2022

LAPORAN

HASIL PENILAIAN

CYBER SECURITY MATURITY (CSM)

DINAS KOMUNIKASI DAN INFORMATIKA PROVINSI JAWA 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 apa pun. 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 Jawa Tengah pada tahun 2022. Dengan adanya perbaikan pada 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 hasil evaluasi tindak lanjut rekomendasi yang dilaksanakan meliputi ruang lingkup pemetaan kematangan keamanan siber yang 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 Juni 2022.

2. Validasi Penilaian CSM

   BSSN melakukan validasi pengisian instrumen CSM pada tanggal 13 - 17 Juni 2022, dengan cara diskusi dengan perwakilan tim Diskominfo Provinsi Jawa Tengah. Tim BSSN yang terlibat:

   1) Dwi Kardono, S.Sos., M.A.
   2) Melita Irmasari, S.ST, M.M.
   3) Carissa Mega Yulianingrum, S.Tr.TP.
   4) Rey Citra Kesuma, S.Tr.TP.

HASIL KEGIATAN

I. Deskripsi Ruang Lingkup Penilaian

Nama Instansi/Lembaga : Dinas Komunikasi dan Informatika Provinsi Jawa Tengah
Alamat : Jalan Menteri Supeno 1/2 Semarang - 50243
Nomor Telp./Fax. : (024) 8319140 / (024) 8412540
Email : diskominfo@jatengprov.go.id
Narasumber Instansi/Lembaga :

1) Eny Soelastri, SH.
2) Widi Nugroho, S.Kom., M.Kom.
3) Subroto Budhi Utomo, S.Kom., M.T.
4) Martiusapun Heses, S.Kom., M.Kom.
5) Rian Septiadi
6) Wisnu Raditya F.
7) Choerul Imam Wibowo

