Vol. 4 No. 2 (2022): 441-452
November 2022
e-ISSN 2656-0194

MONAS Jurnal Inovasi Aparatur

MANAJEMEN PENGETAHUAN PENANGANAN INSIDEN KEAMANAN INFORMASI PADA *SECURITY OPERATION CENTER* DI PEMERINTAH PROVINSI DKI JAKARTA

KNOWLEDGE MANAGEMENT FOR INFORMATION SECURITY INCIDENT HANDLING AT SECURITY OPERATION CENTER OF JAKARTA PROVINCIAL GOVERNMENT

Maman Firmansyah[1],*, Andrie Yuswanto[2]*
[1]Universitas Nusa Mandiri, Jl. Kramat Raya No.18, RW.7, Kwitang, Senen, Jakarta Pusat,
[2]Institut Teknologi Budi Utomo, Jl. Raya Mawar Merah No.23, Pondok Kopi. Jakarta Timur

*mfirmansyah@gmail.com[1], aandoct@gmail.com[2]

ABSTRAK

Insiden keamanan informasi tidak hanya meningkat dari sisi jumlah akan tetapi menjadi lebih beragam dan lebih merusak serta mengganggu ketersediaan pelayanan. Dibutuhkan sistem manajemen insiden untuk dapat mendeteksi dan menangani insiden keamanan informasi dengan cepat, meminimalkan kerugian, mengurangi kerentanan yang dieksploitasi dan memulihkan infrastruktur termasuk layanan. Sistem manajemen insiden perlu untuk dikelola dengan adanya Security Opeation Center (SOC). Penggunaan pengetahuan tacit telah terbukti mampu membantu mempercepat pemecahan masalah di SOC dengan lebih baik dari pengalaman dengan mengadopsi strategi yang telah digunakan sebelumnya. Penerapan pengelolaan pengetahuan di SOC sudah menjadi suatu kebutuhan mendasar. Kemampuan organisasi mengelola knowledge yang ada merupakan kekuatan yang diperlukan untuk dapat tetap bertahan menghadapi gencarnya serangan siber. Tujuan penelitian ini yaitu mengkaji proses menangkap tacit di SOC agar bisa digunakan untuk menganalisa dan menghadapi ancaman siber serta meletakkan dasar bagi manajemen pengetahuan tacit di organisasi untuk peningkatan efisiensi cara kerja dan proses dalam merespons insiden secara efisien dan sistematis.

Kata kunci: *Managemen pengetahuan, Security Operation Center, penanganan insiden, serangan siber, Keamanan Informasi*

ABSTRACT

Information security incidents have increased in number and become more diverse and destructive and disrupt service availability. An incident management system is needed to detect and handle information security incidents quickly, minimize losses, reduce exploited vulnerabilities and restore infrastructure, including services. An incident management system needs to be managed with a Security Operations Center (SOC). The use of tacit knowledge has been shown to help accelerate problem-solving in SOC better than experience by adopting strategies that have been used previously. The application of knowledge management in SOC has become a basic need. An organization's ability to manage existing knowledge is a necessary strength to be able to survive in the face of incessant cyber-attacks. This study aims to examine the process of capturing tacit in SOC so that it can be used to analyze and deal with cyber threats and to lay the foundation for implicit knowledge management in organizations to increase the efficiency of work methods and processes responding to incidents efficiently and systematically.

Keywords*: Knowledge Management, Security Operation Center, Incident Handling, Cyber Threat, Information Security*

PENDAHULUAN

Risiko keamanan terhadap informasi sensitif suatu organisasi semakin meningkat, baik berupa serangan dari sisi eksternal maupun sisi internal menjadi lebih canggih dan persisten (Sindiren & Ciylan, 2018). Penelitian yang dilakukan oleh Juniper Research pada tahun 2017 memperkirakan pelanggaran data akan menelan biaya $8 triliun secara global pada tahun 2022 (Sommestad et al., 2014). Langkah-langkah teknis yang efektif dan robust mampu mencegah risiko cyber dari pelanggaran keamanan informasi (Safa & Von Solms, 2016). Pengelolaan keamanan informasi merupakan tantangan dan terletak pada menerima individu dalam organisasi tidak hanya memiliki identitas yang diberikan oleh peran mereka akan tetapi juga identits pribadi dan social(Ashenden, 2008). Kepatuhan karyawan sangat penting bagi keberlangsungan suatu organisasi karena sebagian besar terjadinya insiden keamanan informasi secara langsung maupun tidak langsung disebabkan oleh pengguna yang melanggar atau mengabaikan kebijakan keamanan informasi yang sudah ditetapkan oleh organisasi (Pham et al., 2021).

