, S.I.P.)	(Marcelina Tri Nasiti W., S.Sos., M.Si(Han))