2021

LAPORAN

HASIL PENILAIAN

CYBER SECURITY MATURITY (CSM)

DINAS KOMUNIKASI INFORMATIKA DAN STATISTIK PROVINSI RIAU

PENDAHULUAN

I. Umum

Tingkat kesiapan keamanan siber di setiap organisasi berbeda-beda, sehingga masing-masing organisasi juga membutuhkan strategi yang berbeda-beda pula dalam menghadapi ancaman, serangan, maupun ancaman siber. Dalam implementasi keamanan siber, beberapa organisasi baru fokus terhadap perbaikan penerapan kontrol keamanan yang lebih proaktif, penyusunan peraturan dan kebijakan keamanan siber, dan penyusunan strategi keamanan berdasarkan hasil deteksi insiden. Selain itu, sebagian organisasi telah mendorong investasi teknologi sebagai kebutuhan keamanan serta telah memberikan dukungan personel di bidang keamanan siber yang kompeten, serta mempertimbangkan risiko siber serta mendorong budaya keamanan siber secara menyeluruh untuk keberlangsungan organisasinya.

Setiap organisasi harus memahami kelemahan dari proses keamanan siber yang dimiliki. Sehingga dapat menentukan target tingkat keamanan siber yang akan dicapai dan memastikan bahwa organisasi tersebut telah siap dalam menghadapi ancaman siber dalam bentuk apapun. Oleh karena itu diperlukan suatu metode pengukuran kematangan keamanan siber agar organisasi dapat melakukan peningkatan dalam pengelolaan proses keamanan siber dan memastikan bahwa telah dioptimalkan sepenuhnya dan berfungsi secara menyeluruh. Untuk itu, Badan Siber dan Sandi Negara (BSSN) telah membentuk suatu *framework* untuk mengukur *cyber security maturity* yang dapat digunakan sebagai metode untuk mengukur tingkat kematangan keamanan siber suatu organisasi.

Tools Cyber Security Maturity merupakan alat bantu yang digunakan untuk mengukur kematangan keamanan siber di organisasi. Sektor pemerintahan sebagai salah satu domain yang memanfaatkan ruang siber diharapkan turut melakukan

peningkatan pengelolaan keamanan siber serta memastikan pengelolaan tersebut berjalan dengan optimal dan berfungsi secara menyeluruh.

II. Tujuan Kegiatan

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

III. Ruang Lingkup Kegiatan

Kegiatan yang dilaksanakan meliputi pemetaan aspek penanganan insiden meliputi:

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

IV. Metodologi Kegiatan

Metodologi yang digunakan berdasarkan hasil pengisian instrumen *Cyber Security Maturity* (CSM), wawancara/diskusi, dan melihat ketersediaan dokumen keamanan siber. Hasil diberikan dalam bentuk Indeks Kematangan, Level Kematangan dan bagan berbentuk radar yang menjelaskan maturitas setiap aspek keamanan siber.

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

$$Level\ Kematangan\ (\%) = \frac{Indeks\ Kematangan}{5}\ x\ 100\%$$

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

Pengisian Instrumen CSM dilakukan oleh internal *stakeholder* (*self assessment*) pada 2 s.d. 3 November 2021 dengan dipandu dan divalidasi oleh Tim BSSN.

HASIL KEGIATAN

I. Informasi *Stakeholder*

Nama Instansi/Lembaga : Dinas Komunikasi Informatika dan Statistik Provinsi Riau

Alamat : Jalan Diponegoro Nomor 24 A

Nomor Telp./Fax. : (0761) 45505

Email : diskominfotik@riau.go.id

Narasumber Instansi/Lembaga :

1. Dodi Sutejo, S.Sos., M.Si. (Kasie Tata Kelola Persandian)
2. T. Nova Sukma, ST (Kasie Operasional Pengamanan Persandian)
3. Tiara Mulia Putri, S.Kom. (Calon Pranata Komputer Pertama
4. Yogi Ferdyan, A.Md. (Staf Sie Pengawasan dan Evaluasi Persandian)
5. Debie Naheldha (Fungsional Sandiman Pelaksana)
6. Nadita Candra (THL Persandian)