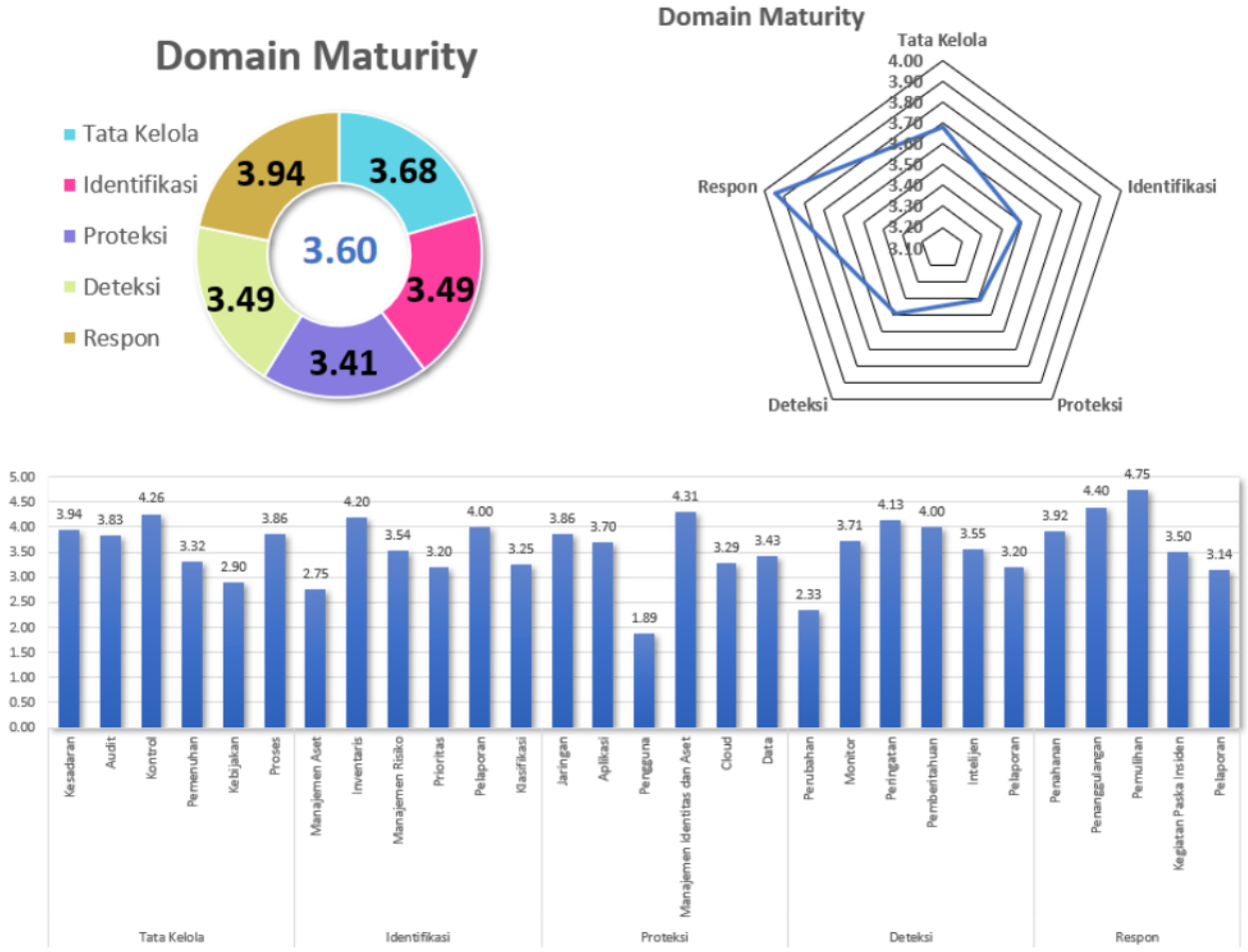
II. Deskripsi Ruang Lingkup Penilaian

1. Ruang Lingkup Penilaian :

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

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

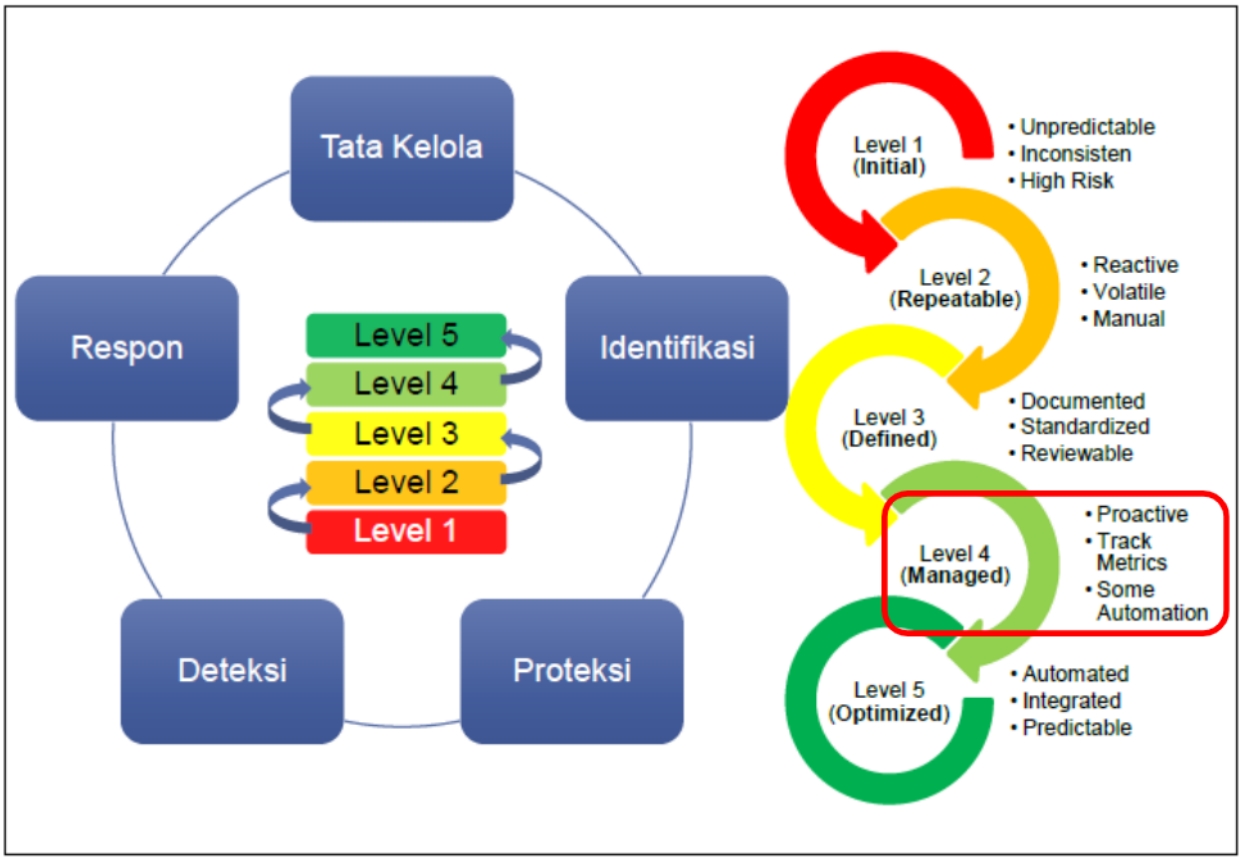
III. Hasil Penilaian CSM



Gambar 1. Hasil Penilaian CSM

Berdasarkan hasil penilaian instrumen CSM, diperoleh hasil sebagai berikut **Total Score Indeks Kematangan : 3,60**, sehingga perhitungan penentuan Level Kematangan didapatkan level kematangan sebagai berikut :

Level Kematangan Tingkat 4



Gambar 2. Capaian Level Kematangan

Level Kematangan 4:

Level kematangan 4 menunjukkan bahwa pengelolaan keamanan siber di Dinas Komunikasi dan Informatika Provinsi Jawa Tengah sudah terorganisir dengan baik namun belum dilakukan proses otomatisasi, bersifat format, dilakukan secara berulang dan direviu secara berkala, serta implementasi perbaikan dilakukan secara berkelanjutan.

Catatan:

Berdasarkan hasil evaluasi tindak lanjut rekomendasi penilaian CSM tahun 2020 yang telah dilakukan pada tahun 2021 dengan total skor indeks kematangan adalah 3,40, terdapat kenaikan 0,20 poin menjadi 3.60 dengan kategori level mengalami peningkatan yaitu dari level 3 menjadi level 4.

IV. Kekuatan/Kematangan

Tata Kelola

1. Organisasi telah memiliki program kesadaran keamanan informasi yang telah dilakukan dan di*review* secara berkala.
2. Peningkatan kompetensi keamanan informasi telah terjadwal.
3. Organisasi telah memberikan pelatihan kepada karyawan tentang *secure authentication*, *social engineering*, pengelolaan data sensitif.
