

2020



LAPORAN

HASIL PENILAIAN

CYBER SECURITY MATURITY (CSM)

DINAS KOMUNIKASI, INFORMATIKA, DAN STATISTIK
PROVINSI DKI JAKARTA

PENDAHULUAN

I. Tujuan Kegiatan

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. Badan Siber dan Sandi Negara telah menyusun *framework* untuk mengukur *cyber security maturity* (CSM) yang dapat digunakan sebagai metode untuk mengukur tingkat kematangan keamanan siber suatu organisasi. Sehingga organisasi diharapkan dapat melakukan peningkatan pengelolaan keamanan siber serta memastikan pengelolaan tersebut.

Kegiatan penilaian CSM di lingkungan Dlnas Komunikasi Informatika dan Statistik (Diskominfo) Provinsi DKI Jakarta bertujuan untuk mengetahui tingkat kematangan keamanan siber di lingkungan Diskominfo Provinsi DKI Jakarta. Dengan adanya tingkat kematangan ini diharapkan dapat memberikan gambaran dan mempermudah organisasi untuk mengetahui kekuatan dan kelemahan yang perlu ditingkatkan pada setiap aspek keamanan siber. Sehingga dapat dijadikan acuan Diskominfo Provinsi DKI Jakarta maupun Badan Siber dan Sandi Negara (BSSN) dalam menyusun strategi peningkatan kematangan *cyber security* dan pengelolaan keamanan siber dengan tepat sasaran.

II. Ruang Lingkup Kegiatan

Ruang lingkup penilaian kematangan keamanan siber (CSM) pada Diskominfo Provinsi DKI Jakarta mencakup 5 aspek yaitu:

1. Tata Kelola

Aspek tata Kelola terdiri dari sub aspek kesadaran, audit, kontrol, pemenuhan, kebijakan dan proses.

2. Identifikasi
Aspek identifikasi terdiri dari sub aspek manajemen aset, inventaris, manajemen risiko, prioritas, pelaporan dan klasifikasi.
3. Proteksi
Aspek proteksi terdiri dari sub aspek jaringan, aplikasi, pengguna, manajemen identitas dan akses, *cloud* dan data.
4. Deteksi
Aspek deteksi terdiri dari sub aspek perubahan, monitor, peringatan, pemberitahuan, intelijen dan pelaporan.
5. Respon
Aspek respon terdiri dari sub aspek penahanan, penanggulangan, pemulihan, kegiatan paska insiden dan pelaporan.

III. Metodologi

Cara pengukuran dilakukan dengan menjawab pertanyaan-pertanyaan mengenai penerapan keamanan siber pada aspek tata kelola, identifikasi, proteksi, deteksi dan respon pada instrument CSM yang telah disiapkan. Disamping itu, dilakukan juga wawancara/diskusi dan dilihat ketersediaan dokumen keamanan siber.

Berdasarkan hasil pengisian setiap pertanyaan pada masing-masing aspek, secara otomatis akan dihasilkan nilai dalam grafik *cyber security maturity*. Nilai tersebut menggambarkan kondisi kematangan keamanan siber pada suatu organisasi pada setiap aspek yang ada.

Level yang digunakan dalam *framework cyber security maturity* ini terdiri dari 5 level, dimulai level 1 hingga level 5.

1. Level 1 (implementasi awal)

Rentang nilai yang dikategorikan pada level 1, yaitu mulai dari 0 sampai dengan 1,5. Pada level 1 ini menggambarkan bahwa dalam penerapan keamanan siber tidak ada proses yang terorganisir, bersifat informal, tidak dilakukan secara konsisten, dan tidak dilakukan secara berkelanjutan. Oleh karena itu, penerapan keamanan siber

pada level ini tidak dapat terukur dengan baik dan organisasi memiliki tingkat risiko siber yang sangat tinggi.

2. Level 2

Rentang nilai yang dikategorikan pada level 2 yaitu lebih dari 1.5 sampai dengan kurang dari 2.5. Pada level 2 ini menggambarkan bahwa dalam penerapan keamanan siber proses yang dilakukan sudah terorganisir, bersifat informal, dilakukan secara berulang namun belum konsisten, serta belum dilakukan secara berkelanjutan. Oleh karena itu, penerapan keamanan siber pada level ini tidak dapat terukur dengan baik dan organisasi memiliki tingkat risiko siber yang tinggi.