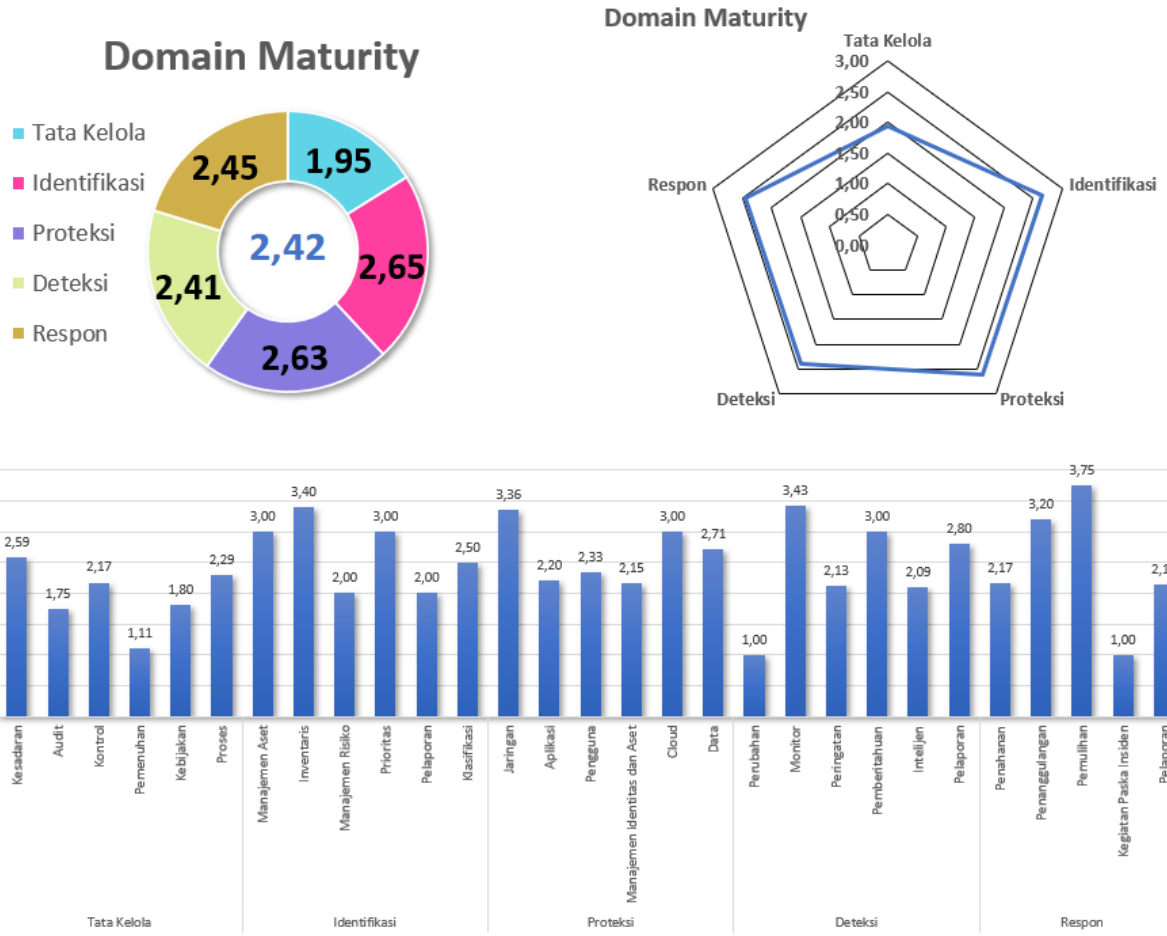
II. Deskripsi Ruang Lingkup Penilaian

1. Ruang Lingkup Penilaian :

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

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

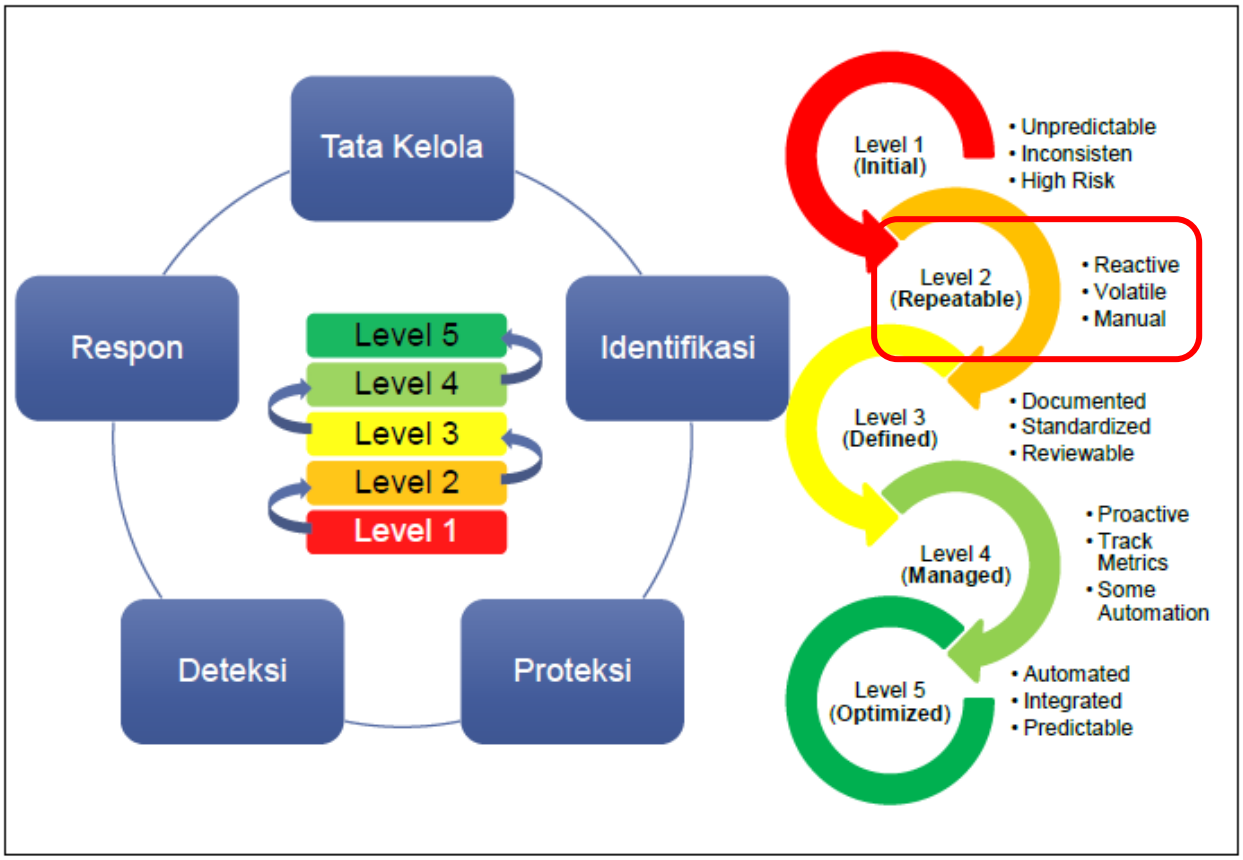
III. Hasil Penilaian CSM



Gambar 1. Hasil Penilaian CSM

Berdasarkan hasil penilaian instrumen CSM, diperoleh hasil sebagai berikut **Total Score Indeks Kematangan : 2,42,** sehingga perhitungan penentuan Level Kematangan didapatkan level kematangan sebagai berikut:

Level Kematangan Tingkat 2



Gambar 2. Capaian Level Kematangan

Level Kematangan 2:

Level kematangan 2 menunjukkan bahwa pengelolaan keamanan siber di Dinas komunikasi Informatika dan Statistik Provinsi Riau sudah terorganisasi, bersifat informal, dilakukan secara berulang namun belum konsisten, serta belum dilakukan secara berkelanjutan.

IV. Kekuatan/Kematangan

Tata Kelola

1. Organisasi telah memberikan pelatihan pegawai tentang cara mengidentifikasi dan menyimpan, mengirim, mengarsipkan, dan memusnahkan informasi sensitif dengan benar.
2. Organisasi telah memastikan sistem manajemen keamanan informasi dapat mencapai hasil yang diharapkan.
3. Organisasi telah menetapkan program untuk vulnerability assessment atau penetration testing secara berkala kepada aplikasi web, aplikasi client-based, aplikasi mobile, wireless, server dan perangkat jaringan.
4. Organisasi sedang membangun kebijakan keamanan informasi yang mengatur mengenai single ID yang unik untuk melakukan semua otentikasi.
5. Organisasi telah menetapkan proses untuk menerima dan menangani laporan kerentanan software berupa SOP Helpdesk.
6. Organisasi telah menerapkan praktik secure coding yang sesuai dengan bahasa pemrograman dan development environment yang digunakan.
7. Organisasi telah melakukan konfigurasi firewall yang terdokumentasi dengan baik dan mereviu terhadap konfigurasi router dan switch.