Ada strategi organisasi yang menggunakan anggaran untuk belanja perangkat canggih seperti firewall, proxy, antivirus, mekanisme pendeteksi penyusup, tanda tangan digital, perangkat jaringan khusus dan lain-lain, dengan asumsi bahwa keamanan informasi dapat dicapai melalui pengadaan solusi teknologi. Ini adalah gagasan yang salah karena penanganan insiden keamanan informasi lebih pada mengelola sistem *end-to-end* daripada hanya memasang perangkat untuk solusi teknis. Seperti halnya sistem lainnya, ini memiliki banyak komponen termasuk orang, kebijakan, prosedur, proses, standar, dan teknologi(Dey, 2007).

Saat ini dunia bisnis telah memasuki era teknologi dan era informasi. Era ini ditandai dengan adanya pergeseran paradigma dari pekerjaan fisik ke pekerjaan yang berbasis penerapan ilmu pengetahuan dan teknologi. Kemajuan teknologi informasi memudahkan para pelaku bisnis untuk mengumpulkan data kemudian mengolahnya menjadi informasi yang akan menghasilkan pengetahuan. Di era berbasis pengetahuan, menjadikan pengetahuan sebagai keunggulan kompetitif dan sebagai sumber daya bagi kelangsungan kehidupan organisasi. Bahkan saat ini, pengetahuan dianggap sebagai kunci penting dalam persaingan dan sebagai sumber memenangkan persaingan yang menguntungkan organisasi. Organisasi membutuhkan pengetahuan untuk mendukung dan meningkatkan kegiatan organisasi. Dan pengetahuan memiliki manajemen yang sistematis, yaitu manajemen pengetahuan (Kusuma et al., 2021) (Saif & Yeop, 2020).

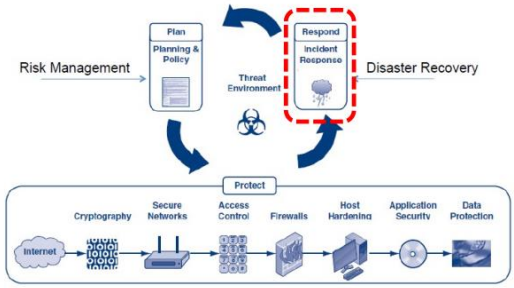
Cyber Security Operation Center (SOC) adalah salah satu pendukung keamanan informasi dan teknologi dalam suatu orgnisasi untuk memantau, melacak, dan menangani insiden dunia maya. Salah satu solusi popular untuk dapat bertahan dari ancaman siber adalah menerapkan SOC sehingga organisasi punya panduan dalam kesiapsiagaan, tanggapan, dan pemulihan terhadap insiden. Transformasi dunia menuju revolusi industri keempat dapat dilihat dari penerapan teknologi diberbagai sector. (Majid & Ariffi, 2019), tak terkecuali pemerintah provinsi DKI Jakarta yang sangat bergantung pada penggunaan teknologi dalam menjalankan roda pemerintahan dan memberikan pelayanan terkait teknologi informasi. Teknologi telah memberikan banyak manfaat dalam memberikan pelayanan bagi masyarakat, dan dapat membantu mengatur tata kelola secara efisien. Namun, dengan meningkatnya ketergantungan pada teknologi, secara tidak langsung juga meningkatkan risiko ancaman dan serangan siber. Serangan siber bukanlah hal baru bagi dunia kita; sudah dimulai sejak tahun 1960-an dimana aktivitas hacking terjadi pada frekuensi sistem telepon. Sejak itu, konsepnya menjadi semakin populer dan berkembang seiring kemajuan teknologi(Halim et al., 2019).

Mengembangkan dan menerapkan *incident response* akan membantu organisasi dalam menangani pelanggaran data dengan cepat efisien dan dengan meminimalkan kerusakan. *Incident Response* selalu menjadi aspek penting dari keamanan informasi. Banyak teknologi, platform, dan infrastruktur yang berkembang pesat untuk menyediakan kemudahan dan layanan kepada pengguna, yang menjadi target point.(Mitropoulos et al., 2006). Kerentanan didalam sistem jika tidak ditangani dengan benar, berpotensi menyebabkan serangkaian tindakan tidak sah