3. Level 3

Rentang nilai yang dikategorikan pada level 3 yaitu mulai dari 2.5 sampai dengan kurang dari 3.5. Pada level 3 ini menggambarkan bahwa dalam penerapan keamanan siber proses yang dilakukan sudah terorganisir dengan jelas, bersifat formal, dilakukan secara berulang, dilakukan reviu berkala, dan konsisten. Namun penerapan perubahan belum dilakukan secara berkelanjutan. Oleh karena itu, penerapan keamanan siber pada level ini mulai dapat terukur.

4. Level 4

Rentang nilai yang dikategorikan pada level 4 yaitu mulai dari 3.5 sampai dengan kurang dari 4.5. Pada level 4 ini menggambarkan bahwa dalam penerapan keamanan siber proses yang dilakukan sudah terorganisir dengan baik namun belum dilakukan proses otomatisasi, bersifat formal, dilakukan secara berulang dan direviu secara berkala, serta implementasi perbaikan dilakukan secara berkelanjutan. Oleh karena itu, penerapan keamanan siber pada level ini dapat terukur dengan baik.

5. Level 5

Rentang nilai yang dikategorikan pada level 5 yaitu mulai dari 4.5 sampai dengan 5. Pada level 5 ini menggambarkan bahwa dalam penerapan keamanan siber proses yang dilakukan sudah terorganisir dengan baik, diterapkan proses otomatisasi, bersifat formal, dilakukan secara berulang secara konsisten, direviu berkala, serta penerapan perbaikan dilakukan secara berkelanjutan. Oleh karena itu, penerapan

keamanan siber pada level ini dapat terukur dengan sangat baik dan keamanan siber telah menjadi bagian budaya secara menyeluruh di organisasi

IV. Pelaksanaan Kegiatan

1. *Self Assesstment*

Pengisian secara mandiri oleh responden dari Bidang Siber dan Sandi, Diskominfotik Provinsi DKI Jakarta dilakukan pada tanggal 30 November 2020.

2. Validasi Penilaian CSM

Kegiatan validasi dilakukan dengan metode wawancara/diskusi dan melihat ketersediaan dokumen keamanan siber secara virtual (menggunakan *zoom meeting*). Kegiatan validasi dilaksanakan pada tanggal 2 Desember 2020.

HASIL KEGIATAN

I. Tim Badan Siber dan Sandi Negara

Tim dari Badan Siber dan Sandi Negara yang melakukan validasi hasil pengisian *framework* CSM, yaitu:

1. Agus Indramawan, S.ST
Sandiman Muda, Direktorat Penanggulangan dan Pemulihan Pemerintah
2. Desi Wulandari, S.S.T.TP
Sandiman Pertama, Direktorat Penanggulangan dan Pemulihan Pemerintah
3. Siti Rahmawati, S.Kom.
Perespon Insiden, Direktorat Penanggulangan dan Pemulihan Pemerintah
4. Moch. Yusuf, A.Md.
Perespon Insiden, Direktorat Penanggulangan dan Pemulihan Pemerintah

II. Informasi *Stakeholder*

Nama Instansi/Lembaga : Dinas Komunikasi, Informatika dan Statistik
Provinsi DKI Jakarta

Alamat : Jalan Merdeka Selatan No. 8-9 Blok G Lantai 13,
Jakarta Pusat

Nomor Telp./Fax. : (021) 3823253/3823449

Email : diskominfotik@jakarta.go.id

Pimpinan Unit Kerja : Atika Nur Rahmania, S.IP., M.Si.
Kepala Diskominfotik Provinsi DKI Jakarta

Narasumber Instansi/Lembaga :

1. Boedi Setiawan, S.H.
Kepala Bidang Siber dan Sandi
2. Tony Yudianto, ST
Kepala Seksi Layanan Siber dan Sandi, Bidang Siber dan Sandi

