2020

LAPORAN

HASIL PENILAIAN

CYBER SECURITY MATURITY (CSM)

DINAS KOMUNIKASI DAN INFORMATIKA
PEMERINTAH PROVINSI KEPULAUAN RIAU

PENDAHULUAN

I. Tujuan Kegiatan

Kegiatan ini bertujuan untuk mengetahui tingkat maturitas keamanan siber di lingkungan Dinas Komunikasi dan Informatika Pemerintah Provinsi Kepulauan Riau. 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.

II. Ruang Lingkup Kegiatan

Kegiatan yang dilaksanakan berupa pemetaan aspek pengelolaan keamanan siber, meliputi :

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

III. 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 %

IV. Pelaksanaan Kegiatan

Pengisian Instrumen CSM dilakukan oleh internal *stakeholder* (*self assessment*) dan dilakukan validasi pada tanggal 1 Desember 2020 oleh Tim BSSN.

HASIL KEGIATAN

I. Informasi *Stakeholder*

Nama Instansi/Lembaga : Diskominfo Pemerintah Provinsi Kepulauan Riau

Alamat : Komplek Pusat Pemerintahan Provinsi Kepulauan Riau, Gedung Sultan Mahmud Riayat Syah (Gedung B2 Lantai III), Pulau Dompang, Tanjungpinang

Nomor Telp./Fax. : 0771-4575023

Email : kominfo@kepriprov.go.id

Narasumber Instansi/Lembaga :

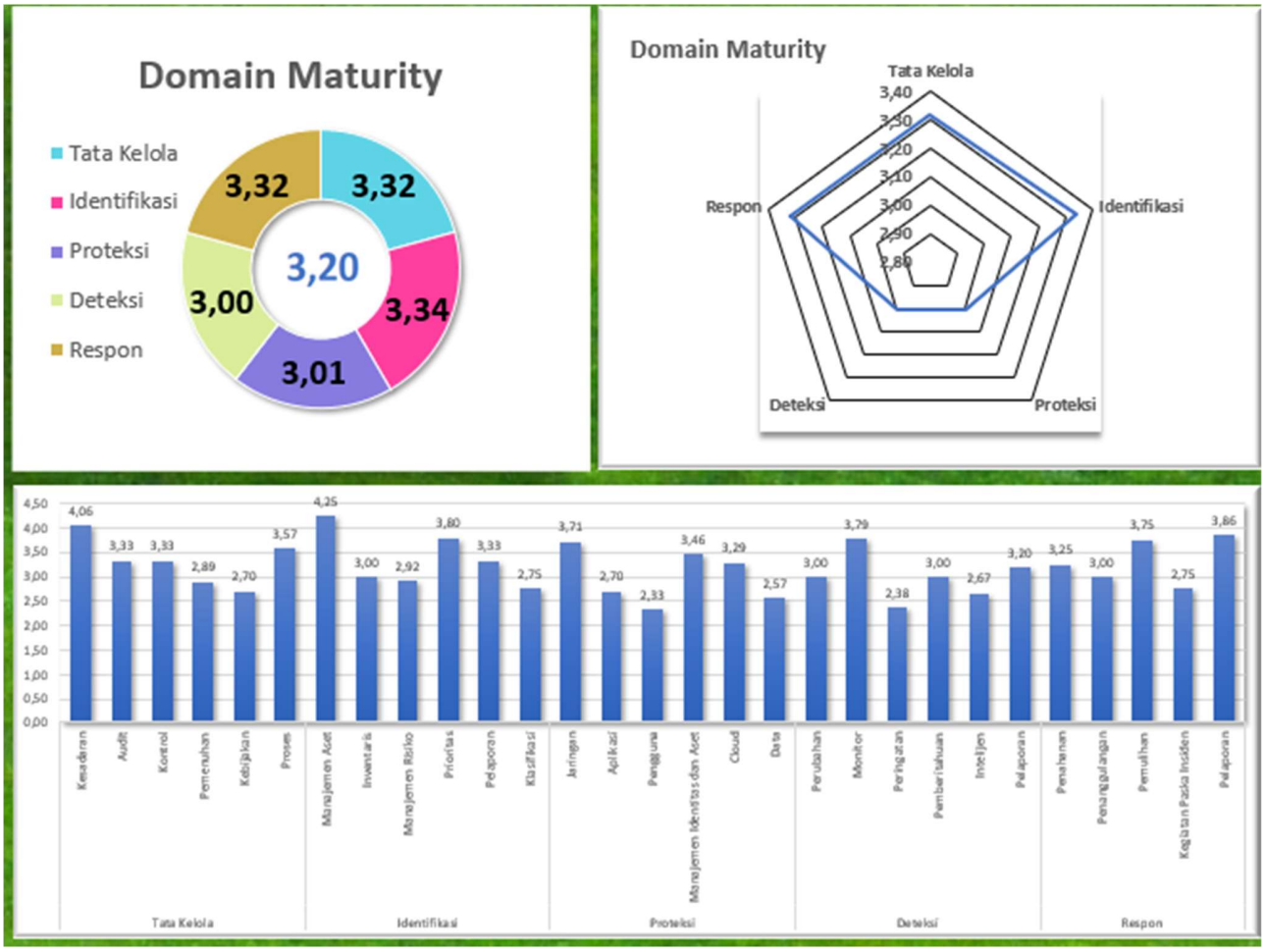
1. Donny Firmansyah, ST
   Kasi Keamanan Informasi e government dan Persandian, Bidang Teknologi Informasi dan Komunikasi