yang bervariasi dari serangan penolakan layanan hingga pencurian identitas. Sangat penting organisasi untuk memperlakukan setiap insiden keamanan (yaitu aktivitas terkait dengan implikasi keamanan negatif sepenuhnya, dengan mengimplemtasikan metode, mekanisme, dan/atau kebijakan respons yang tepat untuk meminimalkan efeknya(Mitropoulos et al., 2006). Tindakan ini harus bertujuan untuk mendapatkan sumber sebenarnya dari sebuah insiden. Penanggulangan ini dapat bervariasi dari perbaikan sederhana (misalnya pembaruan perangkat lunak) hingga Kebijakan *Incident Response* yang sangat kompleks yang harus diterapkan dalam organisasi. *Incident Response* dapat didefinisikan sebagai proses yang bertujuan untuk meminimalkan kerusakan dari insiden keamanan dan malfungsi, serta memantau dan belajar dari insiden tersebut(Mariki Eloff & Jan Eloff, 2003).

Bidang Siber & Sandi pemerintah provinsi DKI Jakarta yang mempunyai tugas pokok untuk menyelenggarakan layanan siber dan sandi serta keamanan informasi bertanggung jawab dalam pelaksanaan literasi dan asistensi pengendalian keamanan serta penanggulangan dan pemulihan insiden keamanan informasi(Bidang Siber dan Sandi DKI, 2021). Untuk memudahkan koordinasi teknis terhadap komplain yang diterima dan bersifat reaktif, dibentuklah Jakarta Prov CSIRT. Dalam pembentukannya, JakartaProv-CSIRT memiliki tujuan untuk membangun mengkoordinasikan, mengkolaborasikan dan mengoperasionalkan sistem mitigasi, manajemen krisis, penanggulangan dan pemulihan terhadap insiden keamanan siber, serta membangun kapasitas sumber daya penanggulangan dan pemulihan insiden keamanan siber pada sektor Pemerintah Daerah Provinsi DKI Jakarta(CSIRT, 2021). Dalam pengelolaan keamanan informasi melalui SOC untuk memberikan layanan e-Government di Pemprov DKI Jakarta saat ini merupakan hal terpenting seiring dengan kejahatan siber/cyber crime yang semakin meningkat (Andrie Yuswanto, 2020)

Manajemen pengetahuan adalah salah satu pendekatan pengelolaan berbagai pengetahuan termasuk dalam penanganan insiden keamanan informasi yang ada di Bidang Siber & Sandi yang siklus di dalamnya meliputi menangkap pengetahuan, berbagi dan diseminasi pengetahuan, dan akuisisi dan penerapan pengetahuan. Pengetahuan dalam menangani inciden keamanan yang kebanyakan merupakan pengetahuan tacit yang dimiliki individu tertentu memerlukan pendekatan yang tepat agar dapat ditangkap untuk kemudian dimanfaatkan organisasi.



Gambar 1. Urgensi penanganan insiden keamanan informasi(Novian Nur Cahya & Operasi Keamanan Siber, 2022)

Pengetahuan dalam penanganan insiden keamanan informasi diperoleh dari *capture tacit knowledge* dari ahli yang sudah memperoleh pengetahuan dan pengalaman serta *trick-trick* dalam menangani dan merespon insiden. *Knowledge* atau pengetahuan dalam menangani insiden adalah salah satu sumber daya yang penting bagi Bidang Siber & Sandi dalam mengemban misi terciptanya sistem keamanan informasi yang handal di lingkungan pemerintah provinsi DKI Jakarta.

METODOLOGI

Untuk mendukung penyusunan manajemen pengetahuan penanganan insiden keamanan informasi ini dilakukan dengan pengamatan lapangan secara langsung serta studi kepustakaan dimana data dan informasi didapatkan melalui buku, artikel dan jurnal yang berkaitan dengan topik knowledge management incident handling serta materi edukasi dan literasi yang diterbitkan Bidang Siber dan Sandi Negara (BSSN).

HASIL DAN PEMBAHASAN

Tim Tanggap Insiden Siber Propinsi DKI Jakarta melaksanakan layanan tanggap insiden siber, berupa layanan reaktif, yaitu layanan yang terkait dengan kebutuhan melakukan respon terhadap insiden siber

termasuk penangkalan, penindakan dan pemulihan siber dan layanan proaktif, yaitu layanan yang mendeteksi dan mencegah serangan siber sebelum ada dampak nyata. Tim Tanggap Insiden Siber Propinsi DKI Jakarta secara resmi di-launching pada 23 Desember 2020. Konstituen Tim Tanggap Insiden Siber meliputi Perangkat Daerah (OPD) di lingkungan Pemerintah Daerah Provinsi DKI Jakarta.