3. Reihan Adinata, ST
Kepala Seksi Tata Kelola Siber dan Sandi, Bidang Siber dan Sandi
4. Lamria Simatupang, S.Si
Pelaksana Seksi Pengendalian, Bidang Siber dan Sandi
5. Rycan Fahmi, S.Kom
Pelaksana Seksi Layanan, Bidang Siber dan Sandi
6. Andy Susanto, S.Kom
Pelaksana Seksi Pengendalian, Bidang Siber dan Sandi
7. Taufik Hidayat
Pelaksana Seksi Tata Kelola, Bidang Siber dan Sandi
8. Ardian Oktadika, ST
Security Specialist Pentester, Bidang Siber dan Sandi
9. Maman Firmansyah, S.Kom
Network & Device Specialist, Bidang Siber dan Sandi
10. Budi Wibowo, ST, MT
Security Analis Riset dan Development, Bidang Siber dan Sandi
11. Rina Yuliani Fadila, ST
Document Control, Bidang Siber dan Sandi

III. Deskripsi Ruang Lingkup Penilaian

1. Ruang Lingkup Penilaian : Bidang Siber dan Sandi
2. Unit Kerja : Diskominfo Provinsi DKI Jakarta
3. Fungsi Kerja

Bidang Siber dan Sandi, Diskominfo Provinsi DKI Jakarta memiliki tugas dan fungsi sebagaimana diatur dalam Peraturan Gubernur Daerah Khusus Ibukota Jakarta Nomor 144 Tahun 2019 tentang Organisasi dan Tata Kerja Dinas Komunikasi, Informatika dan Statistik. Tugas Pokok Bidang Siber dan Sandi adalah menyelenggarakan layanan siber dan sandi serta keamanan informasi. Untuk menyelenggarakan tugas pokok, Bidang Siber dan Sandi mempunyai fungsi sebagai berikut:

- a. penyusunan Rencana Strategis, Rencana Kerja dan Rencana Kerja dan Anggaran Dinas sesuai dengan lingkup tugasnya;
- b. pelaksanaan Dokumen Pelaksanaan Anggaran Dinas sesuai dengan lingkup tugasnya;
- c. perumusan kebijakan, proses bisnis, standar dan prosedur Dinas sesuai dengan lingkup tugasnya;
- d. pelaksanaan kebijakan, proses bisnis, standar dan prosedur Dinas sesuai dengan lingkup tugasnya;
- e. penyusunan arsitektur keamanan siber dan sandi serta mekanisme pemanfaatan sertifikat elektronik/tanda tangan elektronik di lingkungan Pemerintah Daerah;
- f. pelaksanaan literasi dan asistensi penerapan SMPI;
- g. pelaksanaan literasi dan asistensi pengendalian keamanan siber dan sandi;
- h. pelaksanaan identifikasi kerentanan dan penilaian risiko keamanan sistem elektronik;
- i. pelaksanaan asistensi hardening keamanan sistem elektronik;
- j. pelaksanaan penanggulangan dan pemulihan insiden keamanan informasi;
- k. pelaksanaan audit SMKI dan keamanan SPBE;
- l. pelaksanaan pembangunan sistem informasi keamanan siber dan sandi;
- m. pelaksanaan layanan pemanfaatan sertifikat elektronik di Pemerintah Daerah;
- n. pelaksanaan pengelolaan perangkat teknologi keamanan informasi dan sarana pendukung di Pemerintah Daerah;
- o. pelaksanaan pengelolaan Security Operation Center (SOC) siber dan sandi Pemerintah Daerah;
- p. pelaksanaan pengembangan layanan keamanan siber dan sandi;
- q. pelaksanaan jaring komunikasi sandi;
- r. pelaksanaan perlindungan informasi pada kegiatan penting Pemerintah Daerah melalui teknik pengamanan gelombang frekuensi atau sinyal;
- s. pelaksanaan perlindungan informasi pada aset/fasilitas penting milik atau yang akan digunakan Pemerintah Daerah melalui kegiatan kontra penginderaan;
- t. pelaksanaan forensik digital, penanggulangan pemulihan dan proteksi keamanan sistem elektronik;
- u. pelaksanaan layanan pointing nama domain dan sub domain bagi lembaga sesuai dengan standar keamanan informasi;
- v. pelaksanaan koordinasi, pemantauan, evaluasi, pelaporan, dan pertanggungjawaban pelaksanaan tugas Dinas sesuai dengan lingkup tugasnya; dan
- w. pelaksanaan tugas kedinasan lain yang diberikan oleh Kepala Dinas.

