2020

LAPORAN

HASIL PENILAIAN

CYBER SECURITY MATURITY (CSM)

DINAS KOMINFO DAN STATISTIK

PROVINSI GORONTALO

PENDAHULUAN

I. Tujuan Kegiatan

Kegiatan ini bertujuan untuk mengetahui tingkat kematangan keamanan siber di lingkungan Dinas Komunikasi, Informatika, dan Statistik Provinsi Gorontalo. 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 Dinas Komunikasi, Informatika, dan Statistik Provinsi Gorontalo maupun Badan Siber dan Sandi Negara (BSSN) dapat menyusun strategi peningkatan kematangan keamanan siber (*Cyber Security Maturity*) dengan tepat sasaran.

II. Ruang Lingkup Kegiatan

Kegiatan yang dilaksanakan meliputi pemetaan aspek pengelolaan keamanan siber yang meliputi beberapa aspek sebagai berikut :

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 resiko, 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 Kegiatan

Metodologi yang digunakan berdasarkan hasil pengisian instrumen pemetaan Cyber Security Maturity (CSM), wawancara/diskusi, dan melihat ketersediaan dokumen dan/atau data dukung pendukung pengisian instrumen. Hasil diberikan dalam bentuk Indeks Kematangan, Level Kematangan dan bagan berbentuk radar yang menjelaskan maturitas tiap aspek Keamanan Siber.

Penentuan Level Kematangan Keamanan Siber diukur berdasarkan Indeks Kematangan yang didapat. Konversi Indeks Kematangan menjadi Level Kematangan menggunakan formula:

Nilai Level Kematangan dikategorikan menjadi :

- Level 1 (Implementasi Awal)

  Rentang nilai yang dikategorikan pada level 1 yaitu mulai dari 0 sampai dengan 1.5. Pada level 1 (satu) 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.

- Level 2 (Implementasi Berulang)

  Rentang nilai yang dikategorikan pada level 2 yaitu lebih dari 1.5 sampai dengan kurang dari 2.5. Pada level 2 (dua) 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

- Level 3 (Implementasi Terdefinisi)

  Rentang nilai yang dikategorikan pada level 3 yaitu mulai dari 2.5 sampai dengan kurang dari 3.5. Pada level 3 (tiga) 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.
- Level 4 (Implementasi Terkelola)

  Rentang nilai yang dikategorikan pada level 4 yaitu mulai dari 3.5 sampai dengan kurang dari 4.5. Pada level 4 (empat) 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.
- Level 5 (Implementasi Optimal)

  Rentang nilai yang dikategorikan pada level 5 yaitu mulai dari 4.5 sampai dengan 5. Pada level 5 (lima) 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. Pengisian setiap pertanyaan dari *Tools* CSM oleh responden dari Dinas Komunikasi, Informatika, dan Statistik Provinsi Gorontalo dengan asitensi BSSN dilakukan pada tanggal 24 - 25 November 2020.

2. Validasi Pemetaan CSM

   Kegiatan validasi dilakukan dengan metode wawancara/diskusi dan melihat ketersediaan dokumen keamanan siber. Kegiatan validasi dilaksanakan pada 24 - 25 November 2020.

HASIL KEGIATAN

I. Informasi *Stakeholder*

Nama Instansi/Lembaga : Dinas Komunikasi, Informatika, dan Statistik Provinsi Gorontalo
Alamat : Jalan Thaeb M. Gobel, Bone Bolango -Gorontalo
Nomor Telp./Fax. : (0435) 8532554
Email : kominfo@gorontaloprov.go.id

Narasumber Instansi/Lembaga :
Fried Dewi Husain Ahmad, S.Kom., M.Eng.
Kabid Penyelenggaran E-Government

II. Deskripsi Ruang Lingkup Penilaian

1. Ruang Lingkup Penilaian :
   ☐ Organisasi Keseluruhan ☐ Regional, Kanwil, Cabang √ Unit Kerja ☐ Lainnya
2. Unit Kerja : Diskominfo dan Statistik Provinsi Gorontalo
3. Fungsi Kerja

   Dinas Komunikasi, Informatika, dan Statistik Pemerintah Provinsi Gorontalo memiliki tugas dan fungsi Uraian tugasnya diatur dalam Peraturan Gubernur Gorontalo Nomor 68 Tahun 2016 tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi, serta Tata Kerja Dinas Komunikasi, Informatika, dan Statistik Provinsi Gorontalo.

