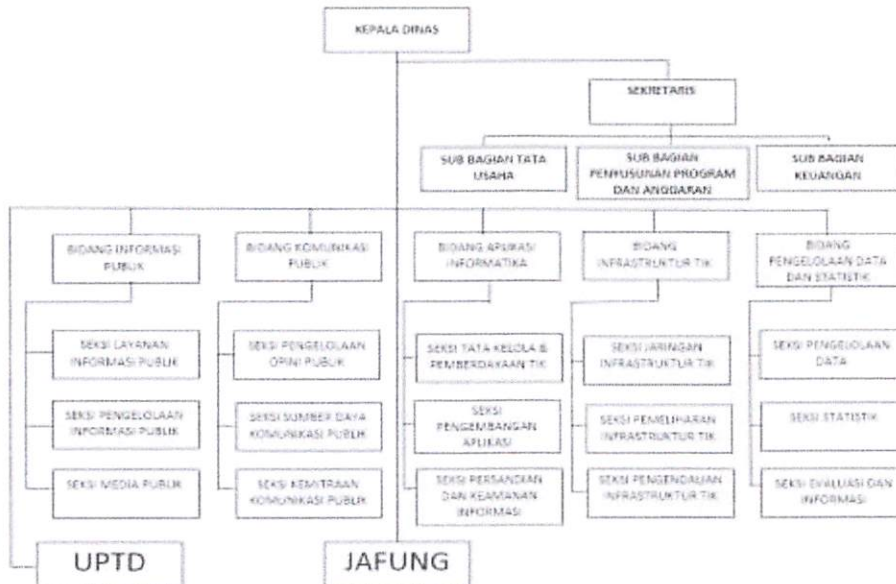


	LAPORAN HASIL VALIDASI CYBER SECURITY MATURITY	CYBER SECURITY MATURITY
Instansi/Lembaga: Dinas Komunikasi dan Informatika Provinsi Jawa Timur	Tim dari BSSN : 1. Afifah 2. Mochamad Jazuly 3. Faizal Wahyu R. 4. Sufatno 5. Dona Novan S.	
Unit Kerja: Bidang Aplikasi dan Informatika	Narasumber : 1. Drs.Ec. Nirmala Dewi, M.M. 2. Aulia Bahar Pernama, S. Kom, M.ISM 3. Ali Firman Herlambang, S.T. 4. Taufiq Ramadhany, S.T. 5. Raden Makaryo Nugrahadi, S. Kom. 6. Adi Kurniawan, S.Kom., M.Kom.	
Alamat: Jl. Ahmad Yani No.242-244, Gayungan	Telepon: Telp (031) 8294608	
Email: csirt@jatimprov.go.id	Pimpinan Unit Kerja: Drs.Ec. Nirmala Dewi, M.M.	
<p>1. Ruang Lingkup</p> <p>Ruang lingkup penilaian kematangan keamanan siber (Cyber Security Maturity) pada Dinas Komunikasi dan Informatika Pemerintah Provinsi Jawa Timur mencakup 5 aspek yaitu aspek tata kelola, aspek identifikasi, aspek proteksi, aspek deteksi, dan aspek respon.</p> <p>2. Fungsi Kerja</p> <p>Dinas Komunikasi dan Informatika Provinsi Jawa Timur memiliki tugas membantu Gubernur menyiapkan bahan pelaksanaan urusan pemerintahan yang menjadi kewenangan Pemerintah Provinsi di bidang komunikasi dan informasi serta tugas pembantuan. Dan Dinas Komunikasi dan Informatika Provinsi Jawa Timur menyelenggarakan fungsi:</p> <ol style="list-style-type: none"> perumusan kebijakan di bidang komunikasi dan informasi; pelaksanaan kebijakan di bidang komunikasi dan informasi; pelaksanaan evaluasi dan pelaporan di bidang komunikasi dan informasi; pelaksanaan administrasi dinas di bidang komunikasi dan informasi; pelaksanaan fungsi lain yang diberikan oleh Gubernur terkait dengan tugas dan fungsinya. <p>3. Lokasi</p> <p>Diskominfo Provinsi Jawa Timur Berkolasi di Jalan A. Yani 242 - 244, Surabaya</p>		

Berdasarkan wawancara terhadap narasumber instansi/lembaga disimpulkan sbb:

I. KONDISI UMUM

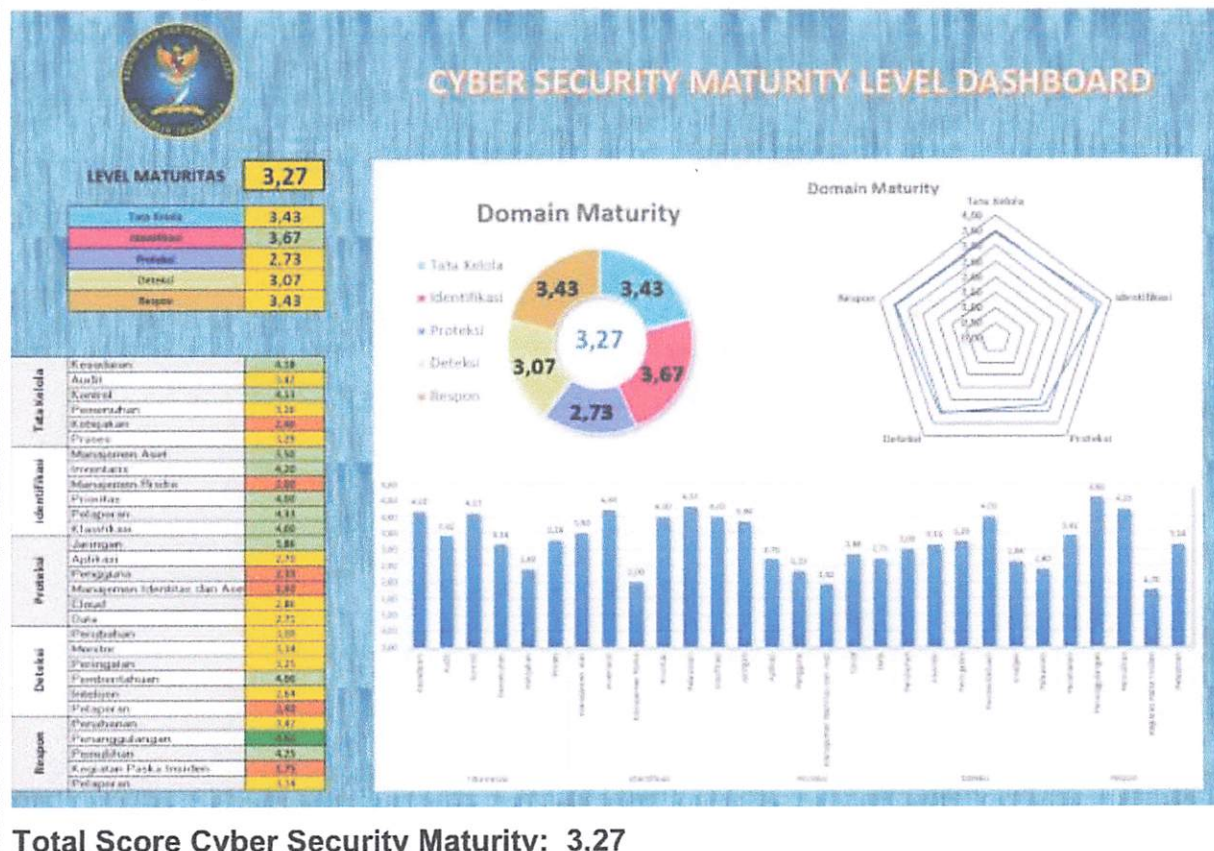
a. Struktur organisasi satuan kerja dalam ruang lingkup



b. SDM pengelola terdiri dari 22 orang ASN dan 8 orang Honorer

c. Berdasarkan wawancara dalam rangka validasi pengisian Cyber Security Maturity diperoleh hasil sebagai berikut:

Hasil Maturity: Level 3



II. KEKUATAN / KEMATANGAN

Berdasarkan hasil validasi penilaian kematangan keamanan siber (*Cyber Security Maturity*), dapat disimpulkan kondisi kekuatan keamanan siber pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur 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. Setiap karyawan baru diberikan pengarahan mengenai keamanan informasi.
4. Gap analisis telah dilakukan untuk memahami skill dan behavior yang tidak dimiliki oleh karyawan, dan menggunakan informasi tersebut untuk membuat roadmap terkait baseline pendidikan dan pelatihan terkait keamanan informasi.
5. Pelatihan mengenai pentingnya penggunaan secure authentication, tentang penyebab kebocoran data secara tidak sengaja, tentang perlindungan data sensitif dan kewajiban menjaga data privasi telah dilaksanakan untuk semua karyawan secara berkala minimal setahun sekali.
6. Pelaksanaan risk assessment dan risk treatment telah dilakukan dan direviu secara berkala setiap setahun sekali. Dan selalu dilakukan pencegahan, atau pengurangan terhadap dampak/efek yang tidak diinginkan dari risk maupun opportunities yang dimiliki organisasi.
7. Pelaksanaan internal audit telah dilakukan setiap setahun sekali.
8. Aliran data di seluruh sistem jaringan telah didokumentasikan dan dilakukan pembaruan setiap ada perubahan.
9. Standar konfigurasi (port, protokol, service) telah diterapkan dan dikonfigurasi.
10. Sistem manajemen keamanan informasi telah dipastikan dapat mencapai hasil yang diharapkan.
11. Semua tanggungjawab keamanan informasi telah ditentukan dan dialokasikan secara menyeluruh.
12. Organisasi telah mewajibkan semua karyawan dan kontraktor untuk menerapkan keamanan informasi sesuai dengan kebijakan yang ditetapkan dan prosedur organisasi.
13. Program untuk vulnerability assessment atau penetrating testing pada aplikasi web, aplikasi client-based, aplikasi mobile, wireless, server dan perangkat,

jaringan telah dilaksanakan secara berkala.