4. Kondisi Umum


a. Struktur organisasi Bidang Siber dan Sandi, Diskominfotik Provinsi DKI Jakarta

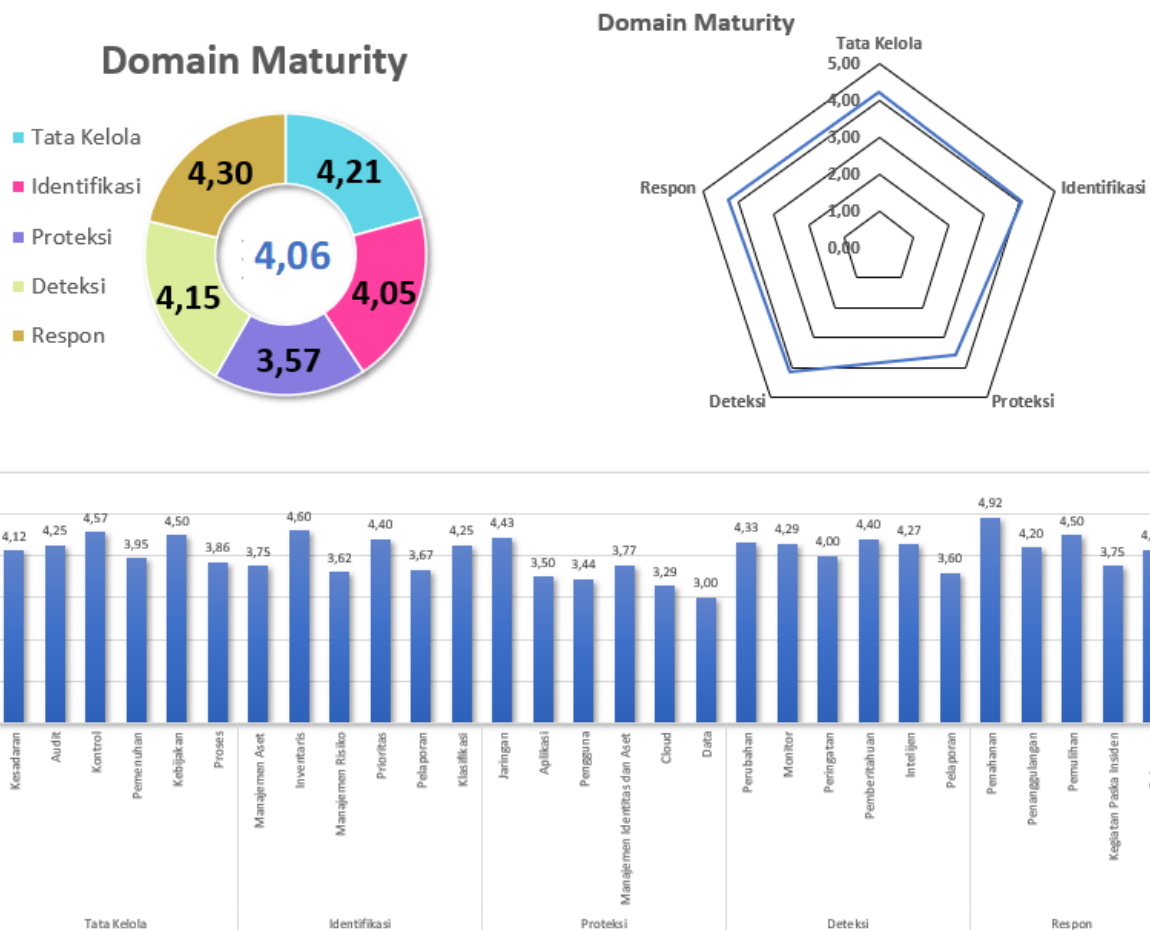


b. Jumlah SDM pengelola di Bidang Siber dan Sandi sejumlah 24 orang, yang terdiri dari 9 pegawai ASN dan 15 pegawai Non ASN.