   Untuk menyelenggarakan tugas pokok Dinas Komunikasi, Informatika, dan Statistik Provinsi Gorontalo mempunyai fungsi sebagai berikut :

   a. Penyelenggaraan perumusan kebijakan, pelaksanaan kebijakan, pelaksanaan evaluasi dan pelaporan dibidang pengelolaan informasi untuk

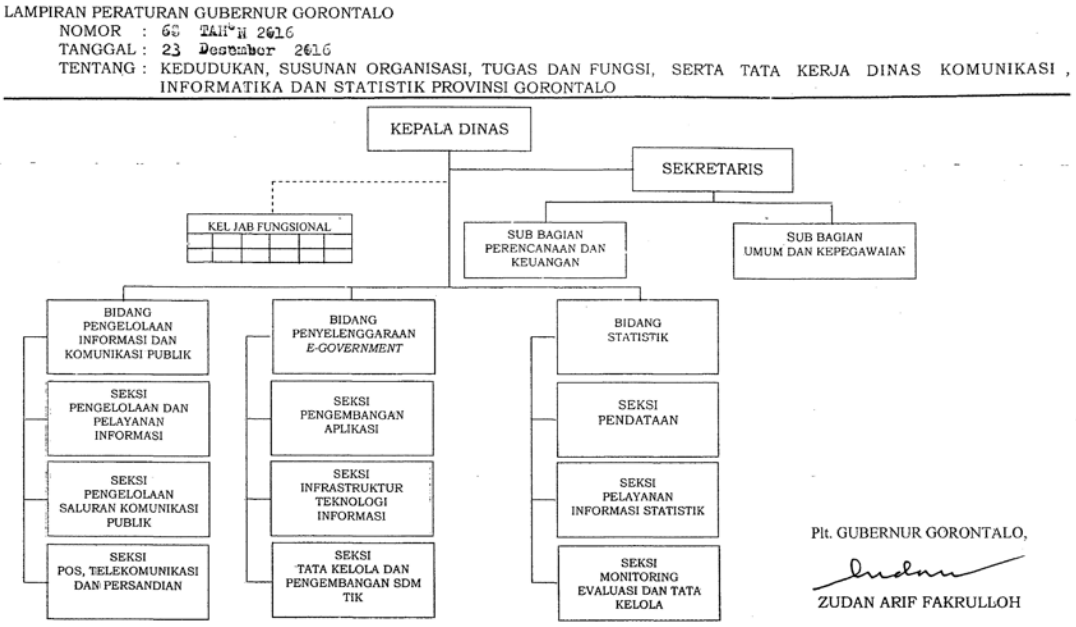
mendukung kebijakan Nasional dan pemerintah daerah, penyediaan konten lintas sektoral, pengelolaan media dan penguatan kapasitas sumber daya komunikasi publik, layanan Infrastruktur dasar TIK, layanan pengembangan intranet dan penggunaan akses internet, layanan pengembangan dan pengelolaan aplikasi generik, integrasi layanan publik dan kepemerintahan, layanan sistem komunikasi intra Pemerintah, tata kelola E-Government, Peningkatan SDM TIK, Menyelenggarakan pengelolaan domain dan sub domain, penyelenggaraan ekosistem TIK *Smart Province*, keamanan informasi dan komunikasi sandi, serta layanan data dan informasi statistika sektoral lingkup provinsi;

b. Penyelenggaraan perumusan, penetapan, pengaturan dan koordinasi serta pelaksanaan kebijakan teknis pos dan telekomunikasi, sarana komunikasi dan diseminasi informasi, telematika serta pengolahan data elektronik;
c. Penyelenggaraan fasilitasi dan pengendalian komunikasi dan informatika meliputi pos dan telekomunikasi, sarana komunikasi dan diseminasi informasi, telematika, serta pengolahan data elektronik;
d. Koordinasi pelaksanaan tugas, pembinaan, dan pemberian dukungan administrasi kepada seluruh unsur organisasi di lingkungan Dinas Komunikasi Informatika dan Statistik;
e. Pengelolaan barang milik/kekayaan daerah yang menjadi tanggung jawab Dinas Komunikasi Informatika dan Statistik;
f. Pengawasan atas pelaksanaan tugas di lingkungan Dinas Komunikasi Informatika dan Statistik;
g. Pelaksanaan bimbingan teknis dan supervisi atas pelaksanaan urusan Dinas Komunikasi Informatika dan Statistik di daerah;
h. Pelaksanaan penelitian dan pengembangan di bidang pengelolaan informasi dan komunikasi publik, penyelenggaraan E-government serta statistik;
i. Pelaksanaan dukungan substantif kepada seluruh unsur organisasi di lingkungan Dinas Komunikasi Informatika dan Statistik; dan

j. Pelaksanaan fungsi lain yang diberikan oleh Gubernur.

Dalam melaksanakan tugas dan fungsinya, Dinas Komunikasi Informatika dan Statistik Provinsi Gorontalo memiliki susunan organisasi yang terdiri atas :

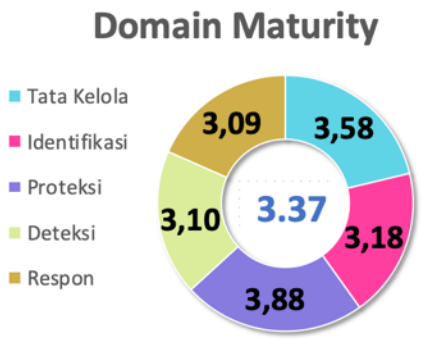
a. Kepala Dinas;
b. Sekretariat;
c. Kepala Bidang Pengelolaan Informasi dan Komunikasi Publik;
d. Kepala Bidang Penyelenggaraan E-govemment;
e. Kepala Bidang Statistik; dan
f. Kelompok Jabatan Fungsional.