14. Aplikasi web organisasi telah dilindungi menggunakan firewall aplikasi web (WAFs).
15. Alamat IP internal di organisasi telah dilindungi oleh NAT (Network Address Translation)
16. Penggunaan IDS/IPS telah diterapkan jaringan internal dan jaringan perimeter, serta diperbarui secara regular dengan threat intelligence.
17. Software anti virus dan anti malware telah diimplementasikan secara terpusat dan selalu update terhadap perangkat endpoint.
18. DLP (Data Loss Prevention) maupun NAC (Network Access Control) telah diimplementasikan di organisasi.
19. Penerapan kontrol keamanan telah dilakukan revidu secara berkala setiap tahun/ setiap ada perubahan untuk meminimalisir risiko.
20. Risk register terkait keamanan informasi yang diperoleh berdasarkan probabilitas dan dampak yang disesuaikan dengan kriteria organisasi.
21. Kebijakan Domain-based Message Authentication Reporting and Conformance (DMARC) atau protokol otentikasi email untuk melindungi domain dari penggunaan yang tidak sah telah diterapkan di organisasi.
22. Peraturan, persyaratan kontrak, dan peraturan lainnya telah diidentifikasi, didokumentasi dan diperbarui untuk setiap sistem informasi.
23. Kepatuhan pengguna terhadap Kebijakan Keamanan Informasi organisasi telah diukur secara berkala setiap setahun sekali.
24. Kontrol kriptografi telah diterapkan sesuai dengan peraturan yang berlaku.
25. 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.
26. Dokumentasi yang dimiliki organisasi dilindungi dan dijaga agar tidak hilang, hancur, dipalsukan, diakses oleh pihak yang tidak sah sesuai dengan persyaratan dan peraturan.
27. Business Continuity Plan dan Disaster Recovery Plan yang dimiliki organisasi telah mencakup backup dan restorasi data berdasarkan prioritas analisis kritisitas data.
28. 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.
29. Risk analisis untuk keamanan TI terkait keamanan fisik dan sistem elektronik telah dilakukan setiap setahun sekali.

30. Kebijakan dan prosedur keamanan informasi telah dikembangkan sesuai dengan kerangka kerja dan standar yang diakui yaitu menggunakan ISO 270001.
31. Informasi dari pihak ketiga yang akan digunakan untuk melaporkan insiden keamanan telah dihimpun dan dijaga.
32. Konfigurasi firewall terdokumentasi dengan baik dan dilakukan reviu terhadap konfigurasi router dan switch minimal setiap 6 bulan.
33. Konfigurasi dan akun default selalu diubah sebelum digunakan, serta didokumentasikan.

b. Aspek Identifikasi

1. Organisasi telah melakukan inventarisasi data yang ada pada semua aset perangkat keras maupun perangkat lunak. Dan aset yang diidentifikasi telah disusun berdasarkan klasifikasi kritikalitas.
2. Organisasi telah melakukan klasifikasi informasi (rahasia, terbatas, umum) dan melakukan inventarisasi
3. Organisasi telah melakukan vulnerability scanning dan/atau penetration testing terhadap semua aset perangkat dan aplikasi secara berkala.
4. Telah dilakukan pemeringkatan pada kerentanan yang teridentifikasi berdasarkan pedoman / standar / acuan organisasi.
5. Risk register telah terdokumentasi untuk semua aplikasi yang memproses data stakeholder.
6. Organisasi telah memiliki Business Impact Analysis terhadap perangkat dan aplikasi TI dan direviu secara berkala setiap setahun sekali atau setiap ada perubahan.
7. Organisasi telah melakukan prioritas upaya remediasi dengan memanfaatkan level risiko dari hasil penilaian risiko.
8. Organisasi telah melakukan prioritas terkait langkah proteksi keamanan siber termasuk strategi untuk memprioritaskan perlindungan data dan aset kritis.
9. Pengelolaan data log keamanan informasi digunakan setiap hari secara otomatis untuk dilaporkan kepada manajemen.
10. Aspek keamanan mempertimbangkan kapasitas server dan perangkat jaringan secara menyeluruh.
11. Organisasi memiliki metode / standar untuk klasifikasi aset TI dan dilakukan reviu secara berkala setahun sekali atau setiap ada perubahan.
12. Organisasi telah melakukan segmentasi jaringan berdasarkan fungsionalitas