IV. Hasil Penilaian CSM

Berdasarkan hasil validasi pengisian CSM di Bidang Siber dan Sandi, Diskominfotik Provinsi DKI Jakarta diperoleh hasil sebagai berikut:

<div>  <h3>CSM TOOLS</h3> </div>									
Tata Kelola		Identifikasi		Proteksi		Deteksi		Respon	
4,21		4,05		3,57		4,15		4,30	
Kesadaran	4,12	Manajemen Aset	3,75	Jaringan	4,43	Perubahan	4,33	Penahanan	4,92
Audit	4,25	Inventaris	4,60	Aplikasi	3,50	Monitor	4,29	Penanggulangan	4,20
Kontrol	4,57	Manajemen Risiko	3,62	Pengguna	3,44	Peringatan	4,00	Pemulihan	4,50
Pemenuhan	3,95	Prioritas	4,40	Manajemen Identitas dan Aset	3,77	Pemberitahuan	4,40	Kegiatan Paska Insiden	3,75
Kebijakan	4,50	Pelaporan	3,67	Cloud	3,29	Intelijen	4,27	Pelaporan	4,14
Proses	3,86	Klasifikasi	4,25	Data	3,00	Pelaporan	3,60		



Berdasarkan hasil penilaian instrumen CSM, diperoleh hasil sebagai berikut:

Total Score Indeks Kematangan : 4,06

Sehingga perhitungan penentuan Level Kematangan didapatkan tingkat level kematangan di Bidang Siber dan Sandi, Diskominfotik Provinsi DKI Jakarta sebagai berikut :

Tingkat Kematangan Level 4

V. Kekuatan/Kematangan

Berdasarkan hasil validasi penilaian kematangan keamanan siber (*Cyber Security Maturity*), dapat disimpulkan kondisi kekuatan keamanan siber pada Bidang Siber dan Sandi, Diskominfotik Provinsi DKI Jakarta sebagai berikut:

Tata Kelola

1. Organisasi secara berkala dan berkelanjutan telah menerapkan program kesadaran keamanan informasi pada sebagian besar pegawai.
2. Organisasi telah melaksanakan audit dan kontrol keamanan siber dengan melakukan kegiatan *vulnerability scanning* dan *risk assessment* oleh tim yang sudah dibentuk.
3. Organisasi telah melakukan pelatihan keamanan informasi secara terjadwal untuk pegawai berdasarkan *roadmap baseline* pendidikan dan pelatihan.
4. Organisasi secara formal membuat dan menyampaikan kebijakan/prosedur keamanan informasi.
5. Organisasi telah mewajibkan pegawai dan kontraktor menerapkan kebijakan/prosedur keamanan informasi.
6. Organisasi telah memastikan dalam pengembangan perangkat lunak/sistem informasi/aplikasi dilakukan analisis statis dan dinamis, dan memastikan versi yang dipakai masih memiliki dukungan pengembang.
7. Organisasi secara berkala melakukan analisis risiko keamanan fisik dan sistem elektronik.
8. Organisasi telah memperhatikan dasar-dasar keamanan informasi, seperti pemisahan lingkungan *production* dan *development*, melakukan pengujian komponen penting dari aplikasi, menerapkan praktik *secure coding* dan memastikan dilakukan pengecekan kesalahan pada semua input pada aplikasi, menerapkan NAT secara menyeluruh, filterisasi lampiran email, pengaturan *Singe ID / Single Sign On* untuk melakukan akses kepada aplikasi milik organisasi, penggunaan NAC, WAF, AV, IDS/IPS.
9. Organisasi telah memiliki dokumen BCP, DRP, penilaian risiko keamanan dan pengendaliannya, serta diriview secara berkala.

Identifikasi

1. Organisasi telah melakukan perencanaan kapasitas secara berkala untuk memastikan bahwa semua aset perangkat dan aplikasi sesuai dengan kebutuhan.
2. Organisasi telah melakukan inventaris terhadap asset perangkat lunak dan perangkat keras secara berkala dan setiap ada perubahan.
3. Organisasi telah mengidentifikasi dan mebatasi akses perangkat yang tidak diizinkan oleh organisasi.
4. Organisasi telah melakukan klasifikasi informasi dan melakukan inventarisasi.
5. Organisasi telah memiliki kebijakan pembatasan penggunaan aset organisasi untuk kepentingan pribadi.
6. Organisasi telah memiliki kebijakan dan implementasi mengenai retensi data sensitif.
7. Organisasi secara berkala telah melakukan *vulnerability scanning/penetration testing* terhadap semua aset perangkat dan aplikasi organisasi.
8. Organisasi telah melakukan klasifikasi secara terorganisir dan berkelanjutan dalam klasifikasi TI dan *cyber threat*.
9. Organisasi telah melakukan segmentasi jaringan berdasarkan fungsionalitas.
10. Organisasi telah konsisten menjadikan aspek keamanan menjadi pertimbangan dan diprioritaskan dalam beberapa pengambilan keputusan TI. Upaya remedasi telah didasarkan pada level risiko serta dilakukan langkah proteksi untuk memprioritaskan data dan asset kritis.
11. Organisasi telah konsisten melakukan manajemen risiko dengan menerapkan *screening* terhadap pihak ketiga ketika menggunakan asset mereka pada jaringan organisasi. Selain itu, terdapat *risk register* yang didokumentasikan untuk semua aplikasi.