Identifikasi

1. Organisasi melakukan perencanaan kapasitas secara berkala untuk memastikan bahwa pengadaan semua aset perangkat dan aplikasi dilakukan sesuai dengan kebutuhan melalui perencanaan pengadaan setiap tahun.
2. Organisasi telah melakukan identifikasi dan inventarisasi data pada perangkat keras dan perangkat lunak secara berkala.
3. Terdapat data otentikasi yang disimpan di perangkat browser end user.
4. Organisasi mempertimbangkan aspek keamanan dalam pengambilan keputusan TI.

5. Organisasi telah melakukan prioritas terkait langkah proteksi keamanan siber termasuk strategi untuk memprioritaskan perlindungan data dan aset kritis.
6. Organisasi sudah menerapkan segmentasi jaringan dengan ditambahkan kontrol keamanan antar segmennya.

Proteksi

1. Organisasi telah melakukan proteksi terhadap jaringan dengan memberikan *firewall*, melakukan filtering pada *inbound* dan *outbound network traffic*.
2. Organisasi telah menerapkan port access control.
3. Organisasi tidak mengijinkan fitur auto-run content terhadap perangkat portable yang terhubung ke sistem atau perangkat.
4. Media penyimpanan eksternal yang dimiliki organisasi telah dienkripsi dan diatur aksesnya (read/write).
5. Organisasi telah mengatur hak akses untuk akses ke data stakeholder.
6. Organisasi dapat melacak dan mendeteksi perilaku anomali transaksi karyawan maupun stakeholder.
7. Organisasi telah menggunakan authorized cloud storage.
8. Organisasi melakukan *backup* data secara berkala.

Deteksi

1. Organisasi sudah melakukan monitoring terhadap akses pada data sensitif, aktivitas lalu lintas jaringan, dan log dari perangkat security control, jaringan dan aplikasi.
2. Organisasi sudah menerapkan Enable Detailed Logging yang mencakup informasi terperinci.
3. Organisasi telah menerapkan SIEM (Security Information Event Monitoring).
4. Organisasi dapat mendeteksi *Wireless* Access *Point* yang terhubung ke jaringan LAN (ethernet) secara manual.
5. Tim monitoring telah mendapatkan peningkatan keterampilan.
6. Organisasi dapat mendeteksi terhadap anomali pada jaringan.

7. Organisasi melakukan pemantauan terhadap aktivitas pihak ketiga dan akses fisik terhadap perangkat yang berada di dalam ruangan data center untuk mendeteksi potensi kejadian keamanan siber.
8. Organisasi memiliki ticketing system yang digunakan untuk melacak progres dari events post-notification.
9. Organisasi telah menyimpan semua log terhadap URL yang diakses oleh karyawan.
10. Organisasi memiliki daftar kontak (contact tree) pihak terkait untuk eskalasi suatu event berupa SK CSIRT dan SOP pelaporan insiden.
11. Organisasi telah menjalankan vulnerability scanning tools secara otomatis untuk mendeteksi kerentanan siber.

Respon

1. Organisasi telah memiliki form pelaporan penanganan insiden yang diketahui oleh pihak terkait.
2. Organisasi mendesain jaringan yang dapat memastikan apabila server DMZ terkena serangan siber, penyerang tidak dapat mengakses server yang lain.
3. Tim respon insiden siber di organisasi telah memiliki peralatan sumber daya analisis insiden.
4. Organisasi telah merancang standar terkait waktu yang diperlukan bagi administrator sistem dan karyawan lainnya.

V. Kelemahan/Kekurangan

Tata Kelola

1. Organisasi belum memiliki program pemahaman kesadaran keamanan informasi yang dilakukan secara berkelanjutan.
2. Organisasi belum memberikan pengarahan mengenai keamanan informasi kepada karyawan baru.