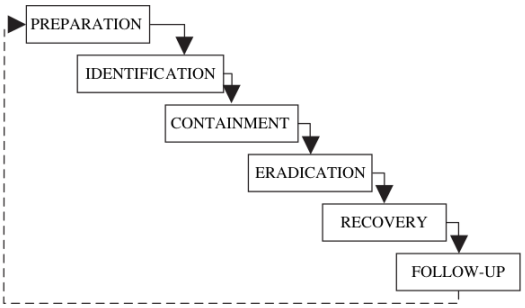
Berdasarkan surat keputusan Kepala Dinas Komunikasi Informatika dan Statistik Povinsi DKI Jakarta Nomor 59 Tahun 2020 tentang Penjabaran Keputusan Sekretaris Daerah mengenai Computer Security Incident Response Team yang mempunyai susunan, pelaksanaan, evaluasi dan pelaporan kendali operasi keamanan siber di lingkungan pemerintah provinsi DKI Jakarta. Salah satu kegiatan dalam melaksanakan tugas tersebut yaitu menyelenggarakan fungsi sebagai Pusat Kontak Siber.

Prosedur Aduan Siber

Gambar 2.Prosedur Aduan Siber (Jakarta Prov CSIRT, n.d.)

1. Penerimaan aduan insiden siber dapat melalui telepon dan whatsapp di nomor +62 813-8887-0152, melalui web https://soc.jakarta.go.id atau surel ke alamat it-security@jakarta.go.id.
2. Jika melalui aplikasi ATIKA, setelah registrasi dengan menggunakan NRK dan telah terverifikasi, maka pemohon dapat membuat aduan/laporan insiden.
3. Pemohon mengisi formulir dengan dilengkapi screenshot kejadian.
4. Informasi status laporan ada dalam daftar pengajuan insiden dan akan segera ditindak lanjuti oleh team Bidang Siber & Sandi.

Tahapan dalam penanganan insiden keamanan informasi :



Gambar 3. Metodologi Model Penanganan Insiden (Mitropoulos et al., 2006)

Fakta bahwa hingga saat ini secara *de jure* di seluruh dunia tidak ada standar *Incident Response* yang lengkap, baik sebagai dokumen khusus atau sebagai bagian dari standar keamanan informasi sebuah organisasi. Seseorang dapat menemukan teknik tertentu yang dirancang secara khusus untuk kasus tertentu. Sebagian besar metodologi *Incident Response* sangat dikombinasikan dengan ilmu forensik digital, yaitu proses penggalian data nilai pembuktian dari komputer dan sistem informasi(Prosise & Mandia, 2001).

Forensik mencakup tindakan yang diperlukan untuk melacak kembali insiden keamanan ke sumber sebenarnya dan dalam banyak kasus, *physical persons* yang menyebabkan insiden tersebut. Forensik membutuhkan pemahaman yang kuat tentang protokol jaringan dan sistem operasi dan menuntut tidak hanya kesabaran tingkat tinggi tetapi juga kemampuan untuk mengikuti aturan dan prosedur yang terkait dengan hukum. Meskipun bidang forensik telah berkembang dan telah matang di Lembaga Penegakan Hukum dan bukan di dunia

penelitian akademis, tampaknya praktik dan metodologi terbaik dapat berhasil ditransfer ke domain Incident Response(Yasinsac & Manzano, 2001).

Untuk menggabungkan tindakan yang tepat secara efisien dan efektif ketika sebuah insiden terjadi, metodologi yang paling dikenal dan mencakup beberapa bagian yang berbeda, sebuah contoh rekomendasi dan praktik terbaik dari metodologi ditunjukkan pada Gambar. 3, berdasarkan fase yang diusulkan di Institut Nasional Standar dan Teknologi (2004), pada tindakan yang mutlak diperlukan yang harus diambil dalam setiap fase, tanpa exhausting all possible options dan solusi alternatif(Paul Cichonski, Tom Millar, Tim Grance, 2012).

Beberapa fase tersebut antara lain:

Fase *Preparation*

Mempertimbangkan bahwa mekanisme keamanan yang diperlukan sudah ada baik di gateway perusahaan (firewall, perangkat lunak antivirus, mekanisme otentikasi yang kuat, dan lain-lain), dan di bagian internal yang kritis (Host dan Sistem Deteksi Intrusi Berbasis Jaringan (IDS)), perangkat lunak khusus tambahan dan perangkat keras harus diinstal juga (misalnya sniffer, perangkat lunak konsolidasi log audit, perangkat lunak cadangan, dan lain-lain). Dalam fase *preparation*, secara umum meliputi beberapa tahapan :

Gambar 4. Fase Preparation (Nur Dwi Muryanto, 2019)