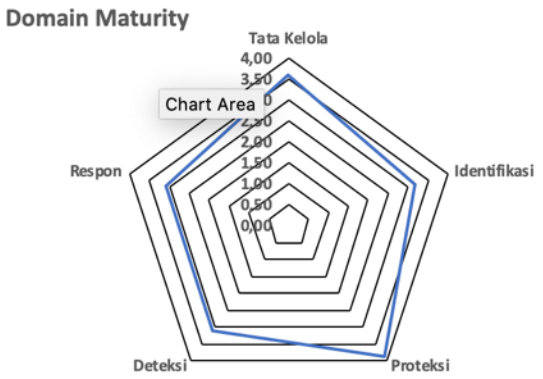


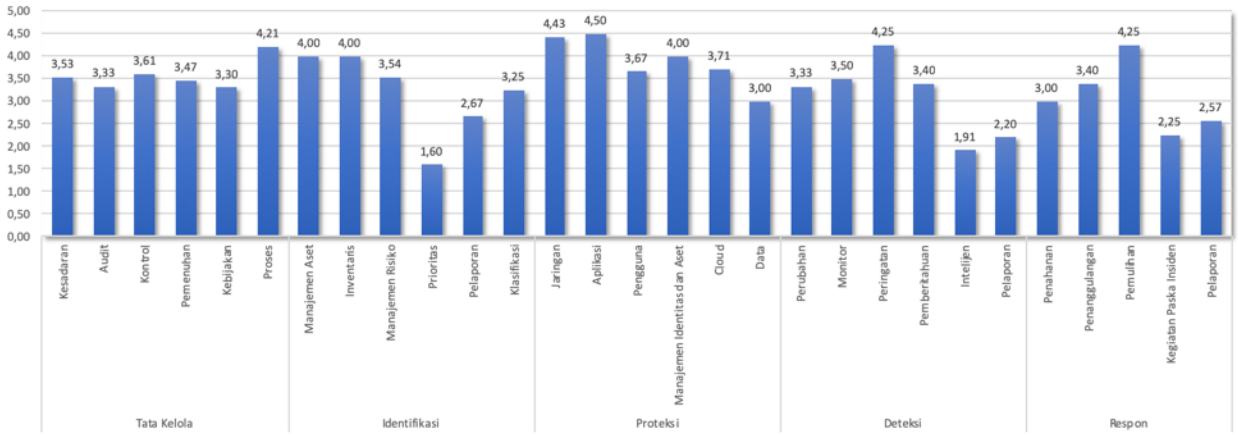
III. Hasil Penilaian CSM

Berdasarkan wawancara dan diskusi dalam rangka validasi pengisian *Cyber Security Maturity* diperoleh hasil sebagai berikut:

Tata Kelola		Identifikasi		Proteksi		Deteksi		Respon	
3,58		3,18		3,88		3,10		3,09	
Kesadaran	3,53	Manajemen Aset	4,00	Jaringan	4,43	Perubahan	3,33	Penahanan	3,00
Audit	3,33	Inventaris	4,00	Aplikasi	4,50	Monitor	3,50	Penanggulangan	3,40
Kontrol	3,61	Manajemen Risiko	3,54	Pengguna	3,67	Peringatan	4,25	Pemulihan	4,25
Pemenuhan	3,47	Prioritas	1,60	Manajemen Identitas dan Aset	4,00	Pemberitahuan	3,40	Kegiatan Paska Insiden	2,25
Kebijakan	3,30	Pelaporan	2,67	Cloud	3,71	Intelijen	1,91	Pelaporan	2,57
Proses	4,21	Klasifikasi	3,25	Data	3,00	Pelaporan	2,20		







Berdasarkan hasil penilaian instrumen CSM, diperoleh hasil sebagai berikut:

Total Score Indeks Kematangan : 3,37

Sehingga perhitungan penentuan Level Kematangan didapatkan tingkat level kematangan sebagai berikut :

Tingkat Kematangan Level 3

IV. Kekuatan/Kematangan

Berdasarkan hasil validasi penilaian kematangan keamanan siber (*Cyber Security Maturity*), dapat disimpukan kondisi kekuatan keamanan siber pada Dinas Kominfo,Informatika & Statistik Provinsi Gorontalo sebagai berikut:

a. Aspek Tata Kelola

1. Program pemahaman kesadaran keamanan informasi telah dilakukan untuk semua karyawan secara berkelanjutan setidaknya setahun sekali.
2. Program kesadaran keamanan informasi diperbarui secara berkala setiap setahun sekali untuk menyesuaikan terhadap teknologi baru, standar, dan persyaratan bisnis serta mengatasi adanya ancaman.
3. Semua karyawan mengetahui dan menerapkan kebijakan keamanan informasi.
4. Setiap karyawan baru di Organisasi mendapatkan pengarahan mengenai keamanan informasi.
5. Pelatihan keamanan informasi secara terjadwal untuk semua karyawan setidaknya setiap tahun.
6. Melatih staff secara khusus tentang kewajiban menjaga data privasi, termasuk hukuman terkait dengan pengungkapan data yang salah.
7. Selalu melakukan manajemen kerentanan siber dan mitigasi terhadap kerentanan.
8. Memberitahukan kepada OPD tentang teknik atau kerentanan siber yang berkembang saat ini yang dapat digunakan dalam peningkatan risiko fraud/penipuan.
9. Melakukan reviu security risk assessment secara berkala minimal 1 tahun sekali
10. Pelaksanaan internal audit telah dilakukan setiap setahun sekali.
11. Diagram yang menggambarkan Aliran data di seluruh sistem jaringan telah didokumentasikan dan dilakukan pembaruan setiap ada perubahan.
12. Standar konfigurasi (port, protokol, service) telah diterapkan dan dikonfigurasikan.