c. Aspek Proteksi

1. Penggunaan IDS dan IPS dengan menggunakan Fortiget;
2. Memanfaatkan sistem enkripsi dalam akses nirkabel;
3. Koneksi ke server dan jaringan sudah menggunakan protocol enkripsi;
4. Penggunaan firewall telah di konfigurasi dengan baik seperti implicit atau explicit deny any/any rule, inbound network traffic dan outbound network traffic;
5. Menerapkan port access control pada perangkat yang terhubung;
6. Menerapkan firewall filtering antar segmen;
7. Sudah menggunakan DNS Filtering;
8. Sudah dilakukan pemisahan sebagian besar server fisik maupun virtual;
9. Pengelolaan patching sudah dilakukan namun masih secara manual;
10. Sudah ada SLA terkait jaminan dalam menentukan RTO dan RPO;
11. Sudah ada whitelist aplikasi dalam memastikan authorized software library;
12. Sudah dilakukan updating secara berkala dalam penggunaan web browser, dan email client dalam organisasi;
13. Penggunaan Anti Virus sudah di gunakan sampai ke end point;
14. Kontrol keamanan serta enkripsi sudah di implementasikan pada perangkat endpoint pengguna;
15. Sudah ada pengaturan kompleksitas terkait password yang digunakan pada aplikasi email;
16. Organisasi sudah memiliki cloud internal yang memiliki proses otorisasi;
17. Sudah dilakukan backup secara berkala terkait aset yang ada di organisasi;
18. Penyimpanan log sudah dilakukan serta pemanfaatan NTP dalam rangka audit dan forensik;
19. Penyimpanan data backup sudah dilindungi baik secara fisik dan non fisik

d. Aspek Deteksi

1. Organisasi melakukan monitoring terhadap log dari perangkat security control, jaringan, dan aplikasi selama 24 jam
2. Organisasi Anda mengaktifkan Enable Detailed Logging yang mencakup informasi terperinci seperti event source, tanggal, user, timestamp, source addresses, destination addresses, dan komponen lainnya
3. Setiap orang yang tergabung dalam tim monitoring pada organisasi mendapatkan peningkatan keterampilan
4. Organisasi memantau akses fisik terhadap perangkat yang berada di dalam

ruangan data center untuk mendeteksi potensi kejadian keamanan siber

5. Organisasi memantau akses fisik terhadap perangkat yang berada di dalam ruangan data center untuk mendeteksi potensi kejadian keamanan siber
6. Organisasi memiliki ticketing system yang digunakan untuk melacak progres dari events post-notification
7. Organisasi memantau akses fisik terhadap perangkat yang berada di dalam ruangan data center untuk mendeteksi potensi kejadian keamanan siber
8. Organisasi memiliki perangkat anti-malware yang secara otomatis melakukan scanning terhadap removable media yang terhubung ke perangkat
9. Organisasi memiliki ticketing system yang digunakan untuk melacak progres dari events post-notification
10. Ticketing system melacak kejadian berdasarkan tingkat keparahan / prioritas / dampak, kategori keamanan, dan jenis log yang berkorelasi untuk suatu kejadian
11. Organisasi memiliki SOC atau manajemen teknis yang dapat dihubungi setiap saat (24x7) untuk menangani kejadian dengan prioritas tinggi dan kritikal
12. Organisasi memiliki contact tree untuk mengeskalisasi dalam merespon suatu kejadian
13. Organisasi memiliki sistem untuk melakukan Malicious Code Detection untuk mendeteksi, menghapus, dan melindungi dari malicious code
14. Organisasi mengetahui atau dapat mendefinisikan dimana program deteksi beroperasi dan tujuan apa yang akan dicapai/diidentifikasi

e. Aspek Respon

1. Organisasi telah memiliki kebijakan penanganan insiden, SOP, DRP yang direviu secara berkala;
2. Sudah dilakukan drill test dalam rangka pelatihan respon insiden yang mencakup peningkatan kemampuan teknis pelapotan insiden.
3. Sudah dilakukan pelatihan tentang cara identifikasi, penanganan dan pelaporan insiden untuk staf TIK;
4. Organisasi telah memiliki kontak pihak terkait apabila terjadi insiden;
5. Rencana respon insiden telah terdokumentasi;
6. Sudah dilakukan backup data karyawan pada cloud organisasi;
7. Tim respon insiden telah memiliki peralatan sumber daya analisis insiden, kemampuan dalam penanganan insiden sampai ke rekomendasi;
8. Sudah ada sumber redundan yang di backup sehingga dapat digunakan sebagai data redundan;

9. Setiap insiden yang terjadi sudah dipastikan bahwa insiden sudah ditangani/celah sudah ditutup;
10. Sudah memiliki metode yang terdokumentasi yang dapat digunakan media informasi ke stakeholder sekaligus digunakan dalam pelaporan oleh stakeholder;
11. Sudah memiliki kontak pihak terkait apabila terjadi insiden;
12. Pelaporan insiden sudah dilakukan yang digunakan sebagai pencatatan langkah-langkah yang dilakukan dalam penanganan insiden;
13. Sudah ada jaminan server dapat kembali normal apabila terjadi insiden;
14. Dalam Analisa insiden sampai ke reviu root cause dalam rangka pencegahan agar insiden tidak berulang kembali;
15. Telah dilakukan reviu dalam rekapl laporan insiden siber;
16. Jika terjadi insiden siber yang berdampak pada kehilangan data pribadi, organisasi telah melakukan investigasi, melakukan perbaikan, menginformasikan pada pihak terkait dan stakeholder;
17. Sudah ada website yang dapat digunakan untuk pelaporan anomali dan insiden siber;
18. Sudah ada standar waktu terkait pelaporan insiden yang tertuang di SOP;
19. Laporan insiden sudah dilaporkan sampai ke middle management