3. Organisasi belum memberikan pelatihan pegawai tentang penggunaan secure authentication.
4. Organisasi belum melatih staf secara khusus tentang kewajiban data privasi.
5. Organisasi belum melakukan simulasi *phishing* secara berkala ke karyawan.
6. Personil yang terlibat dalam pengembangan software/aplikasi belum mendapatkan pelatihan mengenai *secure code*.
7. Organisasi belum memiliki kebijakan mengharuskan penerapan perlindungan data pribadi yang direviu secara berkala.
8. Organisasi tidak menggunakan akun khusus selain akun admin untuk melakukan vulnerability scanning.
9. Organisasi belum menerapkan manajemen risiko.
10. Organisasi belum melakukan reviu izin akses dari akun pengguna setidaknya setiap 3 bulan sekali.
11. Organisasi belum memiliki dokumentasi/diagram aliran data di seluruh sistem dan jaringan.
12. Organisasi belum membuat persyaratan keamanan informasi terkait akses supplier terhadap aset organisasi dan mendokumentasikannya.
13. Web organisasi belum dilindungi firewall aplikasi web (WAFs).
14. Organisasi belum menerapkan software antivirus dan antimalware yang terpusat.
15. Organisasi belum menerapkan continual improvement terhadap keamanan informasi.
16. Organisasi belum mengimplementasikan kebijakan Domain-based Message Authentication Reporting and Conformance (DMARC) atau protokol otentikasi email.
17. Organisasi belum melakukan filterisasi terhadap seluruh jenis file lampiran email.
18. Organisasi belum menerapkan metode sandbox terhadap seluruh lampiran email.
19. Organisasi belum melakukan pengukuran kepatuhan pengguna terhadap Kebijakan Keamanan Informasi.

20. Organisasi belum menerapkan kontrol kriptografi sesuai dengan semua perjanjian, undang-undang, dan peraturan yang berlaku.
21. Organisasi belum memiliki Kebijakan Perlindungan Data stakeholder secara spesifik atau dokumen khusus yang termasuk dalam Kebijakan Keamanan Informasi.
22. Organisasi belum menyusun BCP dan DRP.
23. Organisasi belum memiliki kebijakan keamanan informasi yang telah disetujui manajemen serta dikomunikasikan kepada karyawan dan pihak eksternal terkait.
24. Organisasi belum memiliki kebijakan metode penghapusan data.
25. Organisasi belum memiliki kebijakan dan prosedur keamanan informasi yang dikembangkan sesuai dengan kerangka kerja dan standar yang diakui.
26. Organisasi belum melakukan *threat hunting* secara berkala.

Identifikasi

1. Organisasi belum memiliki *system configuration management tools* untuk otomatisasi konfigurasi perangkat keras dan perangkat lunak.
2. Organisasi tidak memiliki kebijakan pembatasan penggunaan aset organisasi untuk kepentingan pribadi.
3. Organisasi mengizinkan karyawan memiliki akses sebagai administrator pada perangkat milik organisasi serta mengizinkan pihak ketiga menggunakan aset mereka pada jaringan organisasi.
4. Organisasi belum memiliki kebijakan dan implementasi mengenai retensi data sensitif.
5. Dokumen risk register untuk semua aplikasi yang memproses data stakeholder belum ada.
6. Organisasi belum memiliki *Business Impact Analysis* terhadap perangkat dan aplikasi TI.
7. Organisasi belum memiliki metode/standar untuk klasifikasi aset TI yang direviu secara berkala.