13. Sistem manajemen keamanan informasi telah dipastikan dapat mencapai hasil yang diharapkan.
14. Semua tanggungjawab keamanan informasi telah ditentukan dan dialokasikan secara menyeluruh.
15. Organisasi telah mewajibkan semua karyawan dan kontraktor untuk menerapkan keamanan informasi sesuai dengan kebijakan yang ditetapkan dan prosedur organisasi.
16. Program untuk vulnerability assessment atau penetrating testing pada aplikasi web, aplikasi client-based, aplikasi mobile, wireless, server dan perangkat, jaringan telah dilaksanakan secara berkala.
17. Dilakukan pemisahan environment antara sistem production dan developmentdan tidak mengizinkan akses kepada pengembang tanpa pengawasan dari bagian keamanan organisasi
18. Aplikasi web organisasi telah dilindungi menggunakan firewall aplikasi web (WAFs).
19. Alamat IP internal di organisasi telah dilindungi oleh NAT (Network Addresss Translation)
20. Penggunaan IDS/IPS telah diterapkan jaringan internal dan jaringan perimeter, serta diperbarui secara regular dengan threat intelligence.
21. Software anti virus dan anti malware telah diimplementasikan secara terpusat dan selalu update terhadap perangkat endpoint.
22. DLP (Data Loss Prevention) maupun NAC (Network Access Control) telah diimplementasikan di organisasi.
23. Melaksanakan risk assessment terhadap keamanan informasi secara berkala minimal 1 tahun sekali
24. Risk register terkait keamanan informasi yang diperoleh berdasarkan probabilitas dan dampak yang disesuaikan dengan kriteria organisasi.
25. Kebijakan Domain-based Message Authentication Reporting and Conformance (DMARC) atauprotokol otentikasi email untuk melindungi domain dari penggunaan yang tidak sah telah diterapkan di organisasi.

26. Dilakukan filterisasi terhadap seluruh jenis file lampiran email
27. Peraturan, persyaratan kontrak, dan peraturan lainnya telah diidentifikasi, didokumentasi dan diperbarui untuk setiap sitem informasi.
28. Kontrol kriptografi telah diterapkan sesuai dengan peraturan yang berlaku.
29. Prosedur untuk memastikan kepatuhan terhadap peraturan perundang-undangan dan persyaratan kontrak yang berhubungan dengan hak kekayaan intelektual serta penggunaan produk perangkat lunak proprietary telah diterapkan.
30. Dokumentasi yang dimiliki organisasi dilindungi dan dijaga agar tidak hilang, hancur, dipalsukan, diakses oleh pihak yang tidak sah sesuai dengan persyaratan dan peraturan.
31. Kebijakan Perlindungan Data stakeholder / klien / konsumen / pelanggan secara spesifik atau dokumen khusus yang termasuk dalam Kebijakan Keamanan Informasi yaitu referensi untuk pedoman pemrosesan dan persyaratan data pribadi.
32. Privasi dan perlindungan informasi pribadi telah dipastikan sesuai dengan persyaratan dalam undang-undang dan peraturan terkait lainnya yang berlaku
33. Menyampaikan kebijakan data privasi kepada OPD segera setelah terjalin kerjasama
34. Berkomunikasi dengan OPD setidaknya setiap tahun terkait kebijakan data pribadi mereka yang digunakan
35. Dalam pengembangan software, organisasi telah melakukan verifikasi bahwa versi semua software yang diperoleh dari luar organisasi masih didukung oleh pengembang atau dipertegas berdasarkan rekomendasi keamanan pengembang.
36. Memiliki kebijakan yang menetapkan sanksi yang dijatuhkan terhadap karyawan yang tidak patuh pada kebijakan yang berkaitan dengan keamanan siber
37. Kebijakan keamanan informasi mengatur mengenai single ID yang unik untuk melakukan semua otentikasi