Tujuan fase *preparation* adalah untuk membangun komunikasi dan mempersiapkan sumber daya yang dibutuhkan pada saat penanganan insiden. Dalam fase preparation ada beberapa tahapan yang dapat dilakukan, diantaranya:

1. Pembentukan tim penanganan insiden. Tim dapat berasal dari internal Bidang Siber dan Sandi atau bisa juga dari luar institusi (eksternal) yaitu melibatkan personil teknis dari vendor jika memang sangat diperlukan.
2. Mempersiapkan dokumen yang dibutuhkan dalam penanganan insiden. Dokumen ini antara lain:
   - *Standar Operation Procedure (SOP);*
   - Form-form yang akan digunakan, form penanganan insiden, form chain of custody;
   - Gambar diagram terbaru yang menggambarkan topologi jaringan, hubungan antar komponen-komponen aplikasi yang membangun satu sistem seperti website aplikasi (*web server*, *database server*, *framework* aplikasi)
   - Dokumentasi dari sistem operasi, aplikasi, protokol yang digunakan, konfigurasi firewall dan antivirus yang terdapat pada sistem server, dokumen berisi daftar ip yang diprioritaskan untuk diperbolehkan melewati jaringan selama penanganan dan dokumen *baseline performance*
3. Lakukan koordinasi insiden dengan tim terkait yang dapat menangani secara teknis, koordinasi dengan tim CSIRT ataupun Point of Contact untuk mendapatkan infomasi tambahan dalam penanganan insiden. Membangun kontak dengan pengelola *Internet Service Provider (ISP)*, dan menentukan metode koordinasi dan komunikasi antar tim, kapan koordinasi harus dilakukan dan mellaui media komunikasi apa yang akan digunakan, misalkan menggunakan telepon, email atau melalui aplikasi

messaging seperti WhatsApp, telegram atau lainnya.

4. Pengumpulan bukti insiden antara lain berupa tangkapan layar *(screenshot)* atau berupa photo insiden, log server atupun log perangkat pendukung server. Atau jika menemukan file yang mencurigakan dapat dilakukan pendokumentasian file tersebut. Untuk kegiatan forensic dapat juga dilakukan proses imaging baik seluruh storage server ataupun memori (RAM) yang digunakan.
5. Menentukan tempat (ruangan) untuk menangani insiden baik kegiatan rapat maupun kegiatan analisis insiden. Serta menyiapkan tools dan media yang dibutuhkan untuk menangani insiden. Tools yang dapat disiapkan antara lain *scanning tools, forensic tools* dan *monitoring tools*, media yang dapat digunakan berupa *storage external.* Selain itu sebaiknya disiapkan juga *static view* untuk *landing page* kalau sistem *under maintenance*. (Ryan, 2015)

Fase *Identification*

Tahap identifikasi sangat penting. Tahap ini dapat mengidentifikasi titik awal dari suatu peristiwa dan ini adalah tahap ketika keputusan kritis harus dibuat untuk mengkategorikan suatu peristiwa dan merespon sesuai. Jika prosedur gagal dalam tahap ini, seluruh metodologi mungkin runtuh dan tidak ada gunanya.

Awal pengumpulan bukti harus dimulai segera setelah identifikasi atau bahkan kecurigaan suatu kejadian. Keputusan, meskipun, apakah aktivitas abnormal sesuai dengan serangan yang sebenarnya atau pola serangan cukup rumit. Teknologi menawarkan bantuan melalui berbagai metode melalui Intrusion Detection dan (Near) Sistem Manajemen Ancaman Real Time yang memerlukan penyebaran luas ke jaringan perusahaan. Harus disebutkan bahwa dalam kebanyakan kasus itu adalah faktor manusia yang memiliki pengetahuan tentang apa terdiri dari aktivitas abnormal dalam lingkungan perusahaan tertentu.

Dua pendekatan utama mengenai insiden jaringan tergantung pada tingkat keparahannya dapat diidentifikasi:

1. Segera tutup titik masuk penyerang dan hilangkan semua sarana akses yang memungkinkan, atau;
2. Tetap 'terbuka', selama mungkin, dan kumpulkan informasi sebanyak-banyaknya untuk digunakan nanti sebagai bukti.