8. Organisasi belum melakukan klasifikasi terhadap cyber threats yang ditemukan.

Proteksi

1. Organisasi belum mengkonfigurasikan akses nirkabel menggunakan sistem enkripsi.
2. Semua perangkat jaringan belum menggunakan otentikasi terpusat.
3. Organisasi tidak melakukan penonaktifan komunikasi antar workstation dalam satu jaringan yang sama.
4. Organisasi belum menerapkan DNS filtering services.
5. Organisasi belum menerapkan pembatasan terhadap aplikasi yang diunduh, diinstal dan dioperasikan.
6. Organisasi belum menerapkan whitelist aplikasi.
7. Belum ada kebijakan terkait pembatasan penggunaan *scripting tools*.
8. Organisasi belum menerapkan Next Generation Endpoint Protection.
9. Organisasi belum menggunakan antivirus di semua perangkat endpoints termasuk server.
10. Organisasi belum menerapkan URL Filtering, device control, dan application control pada semua perangkat endpoint pengguna.
11. Organisasi belum menerapkan pembatasan akun pada laptop/PC milik organisasi yang digunakan untuk aktivitas tertentu.
12. Organisasi belum menerapkan identity and access management systems untuk seluruh operating system.
13. Penggunaan *Multi Factor Authentication* belum diterapkan.
14. Organisasi belum menerapkan manajemen password yaitu pengaturan kompleksitas password dan penggantian password secara berkala.
15. Belum memanfaatkan metode otentikasi pada saluran yang terenkripsi dan juga penambahan OTP.
16. Organisasi belum menerapkan IP reputation.
17. Organisasi belum menerapkan Single Sign-On pada cloud organisasi.

18. Organisasi belum melakukan enkripsi pada semua data stakeholder saat disimpan.

Deteksi

1. Organisasi belum menerapkan Change Advisory Board (CAB) yang meninjau dan menyetujui semua perubahan konfigurasi.
2. Organisasi belum menerapkan Change Management System untuk melakukan perubahan konfigurasi dan dilakukan reviu secara berkelanjutan.
3. Organisasi belum menerapkan deteksi otomatis perubahan konfigurasi pada peralatan jaringan.
4. Organisasi belum melakukan monitoring terhadap log dari perangkat security control, jaringan, dan aplikasi.
5. Organisasi belum memiliki sistem untuk memonitoring dan mencegah kehilangan data sensitif termasuk data stakeholder.
6. Organisasi belum menjamin alokasi kapasitas penyimpanan log sesuai dengan kebutuhan.
7. Organisasi belum memiliki perangkat antimalware yang secara otomatis melakukan scanning terhadap removable media yang terhubung ke perangkat.
8. Organisasi belum menerapkan automated port scan secara berkala terhadap semua sistem dan memberikan alert.
9. Organisasi belum memiliki ticketing system melacak kejadian berdasarkan tingkat keparahan/prioritas/dampak, kategori keamanan, dan jenis log yang berkorelasi untuk suatu kejadian.
10. Organisasi belum melakukan *escalation profile* untuk setiap *security event* yang ditemukan.
11. Organisasi belum memiliki SOC atau manajemen teknis yang dapat dihubungi setiap saat (24x7).
12. Organisasi belum menerapkan event notification yang berbeda-beda untuk setiap jenis eskalasi.

13. Organisasi belum memperoleh informasi dari multiple threat intelligence feeds untuk mendeteksi serangan siber.
14. Organisasi belum menerapkan threat intelligence feeds yang dikonfigurasi secara otomatis untuk memperbarui kontrol pencegahan.
15. Organisasi masih browsing melalui search engine (seperti website BSSN) untuk memperoleh informasi dan update mengenai isu keamanan siber terkini.
16. Organisasi belum menjalankan *vulnerability scanning tools* secara otomatis menggunakan agent/aplikasi yang diinstal pada endpoint.
17. Organisasi belum menerapkan DNS query logging dalam mendeteksi hostname lookups.
18. Organisasi belum memiliki sistem untuk melakukan Malicious Code Detection.
19. Unit dalam organisasi belum menjalankan fungsi Cyber Threat Intelligence (CTI).
20. Organisasi belum memiliki *Metrik Security Event*.

Respon

1. Organisasi belum melakukan reviu secara berkala terhadap dokumen rencana respon insiden atau disaster recovery plan (DRP) dan standar operasional prosedur (SOP) penanganan insiden.
2. Organisasi membuat skema penilaian insiden dan prioritas berdasarkan potensial dampak.
3. Organisasi belum melakukan latihan respon insiden dan memberikan pelatihan kepada para personil tentang cara penanganan suatu insiden.
4. Organisasi belum memberikan pelatihan untuk karyawan tentang cara mengidentifikasi, penanganan, dan pelaporan suatu insiden keamanan informasi.
5. Organisasi belum mempunyai daftar kontak tim penanganan insiden internal dan eksternal.
6. Organisasi belum menerapkan mekanisme backup data pada pc/laptop karyawan ke cloud organisasi.