38. Kebijakan terminasi diterapkan dengan masa tenggang yang diizinkan terkait hak akses karyawan ke dalam sistem informasi berupa hak akses segera dinonaktifkan
39. Memiliki dokumen BCP dan DRP
40. Kebijakan dan prosedur keamanan informasi telah dikembangkan sesuai dengan kerangka kerja dan standar yang diakui yaitu menggunakan ISO 270001.
41. Menerapkan praktik secure coding yang sesuai dengan bahasa pemrograman dan development environment yang digunakan
42. Source code yang dibuat secara mandiri dilakukan reviu kerentanannya terlebih dahulu oleh pihak ketiga menggunakan teknis otomatis dan manual sebelum masuk ke production
43. Menghimpun dan menjaga informasi dari pihak ketiga yang akan digunakan untuk melaporkan insiden keamanan, seperti penegakan hukum, departemen pemerintah terkait, vendor, dan mitra ISAC
44. Melakukan penetrating testing menggunakan pihak eksternal dan internal secara berkala
45. Prosedur Otorisasi/persetujuan untuk menambah / mengubah / menghapus hak akses ketika terjadi perpindahan karyawan.

b. Aspek Identifikasi

1. Melakukan perencanaan kapasitas secara berkelanjutan untuk memastikan bahwa semua aset perangkat dan aplikasi sesuai dengan kebutuhan
2. Seluruh aset yang diidentifikasi telah disusun berdasarkan klasifikasi kritikalitas (berdasarkan analisis risiko operasional, analisis bisnis, dan analisis strategis organisasi) serta telah ditetapkan penanggung jawab untuk setiap aset tersebut
3. Melakukan klasifikasi informasi (rahasia, terbatas, umum) dan melakukan inventarisasi
4. Kebijakan pembatasan penggunaan aset organisasi untuk kepentingan pribadi
5. Karyawan tidak diiizinkan memiliki akses sebagai administrator pada perangkat (laptop, personal computer, dll) milik organisasi

6. Melakukan vulnerability scanning dan/atau penetration testing terhadap semua aset perangkat dan aplikasi secara berkala.
7. Risk register telah terdokumentasi untuk semua aplikasi yang memproses data stakeholder.
8. Aspek keamanan mempertimbangkan kapasitas server dan perangkat jaringan secara menyeluruh.
9. Melakukan segmentasi jaringan berdasarkan fungsionalitas (segmen bagian development, keuangan, SDM, dll) dengan kontrol keamanan antar segmen

c. Aspek Proteksi

1. Memiliki IPS yang terkonfigurasi dan diupdate
2. Koneksi ke perangkat server dan jaringan di organisasi Anda menggunakan protokol terenkripsi seperti SSH, secure RDP, dll
3. Penggunaan firelwall telah di konfigurasi dengan baik seperti implicit atau explicit deny any/any rule, inbound network traffic dan outbound network traffic;
4. Menerapkan port access control pada perangkat yang terhubung;
5. Menerapkan firewall filtering antar segmen;
6. Menonaktifkan komunikasi antar worskstation untuk mencegah potensi terjadinya serangan siber (compromise neighboring systems) dalam satu jaringan yang sama
7. Membatasi aplikasi yang diunduh, diinstal, dan dioperasikan
8. Semua Aplikasi dilakukan pemisahan sebagian besar server fisik maupun virtual;
9. Email system di organisasi (termasuk yang ada di cloud) memiliki pengecekan otomatis terhadap spam / phishing / malware
10. Penggunaan cloud resources dan services form berupa SLA dari penyedia cloud dijadikan dasar untuk menentukan RTO dan RPO di dalam dokumen Business Continuity Plan (BCP) organisasi
11. Penerapan whitelist aplikasi di organisasi Anda juga memastikan bahwa hanya authorized software library (seperti: *.dll, *.so, *.ocx, *.exe, dsb) dan signed script (seperti: *.py, *.ps1, *.js, *.jar, dsb) yang dapat dijalankan oleh sistem

12. Memastikan web browser, email client yang digunakan pada perangkat milik organisasi masih mendapatkan update support
13. Memastikan penggunaan add-on dan plugin aplikasi sudah sesuai dengan ketentuan organisasi dan terdokumentasi
14. Menggunakan Next Generation Endpoint Protection
15. Semua perangkat endpoints termasuk server menggunakan anti virus
16. Tidak mengijinkan fitur auto-run content terhadap perangkat portable yang terhubung ke sistem atau perangkat di organisasi
17. 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, dan sebagainya
18. Identity and access management systems digunakan untuk seluruh operating system
19. Informasi identitas dan akses pengguna digunakan untuk membatasi hak akses dari dalam jaringan
20. Memastikan secara otomatis penggantian password secara berkala
21. Menerapkan semua metode otentikasi melalui saluran terenkripsi
22. Akses ke data OPD diatur dengan hak akses
23. Menerapkan IP reputation untuk memverifikasi alamat IP yang diizinkan dalam proses transaksi
24. Dapat melacak dan dapat mendeteksi perilaku anomali transaksi yang dilakukan oleh karyawan maupun stakeholder / klien / konsumen / pelanggan
25. Pengguna selain admin database hanya memiliki akses read-only pada akses ke database
26. Hanya mengizinkan traffic pada layanan cloud untuk kebutuhan bisnis organisasi
27. Akses traffic ke cloud di organisasi Anda hanya dibatasi dari alamat IP yang dikenal
28. SSO di organisasi dapat diakses melalui SSL VPN Tunel
29. Semua data OPD dienkripsi saat dikirim