II. Deskripsi Ruang Lingkup Penilaian

1. Ruang Lingkup Penilaian :
   ☐ Organisasi Keseluruhan ☐ Regional, Kanwil, Cabang √ Unit Kerja ☐ Lainnya
2. Instansi/Unit Kerja* : Diskominfo Provinsi Kepulauan Riau

III. Hasil Penilaian CSM

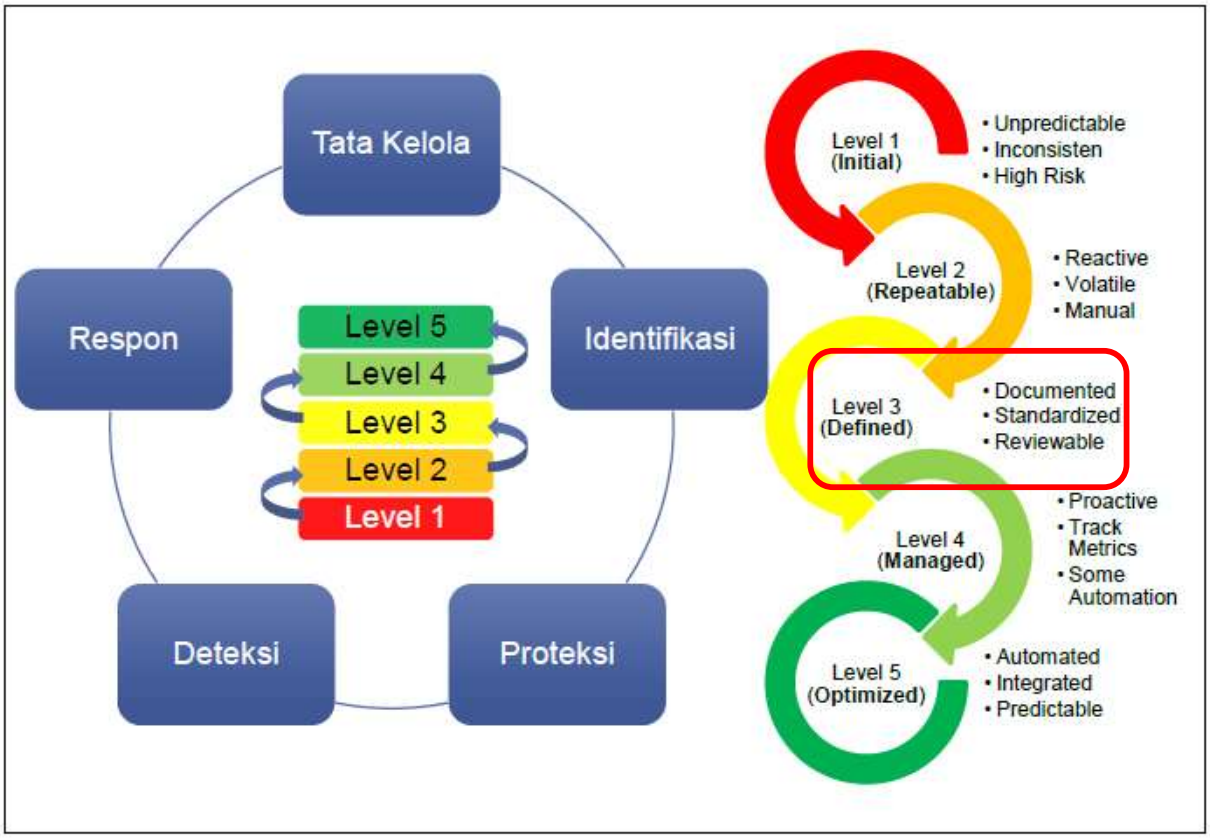
Tata Kelola		Identifikasi		Proteksi		Deteksi		Respon	
3,32		3,34		3,01		3,00		3,32	
Kesadaran	4,06	Manajemen Aset	4,25	Jaringan	3,71	Perubahan	3,00	Penahanan	3,25
Audit	3,33	Inventaris	3,00	Aplikasi	2,70	Monitor	3,79	Penanggulangan	3,00
Kontrol	3,33	Manajemen Risiko	2,92	Pengguna	2,33	Peringatan	2,38	Pemulihan	3,75
Pemenuhan	2,89	Prioritas	3,80	Manajemen Identitas dan Aset	3,46	Pemberitahuan	3,00	Kegiatan Paska Insiden	2,75
Kebijakan	2,70	Pelaporan	3,33	Cloud	3,29	Intelijen	2,67	Pelaporan	3,86
Proses	3,57	Klasifikasi	2,75	Data	2,57	Pelaporan	3,20		