Proteksi

1. Organisasi telah melakukan proteksi terhadap jaringan dengan memberikan *firewall* dan IPS beserta pengaturannya, mengkonfigurasi sistem dan protokol

- terenkripsi, serta melakukan *filtering* pada *inbound /outbond network traffic* serta *filtering* terhadap layanan DNS.
2. Organisasi telah melakukan manajemen aplikasi yang dimiliki dengan konsisten, berupa *patching* aplikasi, memastikan aplikasi masih memiliki *update support* dan memastikan *master images server* tersimpan dengan aman.
 3. Organisasi telah menerapkan pembatasan akun pengguna dan perlindungan user dengan menggunakan *URL filtering*, *device control*, dan *application control*.
 4. Organisasi telah melakukan manajemen identitas dan akses dengan menggunakan identitas dan akses kengguna untuk pembatasan hak akses pada jaringan, *database*, transaksi dan data lain.
 5. Organisasi telah membatasi aplikasi yang dapat diunduh, diinstal dan dioperasikan dan telah menggunakan anti virus pada semua perangkat endpoints, termasuk server.
 6. Organisasi telah menggunakan server terpisah untuk semua aplikasi yang dipakai organisasi.
 7. Email system di organisasi telah memiliki pengecekan otomatis terhadap spam/phishing/malware.

Deteksi

1. Organisasi telah menerapkan monitoring (pemantauan dan notifikasi) terhadap aktivitas lalu lintas jaringan, log dari perangkat *security control*, jaringan dan aplikasi.
2. Organisasi telah melakukan *record* terhadap perubahan dengan deteksi perubahan konfigurasi perangkat jaringan.
3. Organisasi telah memiliki sistem monitoring yang aktif terhadap akses fisik dan logic dan mempersiapkan peningkatan keterampilan bagi tim monitoring.
4. Dalam hal peringatan, organisasi sudah dapat mendeteksi kegagalan login pada akun, adanya alert jika terdapat port yang tidak sah terdeteksi pada suatu sistem.

5. Organisasi telah memiliki perangkat anti-malware yang secara otomatis melakukan scanning terhadap removable media yang terhubung ke perangkat.
6. *System ticketing* sudah diberlakukan berdasarkan dampak dan *event notification* berbeda-beda untuk setiap jenis eskalasi.
7. Organisasi telah memiliki sistem untuk mendeteksi ancaman siber.

Respon

1. Organisasi telah memiliki SOP dan form pelaporan penanganan insiden yang diketahui oleh pihak terkait.
2. Organisasi telah melakukan latihan respon insiden secara rutin dan memberikan pelatihan kepada para personil TI dan Sebagian besar pegawai mengenai tentang cara identifikasi, penanganan dan pelaporan suatu insiden.
3. Organisasi memastikan desain jaringan yang aman dengan pemisahan server DMZ ketika terjadi *compromise*.
4. Organisasi memiliki sumber daya redundan yang cukup (75%-95%) untuk kondisi sistem kritis yang terganggu karena insiden siber.
5. Organisasi memiliki format baku untuk pencatatan respon insiden, dan tim respon dipastikan dapat melakukan pencatatan setiap langkah dalam penanganan insiden
6. Dalam kegiatan pasca insiden, organisasi dapat memastikan pencapaian SLA dalam penanganan insiden

VI. Kelemahan/Kekurangan

Tata Kelola

1. Organisasi belum melakukan dan mendokumentasikan simulasi serangan phishing secara berkala minimal satu kali setiap tahunnya.
2. Organisasi belum memiliki BCP dan DRP yang mencakup *backup* dan *restoration* dari data pribadi.
3. Kegiatan *threat hunting* masih belum dilakukan secara berkala/rutin.