30. Semua critical system clocks telah disinkronkan dengan metode otomatis seperti Network Time Protocol

d. Aspek Deteksi

1. Perubahan konfigurasi pada peralatan jaringan terdeteksi secara otomatis
2. Mengaktifkan Enable Detailed Logging yang mencakup informasi terperinci seperti event source, tanggal, user, timestamp, source addresses, destination addresses, dan komponen lainnya
3. Menjamin alokasi kapasitas penyimpanan log sesuai dengan kebutuhan
4. Setiap orang yang tergabung dalam tim monitoring pada organisasi mendapatkan peningkatan keterampilan
5. Aktivitas pihak ketiga di organisasi dipantau untuk mendeteksi adanya potensi kejadian keamanan siber
6. Memantau akses fisik terhadap perangkat yang berada di dalam ruangan data center untuk mendeteksi potensi kejadian keamanan siber
7. Dapat mendeteksi kegagalan login pada akun admin pada perangkat jaringan, server, dan aplikasi
8. Memiliki perangkat anti-malware yang secara otomatis melakukan scanning terhadap removable media yang terhubung ke perangkat
9. Log hasil deteksi malware terhubung dengan perangkat anti-malware administrations dan event log servers sehingga dapat digunakan untuk analisis
10. Memiliki ticketing system yang digunakan untuk melacak progres dari events post-notification
11. Ticketing system melacak kejadian berdasarkan tingkat keparahan / prioritas / dampak, kategori keamanan, dan jenis log yang berkorelasi untuk suatu kejadian
12. Memiliki contact tree untuk mengeskalasi dalam merespon suatu kejadian

e. Aspek Respon

1. Memiliki kebijakan penanganan insiden dan selaras dengan kebijakan pengaturan kesinambungan organisasi atau business continuity planning (BCP)

2. Terdapat standar operasional prosedur (SOP) dan form pelaporan penanganan insiden yang diketahui oleh pihak terkait
3. Dokumen rencana respon insiden atau disaster recovery plan (DRP) dan standar operasional prosedur (SOP) penanganan insiden di reviu secara berkala setahun sekali dan/atau setiap ada perubahan
4. Melakukan backup data yang ada di pc/laptop karyawan ke cloud organisasi
5. Tim respon insiden siber di organisasi Anda 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)
6. Memiliki metode yang terdokumentasi dan diinformasikan kepada OPD untuk melaporkan penyalahgunaan informasi OPD
7. Jika organisasi mengalami insiden siber, tim respon insiden dapat dengan cepat mendapat bantuan dari tim manajemen krisis (contoh: spesialis keamanan teknis, tim bisnis, spesialis hukum, tim SDM, dan tim komunikasi eksternal) dan dapat dengan cepat mengakses informasi (dari penyedia pihak ketiga, dan informasi pendukung yang penting lainnya)
8. Tim respon insiden di organisasi mencatat setiap langkah yang dilakukan dalam rangka penanggulangan insiden menggunakan format yang baku (telah ditetapkan oleh organisasi)
9. Hasil reviu terhadap rekap laporan insiden siber dilaporkan ke top management dan didistribusikan kepada para pemangku kepentingan serta digunakan dalam rangka mereviu kontrol yang ada untuk perbaikan respon penanganan insiden siber selanjutnya
10. 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
11. Laporan insiden di organisasi dilaporkan ke top management dan ke pihak eksternal yang berkepentingan/ wajib dilaporkan sesuai regulasi

V. Kelemahan/Kekurangan

Berdasarkan hasil validasi penilaian kematangan keamanan siber (*Cyber Security Maturity*), dapat disimpukan kondisi kelemahan/kekurangan keamanan siber pada Dinas Kominfo,Informatika & Statistik Provinsi Gorontalo sebagai berikut:

a. Aspek Tata Kelola

1. Belum memberikan pelatihan untuk pegawai tentang pentingnya penggunaan secure authentication
2. Belum memberikan pelatihan untuk karyawan tentang cara mengidentifikasi berbagai bentuk serangan social engineering, seperti phishing, scam phone, dan impersonation call.
3. Belum memberikan pelatihan untuk karyawan tentang cara mengidentifikasi dan menyimpan, mengirim, mengarsipkan, dan memusnahkan informasi sensitif dengan benar
4. Belum memberikan pelatihan untuk karyawan terkait kesadaran tentang penyebab kebocoran data secara tidak sengaja, seperti kehilangan perangkat seluler karyawan atau ketidaksengajaan mengirim email ke orang yang salah
5. Belum melakukan simulasi phising setidaknya setiap tahun
6. Belum memiliki kebijakan yang mengharuskan penerapan perlindungan data pribadi dan dilakukan proses reviu secara berkala
7. Organisasi masih menggunakan satu akun untuk melakukan vulnerability scanning dan belum ada akun khusus
8. Setiap akun pengguna atau sistem yang digunakan dalam melakukan penetrating testing belum 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
9. Belum melakukan reviu security risk treatment