Gambar 1. Hasil Penilaian CSM

Berdasarkan hasil penilaian instrumen CSM, diperoleh hasil sebagai berikut **Total Score Indeks Kematangan : 3,20** 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 Pemerintah Provinsi Kepulauan Riau sudah terdokumentasikan, terstandar dan direviu.

IV. Kekuatan/Kematangan

Tata Kelola

1. Organisasi membuat program pemahaman kesadaran keamanan informasi untuk semua karyawan secara berkala diantaranya dengan melakukan pelatihan keamanan informasi secara terjadwal untuk semua karyawan.
2. Setiap karyawan baru di organisasi mendapatkan pengarahan mengenai keamanan informasi melalui penandatanganan NDA (*Non Disclosure Agreement*).
3. Dalam pengembangan software/aplikasi di organisasi, personel yang terlibat dalam pengembangan software/aplikasi telah mendapatkan pelatihan dalam membuat secure code yang baik.
4. Organisasi menggunakan tool vulnerability scanning secara mandiri, yang mana hasil vulnerability assessment digunakan sebagai titik awal dalam melakukan penetrating testing dan melaksanakan vulnerability assessment atau penetrating testing kepada aplikasi web, aplikasi client-based, aplikasi mobile, wireless, server dan perangkat jaringan.
5. Dalam pengembangan software, organisasi melakukan kerjasama dengan pihak ketiga yang tepercaya dan memastikan bahwa versi software yang diperoleh dari luar organisasi masih didukung oleh pengembang.
6. Keamanan informasi termasuk dalam fase perencanaan, pembangunan, dan pengembangan di semua proyek TI.
7. Organisasi melakukan penetrating testing menggunakan pihak eksternal dan internal secara berkala.

Identifikasi

1. Organisasi melakukan perencanaan kapasitas secara berkala untuk memastikan bahwa pengadaan semua aset perangkat dan aplikasi dilakukan sesuai dengan kebutuhan melalui perencanaan pengadaaan setiap tahun.
2. Organisasi menerapkan patch keamanan pada semua perangkat keras dan perangkat lunak saat ada update patch yang sudah diriliis.
3. Aset milik organisasi yang diidentifikasi telah disusun berdasarkan klasifikasi kritikalitas serta telah ditetapkan penanggung jawab untuk setiap aset tersebut.
4. Organisasi melakukan prioritasi terkait langkah proteksi keamanan siber termasuk strategi untuk memprioritaskan perlindungan data dan aset kritis.
5. Pihak ketiga diizinkan untuk menggunakan aset mereka pada jaringan organisasi setelah melalui screening oleh Bagian TI.
6. Organisasi melakukan klasifikasi terhadap ancaman siber yang ditemukan pada organisasi.
7. Organisasi melakukan segmentasi jaringan berdasarkan fungsionalitas (segmen bagian development, keuangan, SDM, dll).