4. Belum adanya kontrol untuk mengukur kepatuhan pengguna terhadap kebijakan keamanan informasi organisasi, misalnya seperti *survey* atau yang lainnya.
5. Pelatihan terkait keamanan informasi (seperti *secure authentication*, berbagai bentuk serangan *social engineering* dan sejenisnya) baru diikuti oleh sebagian pegawai.

Identifikasi

1. Metode atau standar untuk klasifikasi data organisasi belum dikontrol dengan DRM (*Digital Right Management*) dan belum didukung dengan DLP (*Data Lost Prevention*).
2. Pengelolaan data log keamanan informasi belum setiap hari secara otomatis dilaporkan kepada manajemen.
3. Organisasi belum menon-aktifkan aset perangkat dan aplikasi yang tidak diperlukan oleh organisasi (seperti port, *akses smartphone*, dll).
4. Organisasi belum mengidentifikasi seluruh aset berdasarkan klasifikasi kritikalitas.
5. Masih ada data otentikasi yang disimpan di perangkat *browser end user*.

Proteksi

1. Karyawan di organisasi belum mengaktifkan fitur *wireless* pada perangkat yang hanya sesuai kebutuhan organisasi.
2. Organisasi belum menerapkan whitelist aplikasi yang memastikan hanya *authorized software library* dan *signed script* yang dapat dijalankan oleh sistem.
3. Organisasi belum melakukan pembatasan penggunaan scripting tools.
4. Baru sebagian laptop pegawai yang secara otomatis meminta kata sandi setelah beberapa saat tidak aktif.
5. Belum semua media penyimpanan eksternal di organisasi dilakukan enkripsi.
6. Organisasi belum menggunakan *next generation endpoint protection*.
7. Organisasi belum secara optimal memanfaatkan *Multi-Factor Authentication* atau verifikasi *One Time Password (OTP)* melalui SMS, *WhatsApp Messenger*, Telepon,

Elektronik Mail, Google Authenticator, atau media lainnya untuk transaksi yang berisiko tinggi.

8. Organisasi belum menerapkan *single sign-on* pada cloud dan belum membatasi akses *traffic* ke cloud hanya dari alamat IP yang dikenal.

Deteksi

1. Organisasi masih mendeteksi *wireless access point* yang terhubung ke jaringan LAN secara manual.
2. Belum ada notifikasi secara otomatis kepada admin saat terjadi kegagalan login pada akun admin pada perangkat jaringan, server dan aplikasi.
3. Organisasi belum memiliki sistem untuk memonitoring dan mencegah kehilangan data sensitif (belum menggunakan DLP).
4. Organisasi belum mengaktifkan DNS query logging dalam mendeteksi hostname lookups untuk mengetahui adanya malicious domain.
5. Mekanisme sharing informasi hasil deteksi baru untuk internal saja.

Respon

1. Pelatihan tentang cara identifikasi, penanganan dan pelaporan suatu insiden baru dilaksanakan untuk personil IT dan sebagian pegawai.
2. Laporan insiden di organisasi belum dilaporkan ke *top management* dan ke pihak eksternal yang berkepentingan.

VII. Rekomendasi

1. Untuk meningkatkan aspek Tata Kelola keamanan siber di Bidang Siber dan Sandi, Diskominfo Provinsi DKI Jakarta maka dapat dilakukan hal-hal sebagai berikut:
 - a. Organisasi perlu melakukan simulasi serangan phishing secara berkala minimal satu kali setiap tahunnya.
 - b. Dokumen BCP dan DRP organisasi sebaiknya mencakup *backup* dan *restoration* dari data pribadi.