III. KELEMAHAN / KEKURANGAN

Berdasarkan hasil validasi penilaian kematangan keamanan siber (*Cyber Security Maturity*), dapat disimpulkan kondisi kelemahan/kekurangan keamanan siber pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur sebagai berikut:

a. Aspek Tata Kelola

1. Organisasi belum melakukan simulasi phising setidaknya setiap tahun
2. Organisasi belum menginformasikan kepada stakeholder tentang teknik atau kerentanan siber yang berkembang saat ini yang dapat digunakan dalam peningkatan risiko fraud/penipuan.
3. Organisasi belum memiliki kebijakan yang mengharuskan penerapan perlindungan data pribadi.
4. Organisasi masih menggunakan satu akun untuk melakukan vulnerability scanning.
5. Organisasi belum melakukan review izin akses dari akun pengguna setidaknya setiap tiga bulan.

6. Organisasi 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.
7. Belum dilakukuan filterisasi terhadap seluruh jenis file lampiran email.
8. Organisasi belum menerapkan metode sandbox terhadap seluruh lampiran email guna mencegah dan analisis keamanan lebih lanjut terhadap malicious behaviour.
9. Belum ada kebijakan perlindungan data stakeholder secara spesifik atau dokumen khusus yang termasuk dalam Kebijakan Keamanan Informasi. Serta belum ada kebijakan apapun yang mengatur tentang data pribadi.
10. Privasi dan perlindungan informasi pribadi belum dipastikan sesuai dengan persyaratan dalam undang-undang dan peraturan terkait lainnya yang berlaku.
11. Belum ada personil yang ditunjuk secara khusus bertanggungjawab untuk pengembangan dan implementasi kebijakan dan prosedur perlindungan data pribadi.
12. Tidak ada kebijakan yang terdokumentasikan terkait penetapan sanksi yang dijatuhkan terhadap karyawan yang tidak patuh pada kebijakan yang berkaitan dengan keamanan siber.
13. Belum ada kebijakan keamanan informasi mengatur mengenai single ID yang unik untuk melakukan semua otentikasi.
14. Belum ada kebijakan yang mengatur semua akun di organisasi memiliki tenggat waktu kadaluarsa.
15. Belum ada kebijakan terminasi diterapkan dengan masa tenggang yang diizinkan terkait hak akses karyawan ke dalam sistem informasi.
16. Belum ada kebijakan yang mengakomodir laporan karyawan ataupun stakeholder terkait kehilangan perangkat laptop/smartphone yang kemungkinan dapat digunakan sebagai kegiatan penipuan/kejahatan
17. Belum ada pengembangan software di organisasi secara internal/mandiri sehingga belum diterapkan aspek-aspek keamanan yang dapat diimplementasikan seperti verifikasi secure code secara mandiri, pelatihan personil yang terlibat, dll.
18. Organisasi belum menerapkan praktik secure coding yang sesuai dengan bahasa pemrograman dan development environment yang digunakan.
19. Organisasi belum memiliki kebijakan metode penghapusan data.

b. Aspek Identifikasi

1. Tidak dilakukan identifikasi maupun pembatasan akses perangkat yang tidak diijinkan oleh organisasi.
2. Organisasi belum melakukan analisa keterkaitan antara keamanan dan kenyamanan dari penggunaan aset perangkat dan aplikasi dalam rangka penyusunan standar keamanan informasi.
3. Belum ada kebijakan pembatasan penggunaan aset organisasi untuk kepentingan pribadi.
4. Karyawan diizinkan memiliki akses sebagai administrator pada perangkat (laptop, personal computer, dll) milik organisasi.
5. Pihak ketiga diizinkan untuk menggunakan aset mereka pada jaringan organisasi.
6. Tidak ada dokumentasi mengenai alur informasi yang memproses data stakeholder termasuk yang dikelola oleh pihak ketiga.
7. Tidak kebijakan dan implementasi mengenai retensi data sensitive termasuk data stakeholder / klien / konsumen / pelanggan di organisasi dengan kebijakan regulasi dan kebutuhan bisnis.
8. Belum ada metadata sensitif termasuk data stakeholder yang disimpan (secara elektronik dan hardcopy) dan memuat metadata informasi periode retensi, pemilik data, dan penggunaan data.
9. Organisasi belum menon-aktifkan aset perangkat dan aplikasi yang tidak diperlukan oleh organisasi.
10. Masih terdapat data otentikasi yang disimpan diperangkat browser end user.
11. Organisasi tidak memperbaharui roadmap keamanan TI organisasi dalam jangka waktu tertentu.
12. Organisasi belum melakukan klasifikasi terhadap cyber threats yang ditemukan pada organisasi.