Proteksi

1. Organisasi memiliki IPS dan telah menerapkan rules inbond dan outbond network traffic serta telah menerapkan anti virus.
2. Akses nirkabel di organisasi menggunakan sistem enkripsi.
3. Koneksi ke perangkat server dan jaringan di organisasi menggunakan protokol terenkripsi.
4. Organisasi menerapkan port access control.
5. Organisasi menerapkan DNS filtering services.
6. Aplikasi yang kritikal bagi organisasi menggunakan server terpisah.
7. Organisasi telah menerapkan pengelolaan patch, walaupun secara manual.

8. Organisasi memiliki pengecekan otomatis terhadap spam/phishing/malware di email system.
9. Organisasi sudah menerapkan web URL filtering, device control, application control, enkripsi pada perangkat mobile dan otentikasi ulang pada perangkat setelah beberapa saat tidak aktif, pada sebagian perangkat.
10. Informasi identitas dan akses pengguna digunakan untuk membatasi hak akses.
11. Organisasi memastikan penggunaan password yang kompleks untuk semua akses login.
12. Organisasi memastikan penggantian password secara berkala.
13. Organisasi menerapkan metode otentikasi melalui saluran terenkripsi.
14. Organisasi dapat melacak dan mendeteksi perilaku anomali transaksi.
15. Organisasi melakukan identifikasi perangkat pada setiap transaksi yang dilakukan.
16. Pengguna selain admin database hanya memiliki akses read-only pada akses ke database.
17. Organisasi menggunakan email provider.
18. Organisasi telah melakukan backup secara berkala pada semua data penting walaupun dilakukan secara manual.
19. Organisasi telah menyimpan log selama setidaknya 1 tahun tanpa File Integrity Monitoring
20. Sebagian data dienkripsi pada saat disimpan dan dikirim.
21. Penyimpanan data backup telah disimpan di lokasi yang aman, walaupun belum dienkripsi.

Deteksi

1. Organisasi telah memiliki *Change Advisory Board* (CAB) yang meninjau dan menyetujui perubahan konfigurasi, walaupun tidak semua perubahan.
2. Organisasi menyimpan dan monitoring log yang detail dari perangkat security control, jaringan dan aplikasi, ketika diketahui ada masalah.

3. Organisasi melakukan monitoring terhadap akses pengguna, koneksi jaringan, perangkat keras dan perangkat lunak yang ada di data center.
4. Organisasi dapat mendeteksi Wireless Access Point yang terhubung ke jaringan LAN.
5. Setiap orang yang tergabung dalam tim monitoring di organisasi mendapatkan peningkatan keterampilan.
6. Organisasi melakukan deteksi terhadap anomali pada jaringan, walaupun masih secara manual.
7. Organisasi memantau akses fisik terhadap perengakat dalam data center.
8. Organisasi memiliki mekanisme untuk mendeteksi adanya akses yang tidak diizinkan pada sistem.
9. Organisasi dapat mendeteksi kegagalan login pada akun admin pada perangkat jaringan, server dan aplikasi.
10. Organisasi memiliki perangkat anti-malware yang secara otomatis melakukan scanning terhadap removable media yang terhubung ke perangkat.
11. Organisasi telah memiliki escalation profile untuk setiap security event yang ditemukan.
12. Organisasi memiliki contact tree untuk mengeskalasi dalam merespon suatu kejadian.
13. Organisasi mendapatkan update informasi dari asosiasi terkait isu keamanan siber terkini.
14. Organisasi mengaktifkan DNS query logging.
15. Metrik security event di organisasi di reviu setiap tahun.
16. Top Management menerima briefing tentang kondisi keamanan siber terkini minimal satu tahun sekali.
17. Organisasi memiliki mekanisma sharing informasi hasil deteksi, hanya untuk internal organisasi.