10. Belum melakukan reviui izin akses dari akun pengguna setidaknya setiap tiga bulan.
11. Belum diilakukan pengujian terhadap keberadaan informasi yang dapat berguna bagi penyerang seperti network diagram, file konfigurasi, laporan uji penetrasi, email atau dokumen yang berisi kata sandi atau informasi lain yang penting untuk sistem operasi
12. Belum membentuk Red Team dan Blue Team serta belum melakukan pengujian secara berkala dalam mengukur kesiapan organisasi untuk mengidentifikasi dan menghentikan serangan atau merespon dengan cepat dan efektif dari insiden keamanan yang terjadi.
13. Belum melakukan pencegahan, atau pengurangan terhadap dampak/efek yang tidak diinginkan dari risk maupun opportunities yang dimiliki organisasi
14. Belum ada kebijakan atau prosedur mengenai pemberitahuan jika terjadi pelanggaran terhadap data pribadi dan apakah didokumentasikan
15. Belum ada orang yang ditunjuk secara khusus bertanggungjawab untuk pengembangan dan implementasi kebijakan dan prosedur perlindungan data pribadi
16. Belum ada kegiatan penelusuran yang memastikan bahwa data OPD yang disimpan adalah data yang akurat
17. Belum melakukan risk analisis untuk keamanan TI terkait keamanan fisik dan sistem elektronik
18. Kebijakan keamanan informasi dan hasil evaluasi pelaksanaan kebijakan keamanan informasi belum dijadikan acuan oleh pimpinan dalam menentukan strategi organisasi
19. Belum memiliki kebijakan metode penghapusan data

b. Aspek Identifikasi

1. Belum ada dokumentasi mengenai alur informasi yang memproses data OPD termasuk yang dikelola oleh pihak ketiga

2. Data sensitif termasuk data OPD yang disimpan (secara elektronik dan hardcopy) belum memuat metadata informasi periode retensi, pemilik data, dan penggunaan data tersebut
3. Belum dilakukan pemeringkatan pada kerentanan yang teridentifikasi berdasarkan pedoman / standar / acuan organisasi
4. Belum memperbaharui roadmap keamanan TI organisasi dalam jangka waktu tertentu
5. Belum memiliki Business Impact Analysis terhadap perangkat dan aplikasi TI dan direviu secara berkala.
6. Belum melakukan prioritasi upaya remediasi dengan memanfaatkan level risiko dari hasil penilaian risiko
7. Belum melakukan prioritasi terkait langkah proteksi keamanan siber termasuk strategi untuk memprioritaskan perlindungan data dan aset kritis
8. Belum ada profil keamanan informasi mencakup prioritas kerentanan dan rencana mitigasinya
9. Belum melakukan klasifikasi terhadap cyber threats yang ditemukan pada organisasi

c. Aspek Proteksi

1. Belum melakukan disable peer-to-peer pada wireless client di perangkat endpoint
2. Belum dilakukan pembatasan penggunaan scripting tools (seperti: Microsoft PowerShell dan Python) di organisasi
3. Belum menerapkan pengaturan akses (read/write) terhadap perangkat USB/media penyimpanan eksternal
4. Belum penerapan Multi-Factor Authentication (MFA) yang digunakan untuk mengakses data sensitif (misal data pribadi, data keuangan, dll)
5. Belum memastikan penggunaan password yang kompleks untuk semua akses login

6. Belum menambahkan verifikasi On Time Password (OTP) melalui SMS, WhatsApp Messenger, Telepon, Elektronil Mail, Google Authenticator, atau media lainnya untuk transaksi yang berisiko tinggi
7. Pada cloud belum menerapkan Single Sign-On
8. Belum semua data OPD dienkripsi saat disimpan
9. Penyimpanan data backup belum dilindungi secara tepat, baik secara fisik maupun non fisik (seperti: enkripsi, dsb)

d. Aspek Deteksi

1. Semua perubahan konfigurasi belum melalui proses Change Management System dan tidak dilakukan reviu secara berkelanjutan
2. Belum terdapat mekanisme monitoring terhadap akses dan perubahan pada data sensitif? (seperti File Integrity Monitoring atau Event Monitoring)
3. Belum memiliki mekanisme monitoring dan deteksi terhadap penggunaan enkripsi yang tidak sah
4. Belum melakukan monitoring terhadap log dari perangkat security control, jaringan, dan aplikasi
5. Belum memiliki sistem untuk memonitoring dan mencegah kehilangan data sensitif termasuk data OPD contohnya penggunaan DLP (Data Loss Prevention)
6. Belum menerapkan SIEM atau Log Analytic Tools untuk keperluan dokumentasi, korelasi, dan analisis log
7. Escalation profile belum dibuat untuk setiap security event yang ditemukan, dan tidak disimpan sebagai panduan untuk digunakan di masa mendatang
8. Belum memiliki SOC atau manajemen teknis yang dapat dihubungi setiap saat (24x7) untuk menangani kejadian dengan prioritas tinggi dan kritikal
9. Belum memperoleh informasi dari multiple threat intelligence feeds untuk mendeteksi serangan siber
10. Threat intelligence feeds belum dikonfigurasi secara otomatis untuk memperbarui kontrol pencegahan, seperti pembaruan signature IPS, update rules, dan konfigurasi lainnya