Sangat penting untuk mendapatkan informasi yang cukup tentang serangan sehingga tim respon dapat memprioritaskan langkah selanjutnya dalam menangani insident tersebut. Kemampuan untuk mengidentifikasi dan memahami sifat dari serangan dan target akan membantu dalam proses *containment* dan pemulihan. Langkah-langkah yang dapat diambil pada fase *identification* antara lain:

a. Mengetahui perilaku “normal” dari lalu lintas jaringan, penggunaan CPU, penggunaan memori dari host, sehingga alat monitoring jaringan akan memberikan informasi berupa peningkatan terhadap perubahan abnormal. Beberapa indikasi telah terjadi serangan diantaranya :
   - Melambatnya lalu lintas jaringan
   - Melambatnya proses pada komputer *host*
   - Penggunaan ruang disk yang bertambah
   - Layanan tidak dapat diakses atau sistem *crash*
   - Waktu login yang lama bahkan ditolak
   - Log penuh
   - Anomali pada fungsi port
b. Mengidentifikasi komponen infrastruktur yang terkena dampak dan keparahan insiden *(impact and severity of impact)*
c. Berkoordinasi dengan pihak terkait untuk mengetahui apakah jaringan organisasi merupakan target utama atau korban dari imbas (misalnya

imbas dari serangan terhadap penyedia layanan internet.

d. Memeriksa lalu lintas jaringan seperti source *IP address, destinantion port, urls, protocol, tcp sync, udp, icmp dan traffic netflow* misalnya menggunakan tcpdump, wireshark, snort dan membandingkan dengan lalu lintas jaringan "normal". Dengan memeriksa lalu lintas jaringan, juga dapat diketahui sumber dan jenis serangan.
e. Menganalisa file log yang tersedia (file log server, router, firewall, aplikasi dan infrastruktur lainnya yag terkena dampak) untuk mengetahui jenis serangan, sumber serangan, apa yang menjadi sasaran, serta kemungkinan motif yang dilakukan oleh penyerang.(Ryan, 2015)

Fase Containment

Langkah selanjutnya adalah menerapkan solusi segera, sehingga membatasi tingkat insiden dan membiarkan penghapusan lengkap akses penyusup dan identifikasi kemungkinan perubahan Penyerang biasanya meninggalkan program *backdoor* atau *Trojan horse* untuk dapat memperoleh akses di lain waktu. Untuk mengecek validitas file perlu dilakukan perbandingan file sistem kritis dengan *checksum* kriptografi. Perbandingan ini menjamin bahwa tidak ada modifikasi yang dilakukan selama insiden tersebut. Jika waktu memungkinkan dan jika *checksum* kriptografi dicatat selama fase persiapan, perbandingan yang sama harus dilakukan mengenai data. Meskipun ini bukan praktik umum, ini dapat memberikan informasi yang berguna.

Fase *containment* bertujuan untuk meminimalisir efek/dampak serangan pada system yang ditargetkan dan mencegah kerusakan lebih lanjut. Prosedur yang dapat dilakukan pada tahap ini adalah:

a. Jika sumber bottleneck berada pada fitur tertentu dari suatu aplikasi (dalam artian suatu aplikasi sedang menjadi target), maka perlu mempertimbangkan untuk menonaktifkan *(takedown)* sementara aplikasi tersebut.
b. Jika bottlenecknya berada di ISP, maka perlu berkoordinasi dengan pihak ISP untuk meminta filtering.
c. Merelokasi target ke alamat ip lain jika suatu host tertentu sedang menjadi target (sebagai solusi sementara).
d. Jika memungkinkan, memblokir lalu lintas yang terhubung dengan jaringan (router, firewall, load balancer, dan perangkat lainnya).
e. Mengontrol lalu lintas data dengan menghentikan koneksi atu proses yang tidak diinginkan pada server atau router.
f. Melakukan filter sesuai karkterisktik serangan, misalnya memblokir paket echo icmp.
g. Menerapkan rate limiting untuk protocol tertentu, mengijinkan dan membatasi jumlah paket per detik untuk protocol tertentu dalam mengakses suatu host.
h. Jika sudah dipastikan serangan berupa phising, maka mitigasi serangan perlu dilakukan agar tidak terjadi kerusakan lebih dalam, misalnya menyebarkan url phising dan konten email pada pihak spam-reporting website misalnya ke phishtank.com
i. Menginformasikan serangan kepada pengguna lainnya agar pengguna mengetahui dan tidak terkena dampak serangan.(Ryan, 2015)