Respon

1. Organisasi memiliki kebijakan penanganan insiden.
2. Organisasi memiliki SOP dan form pelaporan penanganan insiden dan direviu setahun sekali dan/atau setiap ada perubahan.
3. Organisasi merencanakan skenario insiden dan melakukan latihan respon insiden, walaupun tidak secara rutin.
4. Organisasi memberikan pelatihan untuk sebagian kecil karyawan tentang cara mengidentifikasi, penanganan dan pelaporan suatu insiden keamanan informasi.
5. Organisasi mempunyai daftar kontak tim penanganan insiden internal dan eksternal walaupun hanya diupdate sebagian.
6. Organisasi memiliki rencana respon insiden yang terdokumentasi dan dapat mendefinisikan peran personel dan pihak eksternal.
7. Dibutuhkan waktu 3 jam untuk melakukan diskoneksi segmen jaringan untuk mencegah penyebaran malware.
8. Orgnisasi telah mendesain jaringan yang dapat memastikan apabila server DMZ terkena serangan siber, penyerang tidak dapat mengakses server yang lain.
9. Tim respon insiden organisasi memiliki kemampuan mendeteksi insiden, melakukan analisis dan rekomendasi.
10. Ketika ditemukan kerentanan dan dilakukan patching, maka akan dilakukan scanning ulang untuk memastikan bahwa kerentanan tersebut sudah ditutup.
11. Tim respon insiden organisasi dapat dengan cepat mendapat bantuan dari pihak eksternal, ketika mengalami insiden siber.
12. Tim respon insiden organisasi mencatat setiap langkap yang dilakukan dalam rangka penanggulangan insiden menggunakan format yang baku.
13. Jika terjadi insiden siber, backup dapat digunakan dalam kurun waktu kurang dari 3 jam.
14. Waktu RPO untuk merestore data dari backup adalah 1 hari sampai dengan 1 minggu.

15. Organisasi melakukan reviu terhadap root cause dari suatu insiden siber untuk mencagah kejadian serupa berulang.
16. Organisasi melakukan reviu terhadap rekap laporan insiden siber yang pernah terjadi untuk melihat apakah prosedur insiden respon sudah sesuai dengan standar yang ditetapkan dan hasil reviu tersebut dilaporkan ke top management.
17. Organisasi merekam semua insiden dan pelanggaran berdasarkan tren insiden dalam waktu 1 tahun.
18. Organisasi akan melakukan investigasi, perbaikan dan menginformasikan kepada stakeholder jika terjadi kehilangan data pribadi stakeholder.
19. Organisasi mempublikasikan informasi untuk semua karyawan mengenai mekanisme pelaporan insiden siber yang dilakukan secara rutin.
20. Organisasi merancang standar waktu, mekanisme pelaporan dan jenis informasi yang diperlukan bagi administrator sistem dan karyawan lain untuk melaporkan kejadian yang tidak wajar kepada tim penanganan insiden.
21. Laporan insiden dilaporkan ke top management dan pihak eksternal yang berkepentingan.

V. Kelemahan/Kekurangan

Tata Kelola

1. Organisasi belum memiliki kebijakan mengharuskan penerapan perlindungan data pribadi dan belum melatih staf secara khusus tentang kewajiban menjaga data privasi, termasuk hukuman terkait pengungkapan data yang salah.
2. Organisasi belum melindungi aplikasi web menggunakan firewall aplikasi web (WAF).
3. Organisasi belum mengimplementasikan software anti virus dan anti malware secara terpusat dan selalu update terhadap perangkat endpoint.
4. Organisasi belum memiliki *Business Continuity Plan* (BCP) dan *Disaster Recovery Plan* (DRP) yang mencakup backup dan restoration dari data pribadi.

5. Organisasi belum melakukan internal audit keamanan informasi secara berkala.
6. Organisasi belum memiliki kebijakan yang menetapkan sanksi yang dijatuhkan terhadap karyawan yang tidak patuh pada kebijakan yang berkaitan dengan keamanan siber.
7. Organisasi belum memiliki kebijakan keamanan yang mengatur mengenai single ID yang unik untuk melakukan semua otentikasi.

Identifikasi

1. Organisasi belum melakukan klasifikasi informasi (rahasia, terbatas, umum) dan melakukan inventarisasi dan belum memiliki metode atau standar untuk klasifikasi data.
2. Belum ada kebijakan dan implementasi mengenai retensi data sensitif termasuk data pegawai di organisasi sesuai dengan kebijakan regulasi.
3. Belum dilakukan pemeringkatan pada kerentanan yang teridentifikasi berdasarkan pedoman / standar / acuan organisasi.
4. Organisasi belum memiliki *Business Impact Analysis* (BIA) terhadap perangkat dan aplikasi TI.