- c. Organisasi perlu melakukan kegiatan *threat hunting* secara berkala.
 - d. Organisasi menyediakan kontrol untuk mengukur kepatuhan pengguna terhadap kebijakan keamanan informasi organisasi, misalnya seperti *survey*/kuesioner yang memuat pengetahuan dan pelaksanaan terhadap kebijakan keamanan informasi organisasi.
2. Untuk meningkatkan aspek Identifikasi keamanan siber di Bidang Siber dan Sandi, Diskominfo Provinsi DKI Jakarta, maka dapat dilakukan hal-hal sebagai berikut:
- a. Metode atau standar untuk klasifikasi data organisasi sebaiknya dikontrol dengan DRM (*Digital Right Management*) dan DLP (*Data Lost Prevention*).
 - b. Organisasi perlu menon-aktifkan aset perangkat dan aplikasi yang tidak diperlukan oleh organisasi (seperti port, *akses smartphone*, dll).
 - c. Organisasi melakukan identifikasi seluruh aset berdasarkan klasifikasi kritikalitas.
 - d. Data otentikasi sebaiknya tidak disimpan di perangkat *browser end use*
3. Untuk meningkatkan aspek Proteksi keamanan siber di Bidang Siber dan Sandi, Diskominfo Provinsi DKI Jakarta, maka dapat dilakukan hal-hal sebagai berikut:
- a. Diperlukan penambahan perangkat yang mampu mendeteksi *malware*, perilaku anomali pengguna atau serangan secara otomatis.
 - b. Diperlukan whitelist aplikasi yang memastikan hanya *authorized software library* dan *signed script* yang dapat dijalankan oleh sistem.
 - c. Diperlukan pembatasan penggunaan scripting tools.
 - d. Diperlukan kebijakan bahwa laptop pegawai secara otomatis meminta kata sandi setelah beberapa saat tidak aktif.
 - e. Semua media penyimpanan eksternal di organisasi sebaiknya dilakukan enkripsi.
 - f. Penyusunan Kebijakan yang mengatur mengenai penggunaan perangkat, jaringan dan aplikasi milik pengguna.
 - g. Pertimbangan untuk menggunakan *Multi-Factor Authentication* dan Verifikasi *One Time Password* untuk Sistem Informasi dengan transaksi berisiko tinggi.

4. Untuk meningkatkan aspek Deteksi keamanan siber di Bidang Siber dan Sandi, Diskominfo Provinsi DKI Jakarta, maka dapat dilakukan hal-hal sebagai berikut:
 - a. Sebaiknya ada notifikasi secara otomatis kepada admin saat terjadi kegagalan login pada akun admin pada perangkat jaringan, server dan aplikasi.
 - b. Mekanisme sharing informasi hasil deteksi sebaiknya dilakukan untuk internal dan eksternal.
5. Untuk meningkatkan aspek Respon keamanan siber di Bidang Siber dan Sandi, Diskominfo Provinsi DKI Jakarta, maka dapat dilakukan hal-hal sebagai berikut:
 - a. Organisasi dapat menyelenggarakan simulasi penanganan insiden siber, meliputi insiden malware, *web defacement*, DDOS, *ransomware*, dan sejenisnya.
 - b. Laporan insiden di organisasi sebaiknya dilaporkan ke *top management* dan ke pihak eksternal yang berkepentingan
 - c. SOP terkait penanganan insiden siber (malware, *web defacement*, DDOS, *ransomware*, dan sejenisnya) sebaiknya dilakukan review secara berkala untuk melihat efektivitas dari SOP tersebut.
6. Ruang lingkup penilaian CSM di tahun berikutnya sebaiknya diperluas sampai Diskominfo Provinsi DKI Jakarta atau seluruh organisasi Pemerintah Provinsi DKI Jakarta, dengan tujuan untuk mengetahui tingkat kematangan keamanan siber di ruang lingkup tersebut. Dengan adanya tingkat kematangan ini diharapkan dapat memberikan gambaran dan mempermudah organisasi untuk mengetahui kekuatan dan kelemahan yang perlu ditingkatkan pada setiap aspek keamanan siber. Sehingga dapat dijadikan acuan dalam menyusun strategi peningkatan kematangan *cyber security* dan pengelolaan keamanan siber dengan tepat sasaran



PENUTUP

Demikian disampaikan laporan kegiatan penilaian CSM pada Bidang Siber dan Sandi, Diskominfo Provinsi DKI Jakarta, Pemerintah Provinsi DKI Jakarta sebagai bahan masukan bagi pimpinan dalam menentukan kebijakan lebih lanjut.

Jakarta, Desember 2020

Mengetahui,
Kasubdit PPPDW 1

Ketua Tim BSSN

(Sriyanto, S.Sos., M.M.)
NIP. 19630921 198311 1 002

(Agus Indramawan, S.ST)
NIP. 19830822 200312 1 005