4. Organisasi telah melakukan manajemen kerentanan siber.
5. Organisasi telah melakukan pemeriksaan *background* pada karyawan baru.
6. Organisasi telah memiliki *tool vulnerability scanning* secara mandiri.
7. Organisasi menggunakan akun khusus untuk melakukan *vulnerability scanning*, dan akan dihapus jika sudah tidak terpakai.
8. Organisasi telah memiliki *risk assessment*, *risk treatment*, internal audit keamanan informasi.
9. Organisasi telah menerapkan dan mendokumentasikan standar konfigurasi (port, protokol, service) untuk semua sistem.
10. Organisasi telah memiliki WAFs, *firewall* pada *end user*, NAT, DMARC, filter terhadap seluruh jenis file lampiran email.
11. Organisasi telah melakukan konfigurasi *firewall* secara berkala dan telah didokumentasikan.
12. *Vulnerability assessment* dan *penestration testing* telah dilakukan dengan melibatkan pihak internal dan eksternal.
13. Organisasi telah mengimplementasikan software anti virus dan anti malware secara terpusat dan selalu update terhadap perangkat endpoint.
14. Organisasi telah menerapkan kontrol kriptografi sesuai dengan semua perjanjian, undang-undang, dan peraturan yang berlaku.
15. Organisasi telah melakukan pemisahan *environment* antara sistem *production* dan *development* namun belum optimal.

16. Organisasi telah menerapkan metode *sandbox* terhadap seluruh lampiran email guna mencegah dan analisis keamanan lebih lanjut terhadap *malicious behaviour*.
17. Organisasi Anda melakukan *penetrating testing* menggunakan pihak eksternal dan internal secara berkala.