c. Aspek Proteksi

1. Belum menggunakan otentikasi terpusat;
2. Belum ada pembatasan komunikasi antar workstation, pembatasan fitur wireless, koneksi peer-to-peer pada wireless client;
3. Belum ada pembatasan aplikasi yang diunduh, di install dan di operasikan ;
4. Belum ada pengecekan otomatis terhadap spam/phising/malware yang ada di cloud;
5. Belum ada pembatasan penggunaan scripting tools;
6. Master image belum dilakukan penyimpanan;

7. Penggunaan add-on dan plugin aplikasi belum ada pembatasan;
8. Belum ada otomatisasi permohonan kata sandi pada perangkat yang tidak aktif;
9. Belum ada batasan fitur auto-run content dan pengaturan akses read/write pada perangkat USB;
10. Enkripsi belum dilakukan pada perangkat eksternal organisasi;
11. Belum ada pembatasan akun pada laptop organisasi;
12. Belum ada pemanfaatan identity and access management system, Multi-Factor Authentication;
13. Belum memanfaatkan metode otentikasi pada saluran yang terenkripsi dan juga penambahan OTP;
14. Penggunaan IP reputation belum dimanfaatkan secara maksimal;
15. Organisasi belum dapat melakukan pelacakan dan mendeteksi perilaku anomali dari karyawan ataupun stakeholder;
16. Belum dilakukan identifikasi perangkat yang terhubung;
17. Akses akun database hanya ada satu yaitu admin;
18. Belum ada penerapan SSO, pembatasan IP dan MMA pada akses cloud;
19. Belum ada Data Center Redudancy terkait cloud yang ada di organisasi;
20. Pengujian data integrity pada data yang dibackup belum dilakukan;
21. Data juga belum dilakukan enkripsi dalam penyimpanan dan pengiriman;

d. Aspek Deteksi

1. Perubahan konfigurasi pada peralatan jaringan tidak terdeteksi secara otomatis
2. Organisasi tidak memiliki mekanisme monitoring terhadap akses dan perubahan pada data sensitif (seperti File Integrity Monitoring atau Event Monitoring)
3. Organisasi tidak memiliki mekanisme monitoring dan deteksi terhadap penggunaan enkripsi yang tidak sah
4. Organisasi tidak menerapkan SIEM atau Log Analytic Tools untuk keperluan dokumentasi, korelasi, dan analisis log
5. Organisasi belum menjamin alokasi kapasitas penyimpanan log sesuai dengan kebutuhan
6. Organisasi tidak memantau aktifitas pihak ketiga untuk mendeteksi adanya potensi kejadian keamanan siber
7. Log hasil deteksi malware belum terhubung dengan perangkat antimalware administrations dan event log servers sehingga dapat digunakan untuk analisis

8. Escalation profile belum dibuat untuk setiap security event yang ditemukan, dan tidak disimpan sebagai panduan untuk digunakan di masa mendatang
9. Organisasi tidak menerapkan event notification yang berbeda-beda untuk setiap jenis eskalasi
10. Organisasi belum memperoleh informasi dari multiple threat intelligence feeds untuk mendeteksi serangan siber
11. Organisasi belum menjalankan vulnerability scanning tools secara otomatis untuk mendeteksi kerentanan siber
12. Organisasi belum memiliki unit yang melakukan Cyber Threat Intelligence (CTI)

e. Aspek Respon

1. Belum dilakukan penilaian insiden dalam rangka triase insiden;
2. Diskoneksi segmen jaringan dilakukan dalam waktu 60 menit;
3. Belum ada jaminan penyerang dapat mengakses server backup apabila DMZ terkena serangan siber;
4. Rekap insiden siber sudah dilaporkan namun belum sampai ke Top Management dan belum di distribusikan pada pemangku kepentingan;
5. Belum ada SLA dalam penanganan insiden;
6. Rekaman insiden dan pelanggaran di organisasi belum disimpan dan dilaporkan;
7. Belum ada perhitungan manfaat dalam penganggaran di organisasi;

IV. REKOMENDASI:

Berdasarkan hasil validasi penilaian kematangan keamanan siber (*Cyber Security Maturity*), berikut ini rekomendasi yang dapat dilakukan dalam rangka peningkatan kematangan siber pada Dinas Komunikasi dan Informatika Provinsi Jawa Timur sebagai berikut:

1. Menyelenggarakan simulasi phising setidaknya setiap tahun.
2. Menginformasikan kepada stakeholder tentang teknik atau kerentanan siber yang berkembang saat ini yang dapat digunakan dalam peningkatan risiko fraud/penipuan.
3. Menyusun kebijakan perlindungan data stakeholder secara spesifik atau dokumen khusus yang termasuk dalam Kebijakan Keamanan Informasi dan aturan yang berkaitan dengan data pribadi antara lain:
 - a. Kebijakan mencakup keharusan penerapan perlindungan data pribadi.