Fase Eradication

Tahap ini mengacu pada solusi jangka menengah dan jangka panjang yang harus diterapkan pada sistem yang terpengaruh untuk menghilangkan segala cara yang mungkin untuk terulangnya serangan tertentu. Kemungkinan penanggulangan pada tahap ini termasuk pemeriksaan kepatuhan kebijakan, audit keamanan independen, pembaruan

kebijakan, dan lain-lain. Tahap ini dilakukan :

a. Hapus *malicious content* (termasuk konten *deface*).
b. Hapus aplikasi mencurigakan
c. Jalankan service yang diperlukan saja
d. Patching keamanan aplikasi web
e. Periksa dan hapus *backdoor*
f. Lakukan *vulnerability assessment*
g. Pemblokiran jaringan *(source ip address)*
h. Pemfilteran (membatasi jumlah lalu lintas)
i. Traffict-schrubbing, shinkchole, clean pipe dan blackhole routing.(Ryan, 2015)

Fase Recovery

Pemulihan merupakan tahap untuk mengembalikan seluruh sistem bekerja normal seperti semula. Setelah semua langkah sebelumnya berhasil diikuti, pemulihan sistem dan peningkatan mekanisme keamanan harus dimulai untuk mengembalikan seluruh sistem ke produksi tanpa ada celah keamanan yang terbuka. Contohnya termasuk pembangunan kembali sistem yang lengkap, pemulihan data dari media backup, pemasangan mekanisme keamanan ekstra, dan lain-lain. Sebelum memasukkan sistem yang disusupi ke dalam produksi lagi, disarankan untuk menjalankan penilaian kerentanan atau uji penetrasi untuk mengungkapkan kemungkinan kerentanan yang ada. Secara singkat tahap ini bertujuan untuk mengembalikan ke keadaan semula.

Memahami karakteristik serangan diperlukan untuk pemulihan yang cepat dan tepat. Prosedur yang dapat dilakukan pada tahap pemulihan diantaranya sebagai berikut:

a. Memastikan bahwa serangan yang terjadi sudah ditangani dan layanan bias dilakukan kembali.
b. Memastikan sistem atau jaringan yang terdampak telah kembali ke kinerja semula
c. Memastikan bahwa layanan yang terkena dampak dapat dijangkau kembali atau sudah beroperasi kembali.
d. Memastikan bahwa infrastruktur telah kembali ke kinerja semula (tidak ada kerusakan).
e. Memulai layanan, aplikasi dan modul yang ditangguhkan.
f. Mengembalikan ke jaringan asli dan mengalihkan kemali lalu lintas ke jaringan asli.
g. Lakukan update/upgrade/patch semua aplikasi yang digunakan pada web server. Jika menggunakan CMS, lakukan update versi, plugins, themes yang digunakan, selain itu perlu dilakukan update rules pada konfigurasi keamanan yang digunakan.
h. Lakukan automatic update pda setiap aplikasi yang digunakan
i. Lakukan pembaruan seluruh akun yang digunakan baik pada system operasi maupun aplikasi.
j. Lakukan hardening server ataupun aplikasi yang digunakan seperti mereview *Web Application Firewall (WAF),* memasang aplikasi *anti-defacement (DotDefender, Nagios, Webgaurd)*(Ryan, 2015)

Fase Follow Up

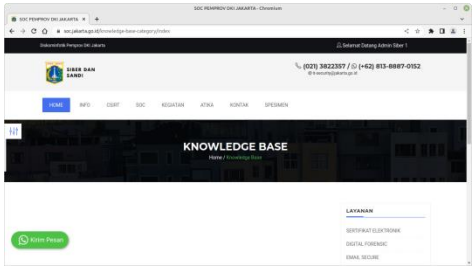
Semua tindakan dan informasi mengenai insiden tersebut harus didokumentasikan dan *electronic evidence* harus *disseminated* untuk analisis secara forensic. Selanjutnya, *post-mortem meeting* dengan manajemen harus dilakukan untuk menilai kerusakan yang terjadi, kekuatan dan kelemahan kebijakan dan prosedur yang harus diikuti. Akibat dari suatu insiden dapat mengindikasikan atau bahkan mengharuskan kebijakan, prosedur, dan pedoman keamanan harus diperbarui agar dapat mengatasi serangan sejenis di masa mendatang. Setelah analisis lengkap insiden dilakukan,

perubahan konfigurasi sistem harus didokumentasikan dan inventaris sistem dan aset jaringan harus diperbarui untuk mencerminkan perubahan ini.
Tahap ini adalah fase dimana semua dokumentasi yang dilakukan dicatat sebagai referensi untuk dimasa mendatang. Tujuan dari tahap ini adalah untuk:

a. Membuat laporan mengenai langkah-langkah dan hasil yang telah didapatkan pada penanganan insiden.
b. Mengambil pelajaran dan membuat rekomendasi untuk mencegah terulangnya insden serupa dimasa mendatang.
c. Evaluasi efektifitas respon
d. Menyempurnakan langkah-langkah respon penanganan serangan yang diambil selama insiden.
e. Mendokumentasikan bukti-bukti yang ditemukan, hal ini terkait dengan proses hokum kedepannya.
f. Memberikan analisa dan penjelasan apa yang harus dilakukan sehingga serangan serupa tidak terulang kembali.
g. Membuat evaluasi dan rekomendasi