7. Organisasi belum memiliki sumber daya redundan yang dapat langsung digunakan saat sistem penting/kritikal mengalami down karena insiden siber.
8. Organisasi belum memiliki metode yang terdokumentasi dan diinformasikan kepada stakeholder untuk melaporkan penyalahgunaan informasi stakeholder.
9. Organisasi belum melakukan reviu terhadap root cause dari suatu insiden siber serta rekap laporan insiden siber yang pernah terjadi.
10. Hasil reviu terhadap rekap laporan insiden siber tidak dilaporkan ke top management dan didistribusikan kepada para pemangku kepentingan serta digunakan dalam rangka mereviu kontrol yang ada untuk perbaikan respon penanganan insiden siber.
11. Organisasi belum memastikan pencapaian SLA dalam penanganan insiden.

VI. Rekomendasi

1. Untuk meningkatkan aspek tata kelola di lingkungan Diskominfotik Pemprov Riau maka dapat dilakukan hal-hal sebagai berikut:
   a. Menyusun program pemahaman kesadaran keamanan informasi yang dilakukan secara berkelanjutan.
   b. Menerapkan manajemen risiko terhadap seluruh aset milik organisasi.
   c. Menyusun BCP dan DRP.
   d. Menyusun kebijakan untuk penerapan perlindungan data pribadi dan direviu secara berkala.
   e. Memberikan pengarahan mengenai keamanan informasi kepada karyawan baru.
   f. Memberikan pelatihan pegawai tentang penggunaan secure authentication dan secure code bagi personil yang terlibat dalam pengembangan software/aplikasi.
   g. Melakukan pengukuran kepatuhan pengguna terhadap Kebijakan Keamanan Informasi.

h. Menyusun Kebijakan Perlindungan Data stakeholder secara spesifik atau dokumen khusus yang termasuk dalam Kebijakan Keamanan Informasi.
i. Menyusun kebijakan keamanan informasi yang telah disetujui manajemen serta dikomunikasikan kepada karyawan dan pihak eksternal terkait dan dikembangkan sesuai dengan kerangka kerja dan standar yang diakui.
j. Menyusun kebijakan metode penghapusan data.
k. Menerapkan kontrol kriptografi sesuai dengan semua perjanjian, undang-undang, dan peraturan yang berlaku.
l. Menyusun dokumentasi/diagram aliran data di seluruh sistem dan jaringan.
m. Menyusun persyaratan keamanan informasi terkait akses supplier terhadap aset organisasi dan mendokumentasikannya.
n. Mengimplementasikan firewall aplikasi web (WAFs) untuk melindungi web organisasi.
o. Menerapkan software antivirus dan antimalware yang terpusat.
p. Menerapkan continual improvement terhadap keamanan informasi.
q. Menerapkan penggunaan akun khusus selain akun admin untuk melakukan *vulnerability scanning*.
r. Mengimplementasikan kebijakan Domain-based Message Authentication Reporting and Conformance (DMARC) atau protokol otentikasi email.
s. Menerapkan filterisasi terhadap seluruh jenis file lampiran email.
t. Menerapkan metode sandbox terhadap seluruh lampiran email.
u. Memprogramkan *threat hunting* secara berkala.

2. Untuk meningkatkan aspek identifikasi, dapat dilakukan hal-hal sebagai berikut:
   a. Menyusun *Business Impact Analysis* terhadap perangkat dan aplikasi TI.
   b. Menyusun dokumen risk register untuk seluruh aset milik organisasi dan semua aplikasi yang memproses data stakeholder.
   c. Melakukan penerapan *system configuration management tools* untuk otomatisasi konfigurasi perangkat keras dan perangkat lunak.

d. Menyusun kebijakan pembatasan penggunaan aset organisasi untuk kepentingan pribadi.
e. Menyusun kebijakan dan implementasi mengenai retensi data sensitif.
f. Menyusun metode/standar untuk klasifikasi aset TI dan direviu secara berkala.