- b. Menunjuk personil yang ditunjuk secara khusus bertanggungjawab untuk pengembangan dan implementasi kebijakan dan prosedur perlindungan data pribadi.
 - c. Menyampaikan/menginformasikan kebijakan data privasi kepada stakeholder segera setelah terjalin kerjasama karena belum ada kebijakan data privasi.
 - d. Menyusun kebijakan atau prosedur mengenai pemberitahuan jika terjadi pelanggaran terhadap data pribadi dan mendokumentasikan.
 - e. Menyusun kebijakan dan prosedur terkait pemberitahuan dan keputusan stakeholder untuk memilih tidak membagikan data mereka.
 - f. Dalam memberikan data stakeholder kepada pihak ketiga, stakeholder memiliki kewenangan untuk mengetahui mengenai distribusi data milik mereka.
4. Menggunakan akun khusus dalam melakukan vulnerability scanning. Dan setiap akun pengguna atau sistem yang digunakan dalam melakukan penetrating testing 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.
 5. Melaksanakan reviu izin akses dari akun pengguna setidaknya setiap tiga bulan.
 6. Pembentukan Red Team dan Blue Team serta melakukan pengujian secara berkala dalam mengukur kesiapan organisasi untuk mengidentifikasi dan menghentikan serangan atau merespon dengan cepat dan efektif dari insiden keamanan yang terjadi.
 7. Melakukan filterisasi terhadap seluruh jenis file lampiran email.
 8. Menerapkan metode sandbox terhadap seluruh lampiran email guna mencegah dan analisis keamanan lebih lanjut terhadap malicious behaviour.
 9. Menyusun kebijakan terkait penetapan sanksi yang dijatuhkan terhadap karyawan yang tidak patuh pada kebijakan yang berkaitan dengan keamanan siber.
 10. Menyusun kebijakan keamanan informasi mengatur mengenai single ID yang unik untuk melakukan semua otentikasi.
 11. Menyusun kebijakan yang mengatur semua akun di organisasi memiliki tenggat waktu kadaluarsa.
 12. Menyusun kebijakan terminasi diterapkan dengan masa tenggang yang diizinkan terkait hak akses karyawan ke dalam sistem informasi.
 13. Menyusun kebijakan yang mengakomodir laporan karyawan ataupun stakeholder terkait kehilangan perangkat laptop/smartphone yang kemungkinan dapat digunakan sebagai kegiatan penipuan/kejahatan
 14. Menyusun kebijakan metode penghapusan data.

15. Dalam pengembangan software di organisasi secara internal/mandiri perlu diterapkan beberapa aspek keamanan sebagai berikut:
 - a. Menerapkan praktik secure coding yang sesuai dengan bahasa pemrograman dan development environment yang digunakan.
 - b. Memastikan bahwa pengecekan kesalahan secara eksplisit dilakukan dan didokumentasikan untuk semua input, termasuk ukuran, tipe data, dan rentang atau format yang diterapkan.
 - c. Melakukan analisis statis dan/atau dinamis untuk memverifikasi bahwa praktik secure coding benar-benar diterapkan pada software yang dikembangkan secara internal.
 - d. Source code yang dibuat secara mandiri dilakukan reвью kerentanannya terlebih dahulu sebelum masuk ke production.
 - e. Melakukan pelatihan dalam membuat secure code yang baik kepada personil yang terlibat.
8. Melakukan identifikasi maupun pembatasan akses perangkat yang tidak diijinkan oleh organisasi.
9. Melakukan analisa keterkaitan antara keamanan dan kenyamanan dari penggunaan aset perangkat dan aplikasi dalam rangka penyusunan standar keamanan informasi.
10. Menyusun kebijakan pembatasan penggunaan aset organisasi untuk kepentingan pribadi.
11. Tidak mengizinkan karyawan memiliki akses sebagai administrator pada perangkat (laptop, personal computer, dll) milik organisasi. Dan tidak mengizinkan pihak ketiga untuk menggunakan aset mereka pada jaringan organisasi.
12. Mendokumentasikan alur informasi yang memproses data stakeholder termasuk yang dikelola oleh pihak ketiga.
13. Menyusun kebijakan dan melakukan implementasi mengenai retensi data sensitive termasuk data stakeholder di organisasi dengan kebijakan regulasi dan kebutuhan bisnis.
14. Membuat metadata sensitif termasuk data stakeholder yang disimpan (secara elektronik dan hardcopy) dan memuat metadata informasi periode retensi, pemilik data, dan penggunaan data.
15. Menon-aktifkan aset perangkat dan aplikasi yang tidak diperlukan oleh organisasi.
16. Data otentikasi tidak diperbolehkan disimpan di perangkat browser end user.
17. Memperbaharui roadmap keamanan TI organisasi dalam jangka waktu tertentu
18. Melakukan klasifikasi terhadap cyber threats yang ditemukan pada organisasi.