Identifikasi

1. Organisasi telah melakukan manajemen aset secara optimal, dengan menerapkan *update* perencanaan kapasitas dan *update patch* terhadap semua aset.
2. Organisasi telah melakukan inventarisasi data yang ada pada semua aset perangkat keras maupun perangkat lunak.
3. Aset yang diidentifikasi telah dilakukan klasifikasi kritikalitas dan ditetapkan penanggungjawabnya.
4. Terdapat dokumentasi mengenai alur informasi yang memproses data *stakeholder* termasuk yang dikelola oleh pihak ketiga serta direviu secara berkala setiap tahunnya.
5. Organisasi telah melakukan manajemen resiko berupa retensi data sensitif.
6. Organisasi telah memiliki *Business Impact Analysis* terhadap perangkat dan aplikasi TI pada Laporan Manajemen Risiko dan Keamanan Informasi, tetapi belum direviu karena dokumen masih baru.
7. Aspek keamanan mempertimbangkan kapasitas server dan perangkat jaringan secara menyeluruh.
8. Organisasi telah memiliki standar untuk melakukan klasifikasi *cyber threat*.
9. Organisasi telah melakukan segmentasi jaringan berdasarkan fungsionalitas.

Proteksi

1. Penggunaan IDS dan IPS dengan menggunakan Sophos dan Fortinet.
2. *Inbound network traffic* telah difilter untuk memeriksa *malware* dan mencegah eksplotasi terhadap kerentanan.

3. Organisasi telah menerapkan *port access control* sebagai pengendalian terhadap otentifikasi perangkat yang terhubung ke jaringan dengan implementasi *port knocking* yang digunakan di sistem CSIRT.
4. Organisasi menerapkan *firewall filtering* antar segmen jaringan lokal.
5. Memanfaatkan sistem enkripsi dalam akses nirkabel.
6. Koneksi ke server dan jaringan sudah menggunakan protokol enkripsi.
7. Penggunaan *firewall* telah dikonfigurasi dengan baik seperti *implicit* atau *explicit deny any/any rule*, *inbound network traffic* dan *outbound network traffic*.
8. Sudah menggunakan DNS *Filtering*.
9. Beberapa aplikasi sudah mulai dilakukan pemisahan sebagian besar server fisik maupun virtual.
10. Pengelolaan *patching* sudah dilakukan dan dilakukan secara otomatis.
11. Pada *email system* dilakukan pengecekan secara otomatis terhadap *spam*/ *phishing*/malware menggunakan *magic spam* dan mail server.
12. Sudah ada *whitelist* aplikasi dalam memastikan *authorized software library* dan *signed script*.
13. Sudah dilakukan *updating* secara berkala dalam penggunaan *web browser*, dan *email client* dalam organisasi.
14. Sistem manajemen identitas dan akses telah digunakan untuk seluruh sistem operasi.
15. *Multi-Factor Authentication* (MFA) telah digunakan pada akses LAN dan VPN serta untuk mengakses data sensitif (dengan menggunakan otentikasi dan *captcha*).
16. Penggunaan *password* telah digunakan pada semua akses login dan dilakukan penggantian berkala secara manual.
17. Penggunaan akses data telah diatur hak akses dan penerapan *whitelist* untuk memverifikasi alamat IP yang mempunyai hak akses.
18. Anomali transaksi oleh karyawan/ *stakeholder*/ klien dapat diidentifikasi dan dilakukan pelacakan/ pendeteksian.
19. Organisasi sudah memiliki *cloud* internal yang memiliki proses otorisasi.

20. Data penting telah dilakukan *backup* secara berkala.
21. Penyimpanan log sudah dilakukan dalam rangka audit dan forensik.
22. Penyimpanan data backup sudah dilindungi baik secara fisik dan non fisik.