11. Belum menjalankan vulnerability scanning tools secara otomatis untuk mendeteksi kerentanan siber
12. Belum melakukan vulnerability scanning secara otomatis menggunakan agent/aplikasi yang diinstal pada endpoint
13. Belum memiliki sistem yang untuk mendeteksi ancaman siber sehingga dapat memberikan input/feed bagi threat intelligence seperti penggunaan deception technology
14. Belum memiliki sistem untuk melakukan Malicious Code Detection untuk mendeteksi, menghapus, dan melindungi dari malicious code
15. Belum memiliki unit yang melakukan Cyber Threat Intelligence (CTI)
16. Metrik security event belum reviu untuk tujuan operasional

e. Aspek Respon

1. Belum membuat skema penilaian insiden dan prioritas berdasarkan potensial dampak (aspek kerugian operasional, bisnis, reputasi, dan hukum) bagi organisasi
2. Belum memberikan pelatihan untuk karyawan tentang cara mengidentifikasi, penanganan, dan pelaporan suatu insiden keamanan informasi
3. Belum mendesain jaringan yang dapat memastikan apabila server DMZ terkena serangan siber, penyerang tidak dapat mengakses server yang lain
4. Belum memiliki sumber daya redundan yang dapat langsung digunakan pada sistem penting/kritikal yang down karena insiden siber
5. Setelah ditemukan kerentanan yang menyebabkan pelanggaran dan telah dilakukan patching, belum dilakukan scanning ulang untuk memastikan bahwa kerentanan tersebut sudah ditutup
6. Belum melakukan reviu terhadap root cause dari suatu insiden siber untuk mencegah kejadian serupa berulang
7. Belum melakukan reviu terhadap rekap laporan insiden siber yang pernah terjadi untuk melihat apakah prosedur insiden respon sudah sesuai dengan standar yang ditetapka

8. Belum ada SLA dalam penanganan insiden;
9. Belum memiliki metrik perhitungan biaya untuk mencegah insiden siber yang menggunakan metode perhitungan ROI (Return of Invesment) pada program keamanan siber di organisasi? Dan apakah di reviu secara berkala
10. Belum menggunakan sumber referensi terpercaya untuk memperhitungkan biaya pengeluaran akibat insiden siber, yang selanjutnya digunakan untuk membuat ROI (Return of Invesment) dalam menentukan skala prioritas tindakan mitigasi risiko dan meminimalisir kerugian biaya akibat terjadinya insiden siber
11. Belum mempublikasikan informasi untuk semua karyawan dan OPD mengenai mekanisme pelaporan anomali dan insiden siber kepada tim penanganan insiden siber organisasi dan informasi tersebut belum dimasukkan dalam kegiatan kesadaran keamanan informasi secara rutin

VI. Rekomendasi

Berdasarkan hasil validasi penilaian kematangan keamanan siber (*Cyber Security Maturity*), berikut ini rekomendasi yang dapat dilakukan dalam rangka peningkatan kematangan siber pada Dinas Kominfo,Informatika & Statistik Provinsi Gorontalo sebagai berikut:

1. Secara umum diperlukan peningkatan terhadap faktor-faktor yang menjadi kelemahan/kekurangan pada aspek tata kelola, aspek identifikasi, aspek proteksi, aspek deteksi, dan aspek respon.
2. Melaksanaan peningkatan kapasitas SDM terutama terkait dengan pengujian keamanan, mekanisme proteksi dan penanganan insiden.
3. Menyusun Pedoman dan Kebijakan Penerapan Keamanan Informasi mengacu pada Standar ISO 27001 khususnya terkait dengan Penerapan kriptografi, Mekanisme Penghapusan Data, dan Pengendalian terhadap Aset Informasi.
4. Menyusun Risk Register berdasarkan kriteria ISO 31000 terkait dengan manajemen risiko yang diantaranya memetakan terkait Aset, Kerentanan, Ancaman, Kemungkinan, Dampak, Level Risiko, Proses Mitigasi, dan Penanggungjawab.

5. Menyusun Dokumen Business Impact Analiis untuk melihat proses bisnis dan aset kritikal berdasarkan aspek Kerahasiaan, keutuhan, ketersediaan, otentikasi dan Anti penyangkalan sehingga dapat dirumuskan prioritas penanganan risiko.
6. Meminta Layanan Sensor Honeypot pada Direktorat Deteksi Ancaman, Deputi Bidang Identifikasi dan Deteksi BSSN dalam rangka proses monitoring dan deteksi dini anomaly ancaman dan serangan siber yang dapat terjadi di sistem/aplikasi yang digunakan.

PENUTUP

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

Gorontalo, 25 November 2020

Kabid Penyelengaraan E-Government

Ditandatangani secara elektronik oleh :
KEPALA BIDANG PENYELENGGARAAN E-GOVERNMENT

FRIED DEWI H. AHMAD, S.Kom, M.Eng
197406212002122004

(Fried Dewi H. Ahmad, S.Kom., M.Eng.)

Tim BSSN

(I Made Mustika Kerta Astawa)

(Nur Dwi Muryanto)

(Indra Dimas Nurdiyanto)

(Haryo Laksono)

(Moch Yusuf)