Proteksi

1. Organisasi belum menonaktifkan komunikasi antar workstation.
2. Organisasi belum melakukan disable peer-to-peer pada wireless client di perangkat endpoint.
3. Organisasi belum membatasi aplikasi yang diunduh, diinstall dan dioperasikan.
4. Organisasi belum melakukan pembatasan penggunaan sripting tools dan software library.
5. Organisasi belum memiliki ketentuan mengenai penggunaan add-on dan plugin
6. Organisasi belum menggunakan Next Generation Endpoint Protection

7. Organisasi belum menerapkan akses (read/write) dan ekripsi terhadap media penyimpanan eksternal.
8. Organisasi belum menerapkan pembatasan akun pada laptop/PC milik organisasi.
9. Organisasi belum menggunakan Multi-Factor Authentication (MFA) untuk akses jaringan dan data sensitif.
10. Organisasi belum menambahkan verifikasi OTP untuk transaksi yang berisiko tinggi.
11. Organisasi belum melakukan pengujian data integrity secara berkala terhadap data yang dibackup dengan melakukan restore data.
12. Belum semua critcal system clocks telah disinkronkan dengan metode otomatis.

Deteksi

1. Perubahan konfigurasi pada peralatan jaringan belum terdeteksi secara otomatis.
2. Organisasi belum memiliki mekanisme monitoring terhadap akses dan perubahan pada data sensitif (seperti File Integrity Monitoring atau Event Monitoring)
3. Organisasi belum memiliki sistem untuk memonitoring dan mencegah kehilangan data sensitif.
4. Organisasi belum menerapkan SIEM.
5. Log hasil deteksi malware belum terhubung dengan perangkat anti-malware administrations dan event log servers sehingga dapat digunakan untuk analisis.
6. Organisasi belum menerapkan automated port scan secara berkala dan memberikan alert jika terdapat port yang tidak sah terdeteksi pada suatu sistem.
7. Organisasi belum memiliki ticketing system untuk melacak proress dari event post-notification.
8. Organisasi belum memiliki SOC.
9. Organisasi belum menerapkan event notification yang berbeda-beda untuk setiap jenis eskalasi.

10. Organisasi tidak memperoleh informasi dari multiple threat intelligence feeds untuk mendeteksi serangan siber.
11. Organisasi belum menjalankan vulnerability scanning secara otomatis untuk mendeteksi kerentanan siber.
12. Metrik security event di organisasi belum menjadi pertimbangan dalam menilai keberhasilan penerapan keamanan.

Respon

1. Organisasi belum membuat skema penilaian insiden dan prioritas berdasarkan potensial dampak.
2. Organisasi belum melakukan backup data yang ada di PC/laptop karyawan ke cloud organisasi.
3. Tim respon insiden belum memiliki peralatan sumber daya analisis insiden.
4. Organisasi belum memiliki sumber daya redundan.
5. Organisasi belum memiliki metode yang terdokumentasi dan diinformasikan kepada karyawan untuk melaporkan penyalahgunaan informasi karyawan.
6. Organisasi belum memiliki SLA.

VI. Rekomendasi

Untuk meningkatkan keamanan data di lingkungan Dinaskominfo Pemprov Kepulauan Riau maka dapat dilakukan hal-hal sebagai berikut:

a. Tata Kelola
   - Menyusun kebijakan yang mengharuskan penerapan perlindungan data pribadi dan melatih staf secara khusus tentang kewajiban menjaga data privasi, termasuk hukuman terkait pengungkapan data yang salah.
   - Melindungi aplikasi web menggunakan firewall aplikasi web (WAF).