Deteksi

1. Organisasi melakukan *monitoring* terhadap *log* dari perangkat *security control*, jaringan, dan aplikasi selama 24 jam.
2. Organisasi Anda mengaktifkan *Enable Detailed Logging* yang mencakup informasi terperinci seperti *event source*, tanggal, *user*, *timestamp*, *source addresses*, *destination addresses*, dan komponen lainnya.
3. Organisasi telah menerapkan *Log Analytic Tools* untuk keperluan dokumentasi, korelasi, dan analisis *log*.
4. Organisasi menjamin alokasi kapasitas penyimpanan log sesuai dengan kebutuhan.
5. Setiap orang yang tergabung dalam tim *monitoring* pada organisasi mendapatkan peningkatan keterampilan.
6. Organisasi memantau akses fisik terhadap perangkat yang berada di dalam ruangan *data center* untuk mendeteksi potensi kejadian keamanan siber.
7. Organisasi memiliki perangkat *anti-malware* yang secara otomatis melakukan *scanning* terhadap *removable media* yang terhubung ke perangkat.
8. Organisasi memiliki SOC atau manajemen teknis yang dapat dihubungi setiap saat (24x7) untuk menangani kejadian dengan prioritas tinggi dan kritikal.
9. Organisasi memiliki *contact tree* untuk mengeskalasi dalam merespon suatu kejadian.
10. Organisasi telah menjalankan *vulnerability scanning tools* secara otomatis untuk mendeteksi kerentanan siber.
11. Organisasi telah memiliki mekanisme *sharing* informasi baik internal maupun eksternal.

Respon

1. Organisasi memiliki SOP pelaporan insiden, SOP penanganan insiden, dan *disaster recovery plan* yang telah di*review* secara berkala.
2. Organisasi merencanakan skenario dan latihan respon insiden kepada karyawan secara rutin.
3. Organisasi memiliki daftar kontak tim penanganan insiden internal dan eksternal.
4. Organisasi mendesain jaringan yang dapat memastikan apabila server DMZ terkena serangan siber, penyerang tidak dapat mengakses server yang lain.
5. Tim respon insiden telah memiliki peralatan sumber daya analisis insiden (misalkan *packet sniffer*, diagram jaringan, alat digital forensik, dll).
6. Ketika organisasi mengalami insiden, tim respon insiden dengan mudah mendapat bantuan dari tim manajemen kritis.
7. Hasil *review* dan rekap laporan penanganan insiden telah dilaporkan ke *top management*.
8. Laporan insiden di organisasi dilaporkan ke *top management* dan ke pihak eksternal yang berkepentingan/wajib dilaporkan sesuai regulasi.

V. Kelemahan/Kekurangan

Tata Kelola

1. Organisasi belum memiliki gap analisis kemampuan sehingga organisasi tidak dapat membuat *baseline* pelatihan keamanan informasi.
2. Organisasi belum memiliki pelatihan *secure code* untuk personel yang terlibat dalam pengembangan aplikasi.
3. Organisasi belum memiliki kebijakan terkait perlindungan data pribadi.
4. Organisasi melakukan reviu izin akses akun pengguna namun penerapannya belum optimal dikarenakan kendala SDM yang kesulitan mengingat *password* yang kompleks dan selalu berganti.

5. Organisasi belum memiliki *red team* dan *blue team*, tetapi telah melakukan pengujian secara berkala dalam mengukur kesiapsiagaan dalam menangani insiden keamanan.
6. Organisasi belum menggunakan DLP (*Data Loss Prevention*) tetapi sudah menggunakan NAC (*Network Access Control*).
7. Organisasi belum memiliki kebijakan yang menetapkan sanksi yang dijatuhkan terhadap karyawan yang tidak patuh pada kebijakan yang berkaitan dengan keamanan siber.

Identifikasi

1. Organisasi belum memiliki *system configuration management tools* untuk otomatisasi konfigurasi perangkat keras dan perangkat lunak.
2. Belum dilakukan identifikasi maupun pembatasan akses perangkat yang tidak diizinkan.
3. Analisis keterkaitan antara keamanan dan kenyamanan dari pengguna aset perangkat dan aplikasi belum dilakukan dalam rangka penyusunan standar keamanan informasi.
4. Karyawan diiizinkan memiliki akses sebagai administrator pada perangkat (laptop, personal computer, dll) milik organisasi.
5. Pihak ketiga diizinkan untuk menggunakan aset mereka pada jaringan organisasi.
6. Risk Register belum didokumentasikan untuk semua aplikasi.
7. Organisasi tidak memperbaharui *roadmap* keamanan Tl organisasi dalam jangka waktu tertentu.
8. Organisasi belum memprioritaskan langkah proteksi keamanan siber dalam perlindungan data dan aset kritis.
9. Organisasi belum memiliki metode/standar klasifikasi aset Tl.