3. Untuk meningkatkan aspek proteksi, dapat dilakukan hal-hal sebagai berikut:
   a. Menerapkan penggunaan *Multi Factor Authentication*.
   b. Menyusun kebijakan terkait pembatasan penggunaan scripting tools.
   c. Menerapkan otentikasi terpusat pada semua perangkat jaringan.
   d. Menerapkan Next Generation Endpoint Protection.
   e. Menerapkan antivirus di semua perangkat endpoints termasuk server.
   f. Menerapkan URL Filtering, device control, dan application control pada semua perangkat endpoint pengguna.
   g. Menerapkan pembatasan akun pada laptop/PC milik organisasi yang digunakan untuk aktivitas tertentu.
   h. Menerapkan identity and access management systems untuk seluruh operating system.
   i. Menerapkan manajemen password yaitu pengaturan kompleksitas password dan penggantian password secara berkala.
   j. Menerapkan metode otentikasi pada saluran yang terenkripsi dan juga penambahan OTP.
   k. Menerapkan DNS filtering services.
   l. Menerapkan whitelist aplikasi.
   m. Menerapkan IP reputation.
   n. Menerapkan Single Sign-On pada cloud organisasi.
   o. Menerapkan enkripsi pada semua data stakeholder saat disimpan.

4. Untuk meningkatkan aspek deteksi, dapat dilakukan hal-hal sebagai berikut:

a. Menerapkan Change Management System untuk melakukan perubahan konfigurasi.
b. Menyusun *escalation profile* untuk setiap *security event* yang ditemukan.
c. Menyusun *Metrik Security Event*.
d. Menerapkan *vulnerability scanning tools* secara otomatis menggunakan agent/aplikasi dan diinstal pada *endpoint*.
e. Menerapkan ticketing system melacak kejadian berdasarkan tingkat keparahan/prioritas/dampak, kategori keamanan, dan jenis log yang berkorelasi untuk suatu kejadian.
f. Memiliki perangkat antimalware yang secara otomatis melakukan scanning terhadap removable media yang terhubung ke perangkat.
g. Menerapkan automated port scan secara berkala terhadap semua sistem dan memberikan alert.
h. Menerapkan DNS query logging dalam mendeteksi hostname lookups.
i. Mengadakan atau menganggarkan pelatihan terkait Cyber Threat Intelligence kepada personil untuk menjalankan fungsi CTI.
j. Menggunakan aplikasi maupun OS dengan lisensi yang original (tidak bajakan) dalam rangka menghindari kerentanan yang timbul pada aplikasi tidak berlisensi.

5. Untuk meningkatkan aspek respon, dapat dilakukan hal-hal sebagai berikut:
   a. Menyusun dokumen rencana respon insiden atau disaster recovery plan (DRP) dan standar operasional prosedur (SOP) penanganan insiden dan menjadwalkan reviu secara berkala.
   b. Melakukan latihan respon insiden dan memberikan pelatihan kepada para personil tentang cara penanganan suatu insiden.
   c. Memberikan pelatihan untuk karyawan tentang cara mengidentifikasi, penanganan, dan pelaporan suatu insiden keamanan informasi.
   d. Menyusun daftar kontak tim penanganan insiden internal dan eksternal.

e. Mengadakan sumber daya redundan yang dapat langsung digunakan saat sistem penting/kritikal mengalami down karena insiden siber.
f. Melakukan reviu terhadap root cause dari suatu insiden siber serta rekap laporan insiden siber yang pernah terjadi.
g. Melaporkan ke top management terkait rekap laporan insiden siber dan mendistribusikannya kepada para pemangku kepentingan.

PENUTUP

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

Pekanbaru, 3 November 2021

Kasie Operasional Pengamanan Persandian	Koordinator Kelompok Manajemen Risiko PTK KSS Pemda
KEPALA SEKSI OPERASIONAL PENGAMANAN PERSANDIAN DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK T. NOVA SUKMA, ST NIP. 19801104 200604 2 008 Balai Sertifikasi Elektronik Dokumen ini telah ditandatangani secara elektronik menggunakan Sertifikat Elektronik yang diterbitkan oleh BSrE	Ditandatangani secara elektronik oleh: Koor Manris PTK KSS Pemda Nurchaerani NIP. 196507081987102003
(T. Nova Sukma, ST)	(Nurchaerani, S.E.)