- Mengimplementasikan software anti virus dan anti malware secara terpusat dan selalu update terhadap perangkat endpoint.
- Menyusun Business Continuity Plan (BCP) dan Disaster Recovery Plan (DRP) yang mencakup backup dan restoration dari data pribadi.
- Melakukan internal audit keamanan informasi secara berkala.
- Menyusun kebijakan yang menetapkan sanksi yang dijatuhkan terhadap karyawan yang tidak patuh pada kebijakan yang berkaitan dengan keamanan siber.
- Menyusun kebijakan keamanan yang mengatur mengenai single ID yang unik untuk melakukan semua otentikasi.

b. Identifikasi
- Melakukan klasifikasi informasi (rahasia, terbatas, umum) dan melakukan inventarisasi.
- Menyusun kebijakan dan implementasi mengenai retensi data sensitif termasuk data pegawai di organisasi sesuai dengan kebijakan regulasi.
- Melakukan pemeringkatan pada kerentanan yang teridentifikasi berdasarkan pedoman / standar / acuan organisasi.
- Menyusun *Business Impact Analysis* (BIA) terhadap perangkat dan aplikasi.

c. Proteksi
- Menonaktifkan komunikasi antar workstation.
- Melakukan disable peer-to-peer pada wireless client di perangkat endpoint.
- Membatasi aplikasi yang diunduh, diinstall dan dioperasikan.
- Menyusun BCP dan DRP.
- Melakukan pembatasan penggunaan sripting tools dan software library.
- Menyusun ketentuan mengenai penggunaan add-on dan plugin

- Menerapkan Next Generation Endpoint Protection
- Menerapkan akses (read/write) dan ekripsi terhadap media penyimpanan eksternal.
- Menerapkan pembatasan akun pada laptop/PC milik organisasi.
- Menggunakan Multi-Factor Authentication (MFA) untuk akses jaringan dan data sensitif.
- Menambahkan verifikasi OTP untuk transaksi yang berisiko tinggi.
- Melakukan pengujian data integrity secara berkala terhadap data yang dibackup dengan melakukan restore data.
- Mensinkronkan semua critcal system clocks dengan metode otomatis.

d. Deteksi

- Mensetting agar perubahan konfigurasi pada peralatan jaringan dapat terdeteksi secara otomatis.
- Menerapkan mekanisme monitoring terhadap akses dan perubahan pada data sensitif (seperti File Integrity Monitoring atau Event Monitoring).
- Menerapkan sistem untuk memonitoring dan mencegah kehilangan data sensitif.
- Menerapkan SIEM.
- Mensetting Log hasil deteksi malware agar dapat terhubung dengan perangkat anti-malware administrations dan event log servers sehingga dapat digunakan untuk analisis.
- Menerapkan automated port scan secara berkala dan memberikan alert jika terdapat port yang tidak sah terdeteksi pada suatu sistem.
- Menerapkan ticketing system untuk melacak proress dari event post-notification.
- Membangun SOC.
- Menerapkan event notification yang berbeda-beda untuk setiap jenis eskalasi.
- Menggunakan informasi dari multiple threat intelligence feeds untuk mendeteksi serangan siber.

- Menerapkan vulnerability scanning secara otomatis untuk mendeteksi kerentanan siber.
- Menjadikan Metrik security event di organisasi sebagai pertimbangan dalam menilai keberhasilan penerapan keamanan.

e. Respon

- Menyusun skema penilaian insiden dan prioritas berdasarkan potensial dampak.
- Melakukan backup data yang ada di PC/laptop karyawan ke cloud organisasi.
- Melengkapi Tim respon insiden dengan peralatan sumber daya analisis insiden.
- Menerapkan sumber daya redundan.
- Menyusun metode yang terdokumentasi dan diinformasikan kepada karyawan untuk melaporkan penyalahgunaan informasi karyawan.
- Menyusun SLA.

PENUTUP

Demikian disampaikan laporan kegiatan penilaian CSM pada Dinas Komunikasi dan Informatika Pemerintah Provinsi Kepulauan Riau, sebagai bahan masukkan bagi pimpinan dalam menentukan kebijakan lebih lanjut.

Tanjungpinang, 2 Desember 2020

Kepala Bidang Teknologi Informasi dan Komunikasi	Ketua Tim
Ditandatangani secara elektronik oleh : Kepala Bidang Teknologi Informasi **DIDI MADJDI, SE** NIP. 19720426 200604 1 003	Ditandatangani secara elektronik oleh : KASUBDIT PENANGGULANGAN DAN PEMULIHAN PEMERINTAH PUSAT, BADAN SIBER DAN SANDI NEGARA **Marcelina Tri N. W., S.Sos., M.Si (han)** Pembina (IV/a)

Dokumen ini telah ditandatangani secara elektronik menggunakan sertifikat elektronik yang diterbitkan oleh Balai Sertifikasi Elektronik (BSrE) Badan Siber dan Sandi Negara