Proteksi

1. Seluruh perangkat jaringan belum menggunakan otentikasi terpusat.
2. Organisasi belum melakukan *disable peer-to-peer* pada *wireless client* di perangkat *endpoint*.
3. Belum ada pembatasan aplikasi yang diunduh, diinstal, dan dioperasikan.
4. Belum dilakukan pembatasan penggunaan *scripting tools*.
5. Semua perangkat *endpoints* termasuk server belum menggunakan *antivirus*.
6. Belum ada batasan fitur *auto-run content* dan pengaturan akses *read/write* pada perangkat USB.
7. Belum melakukan enkripsi pada semua media penyimpanan eksternal.
8. Belum 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.
9. Informasi identitas dan akses pengguna tidak digunakan untuk membatasi hak akses dari dalam jaringan.
10. *Cloud* belum menerapkan *multi-factor authentication*.
11. Belum ada *Data Center Redudancy* terkait *cloud* yang ada di organisasi.

Deteksi

1. Organisasi belum memiliki *Change Advisory Board* (CAB).
2. Organisasi tidak memiliki mekanisme *monitoring* terhadap akses dan perubahan pada data sensitif (seperti *File Integrity Monitoring* atau *Event Monitoring*).
3. Organisasi tidak memiliki mekanisme *monitoring* dan deteksi terhadap penggunaan enkripsi yang tidak sah.
4. Organisasi belum memiliki sistem untuk me*monitoring* dan mencegah kehilangan data sensitif.
5. Organisasi tidak dapat mendeteksi *Wireless Access Point* yang terhubung ke jaringan LAN.

6. Organisasi tidak memantau aktifitas pihak ketiga untuk mendeteksi adanya potensi kejadian keamanan siber.
7. Organisasi tidak menerapkan *event notification* yang berbeda-beda untuk setiap jenis eskalasi.
8. Organisasi belum memperoleh informasi dari *multiple threat intelligence feeds* untuk mendeteksi serangan siber.
9. Organisasi belum memiliki sistem untuk melakukan *Malicious Code Detection* untuk mendeteksi, menghapus, dan melindungi dari *Malicious Code*.

Respon

1. Organisasi belum memiliki kebijakan penanganan insiden dan selaras dengan kebijakan pengaturan kesinambungan organisasi atau *Business Continuity Planning* (BCP).
2. Organisasi belum memiliki skema penilaian insiden dan prioritas berdasarkan potensial dampak.
3. Organisasi belum merancang standar terkait waktu yang diperlukan bagi administrator sistem dan karyawan lainnya untuk melaporkan kejadian yang tidak wajar kepada tim penanganan insiden, mekanisme pelaporan tersebut, dan jenis informasi yang harus dimasukkan dalam pemberitahuan insiden.

VI. Rekomendasi

1. Untuk meningkatkan aspek tata Kelola, organisasi diharapkan:
   a. Melakukan gap analisis untuk memahami *skill* dan *behaviour* yang tidak dimiliki karyawan dan menggunakan informasi tersebut untuk membuat *roadmap* terkait *baseline* pendidikan dan pelatihan terkait keamanan informasi.
   b. Memberikan pelatihan *secure code* untuk personil yang terlibat dalam pengembangan aplikasi.

c. Membuat kebijakan penerapan perlindungan data pribadi dan keamanan informasi.
d. Melakukan perubahan terhadap kebijakan izin akses pengguna misalnya dengan dari yang sebelumnya mengganti *password* 3 bulan sekali menjadi kompleksitas *password*nya harus yang baik.
e. Membentuk *red team* dan *blue team* serta melakukan pengujian secara berkala dalam mengukur kesiapsiagaan dalam menangani insiden keamanan.
f. Menambahkan klausul penetapan sanksi yang dijatuhkan terhadap karyawan yang tidak patuh pada kebijakan yang berkaitan dengan keamanan siber.