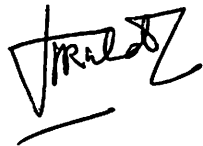
19. Organisasi diharapkan mampu menerapkan otentikasi terpusat;
20. Organisasi diharapkan dapat menerapkan pembatasan komunikasi antar workstation, pembatasan fitur wireless, koneksi peer-to-peer pada wireless client;
21. Organisasi diharapkan dapat menerapkan pembatasan aplikasi yang diunduh, di install dan di operasikan ;
22. Organisasi diharapkan dapat menerapkan pengecekan otomatis terhadap spam/phising/malware yang ada di cloud;
23. Organisasi diharapkan dapat menerapkan ada pembatasan penggunaan scripting tools;
24. Master image sebaiknya disimpan;
25. Organisasi perlu menerapkan pembatasan penggunaan add-on dan plugin aplikasi;
26. Organisasi diharapkan dapat menerapkan otomatisasi permohonan kata sandi pada perangkat yang tidak aktif;
27. Perlu adanya pembatasan fitur auto-run content dan pengaturan akses read/write pada perangkat USB;
28. Enkripsi sebaiknya dilakukan pada perangkat eksternal organisasi;
29. Perlu adanya pembatasan akun pada laptop organisasi;
30. Perlu adanya pemanfaatan identity and access management system, Multi-Factor Authentication;
31. Organisasi sebaiknya memanfaatkan metode otentikasi pada saluran yang terenkripsi dan juga penambahan OTP;
32. Organisasi diharapkan dapat mengoptimalkan penggunaan IP reputation belum;
33. Organisasi diharapkan dapat meningkatkan kemampuan untuk melacak dan mendeteksi perilaku anomali dari karyawan ataupun stakeholder;
34. Organisasi diharapkan dapat melakukan identifikasi perangkat yang terhubung;
35. Akses akun database dilakukan oleh akun khusus selain admin
36. Organisasi diharapkan dapat menerapkan SSO, pembatasan IP dan MMA pada akses cloud;
37. Organisasi sebaiknya memiliki Data Center Redudancy terkait cloud yang ada di organisasi;
38. Organisasi perlu melakukan pengujian data integrity pada data yang dibackup;
39. Data yang disimpan dan dikirim sebaiknya dilakukan enkripsi;
40. Melakukan deteksi perubahan konfigurasi pada peralatan jaringan sehingga dapat terdeteksi secara otomatis

41. Organisasi diharapkan memiliki mekanisme monitoring terhadap akses dan perubahan pada data sensitif (seperti File Integrity Monitoring atau Event Monitoring)
42. Organisasi diharapkan memiliki mekanisme monitoring dan deteksi terhadap penggunaan enkripsi yang tidak sah
43. Organisasi perlu menerapkan SIEM atau Log Analytic Tools untuk keperluan dokumentasi, korelasi, dan analisis log
44. Organisasi diharapkan mampu menjamin alokasi kapasitas penyimpanan log sesuai dengan kebutuhan
45. Organisasi diharapkan dapat memantau aktifitas pihak ketiga untuk mendeteksi adanya potensi kejadian keamanan siber
46. Log hasil deteksi malware diharapkan dapat terhubung dengan perangkat antimalware administrations dan event log servers sehingga dapat digunakan untuk analisis
47. Escalation profile seharusnya dibuat untuk setiap security event yang ditemukan, dan dapat disimpan sebagai panduan untuk digunakan di masa mendatang
48. Organisasi sebaiknya menerapkan event notification yang berbeda-beda untuk setiap jenis eskalasi
49. Organisasi diharapkan dapat memperoleh informasi dari multiple threat intelligence feeds untuk mendeteksi serangan siber
50. Organisasi diharapkan dapat menjalankan vulnerability scanning tools secara otomatis untuk mendeteksi kerentanan siber
51. Organisasi sebaiknya memiliki unit yang melakukan Cyber Threat Intelligence (CTI)
52. Organisasi diharapkan menerapkan penilaian insiden dalam rangka triase insiden;
53. Diskoneksi segmen jaringan diharapkan dapat ditingkatkan;
54. Organisasi diharapkan dapat menjamin penyerang tidak dapat mengakses server backup apabila DMZ terkena serangan siber;
55. Rekap insiden siber diharapkan dapat disampaikan ke Top Management dan distribusikan pada pemangku kepentingan;
56. Organisasi diharapkan memiliki SLA penanganan insiden;
57. Organisasi dapat menyimpan dan melaporkan rekaman insiden dan pelanggaran di organisasi.
58. Organisasi diharapkan memiliki perhitungan ROI dalam penganggaran di organisasi.

Surabaya, 24 November 2020

Narasumber Instansi

Drs.Ec. Nirmala Dewi, M.M.



Tim BSSN :

1. Afifah



2. Mochamad Jazuly



3. Faizal Wahyu R.



4. Sufatno



5. Dona Novan S.