2. Aspek Identifikasi dapat ditingkatkan dengan hal-hal sebagai berikut:
   a. Menggunakan *system configuration management tools* untuk otomatisasi konfigurasi perangkat keras dan perangkat lunak.
   b. Melakukan identifikasi dan pembatasan akses perangkat yang tidak diizinkan dan/atau yang tidak diperlukan oleh organisasi.
   c. Membuat kebijakan terkait karyawan tidak diiizinkan memiliki akses sebagai administrator pada perangkat (laptop, *personal computer*, dll) milik organisasi.
   d. Melakukan penilaian risiko pada seluruh aplikasi yang dimiliki.

3. Untuk meningkatkan Aspek Proteksi dilakukan dengan cara:
   a. Menggunakan otentikasi terpusat untuk seluruh jaringan.
   b. Melakukan pembatasan aplikasi yang diunduh, diinstal, dan dioperasikan.
   c. Menggunakan *antivirus* pada semua perangkat *endpoints* termasuk server.
   d. Menerapkan pembatasan akun pada laptop/PC milik organisasi yang digunakan untuk aktivitas tertentu.
   e. Melakukan enkripsi pada semua media penyimpanan eksternal.
   f. Menerapkan *multi-factor authentication* pada *cloud*.

4. Aspek Deteksi ditingkatkan dengan hal-hal berikut:
    a. Membuat kebijakan atau prosedur *Change Advisory Board* (CAB) untuk meninjau dan menyetujui semua perubahan konfigurasi yang terjadi, baik di sistem, jaringan, maupun aplikasi.
    b. Membuat mekanisme *monitoring* terhadap akses dan perubahan pada data sensitif (*File Integrity Monitoring* atau *Event Monitoring*), deteksi terhadap penggunaan enkripsi yang tidak sah, dan mencegah kehilangan data sensitif.
    c. Melakukan pendeteksian *Wireless Access Point* yang terhubung ke jaringan LAN untuk mengantisipasi adanya AP ilegal yang terhubung ke jaringan lokal.
    d. Membuat mekanisme sistem pemantauan / *monitoring* terhadap kinerja dan akses data yang dilakukan oleh pihak ketiga untuk memantau aktifitas pihak ketiga dalam mendeteksi adanya potensi kejadian keamanan siber.
    e. Menerapkan *event notification* yang berbeda-beda untuk setiap jenis eskalasi yaitu notifikasi menyesuaikan kritikalitas kejadian (bisa dimasukkan dalam kebijakan atau prosedur penanganan insiden.

5. Aspek Respon ditingkatkan dengan cara:
    a. Membuat kebijakan penanganan insiden yang selaras dengan kebijakan *Business Continuity Planning* (BCP).
    b. Membuat skema penilaian insiden dan prioritas berdasarkan potensial dampak (aspek kerugian operasional, bisnis, reputasi, dan hukum).
    c. Menambahkan klausul terkait standar waktu yang diperlukan bagi administrator sistem dan karyawan lainnya untuk melaporkan kejadian yang tidak wajar kepada tim penanganan insiden, mekanisme pelaporan tersebut, dan jenis informasi yang harus dimasukkan dalam pemberitahuan insiden pada dokumen kebijakan atau prosedur penanganan insiden.

PENUTUP

Demikian Laporan Penilaian CSM pada Dinas Komunikasi dan Informatika Provinsi Jawa Tengah ini disusun, sebagai bahan pengambilan keputusan pimpinan dalam Pelaksanaan Pengamanan Siber Pemerintah Daerah Provinsi Jawa Tengah. Agar Pemerintah Daerah Provinsi Jawa 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 Jawa Tengah; dan
3. Sekretaris Daerah Provinsi Jawa Tengah.

Semarang, 17 Juni 2022

Kepala Bidang Persandian dan Keamanan Informasi	Sandiman Madya pada Direktorat Keamanan Siber dan Sandi Pemerintah Daerah
Eny Soelastri, SH.	Dwi Kardono, S.Sos., M.A.
19700515 199001 2 001	19710218 199110 1 001

Mengetahui,
Kepala Dinas Komunikasi dan Informatika
Provinsi Jawa Tengah

PEMERINTAH PROVINSI DISKOMINFO JAWA TENGAH

Riena Retnaningrum, SH.
19641026 198909 2 001