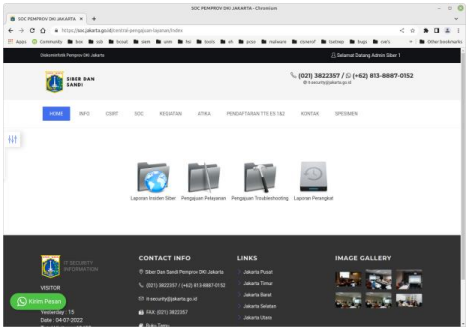
Secara singkat tahap ini bertujuan untuk :
- *Lesson learned*
- Laporan akhir
- Bukti arsip dan dokumentasi
- Menutup proses penanganan insiden(Ryan, 2015)

Pengelolaan pengetahuan mengubah *tacit knowledge* menjadi *explicit knowledge* dan didokumentasikan dalam bentuk *standard operation procedure* dan dapat dakses oleh seluruh user, seperti terlihat dalam gambar berikut.



Gambar 5. Aplikasi *knowledge* manajemen berbasis web

Pada menu *knowledge base* tedapat beberapa kategori diantaranya *email secure, security operation cente, digital forensic, incident response beserta* kategori *knowledge lainnya*

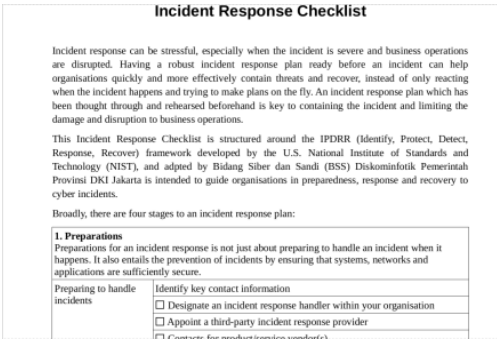


Gambar 6. Aplikasi laporan insiden siber berbasis web

Rencana respons insiden adalah seperangkat alat dan prosedur yang dapat digunakan tim keamanan Anda untuk mengidentifikasi, menghilangkan, dan memulihkan dari ancaman keamanan siber. Ini dirancang untuk membantu tim merespons dengan cepat dan seragam terhadap segala jenis ancaman eksternal.

Respons insiden dapat membuat stres, terutama ketika insiden itu parah dan operasi bisnis terganggu. Memiliki rencana respons insiden yang kuat yang siap sebelum insiden dapat membantu organisasi dengan cepat dan lebih efektif mengatasi ancaman dan memulihkannya, daripada hanya bereaksi ketika insiden terjadi dan mencoba membuat rencana dengan cepat. Rencana respons insiden yang telah dipikirkan dan dilatih

sebelumnya adalah kunci untuk menahan insiden dan membatasi kerusakan dan gangguan pada operasi bisnis. Daftar Periksa Tanggapan Insiden ini disusun berdasarkan kerangka kerja IPDRR *(Identify, Protect, Detect, Response, Recover)* yang dikembangkan oleh Institut Standar dan Teknologi Nasional AS (NIST), dan dimaksudkan untuk memandu organisasi dalam kesiapsiagaan, respons, dan pemulihan terhadap insiden dunia maya.



Incident Response Checklist

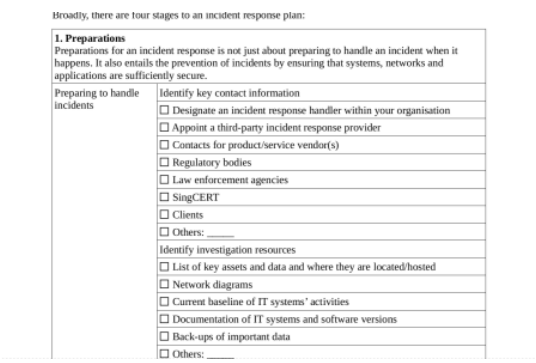
Incident response can be stressful, especially when the incident is severe and business operations are disrupted. Having a robust incident response plan ready before an incident can help organisations quickly and more effectively contain threats and recover, instead of only reacting when the incident happens and trying to make plans on the fly. An incident response plan which has been thought through and rehearsed beforehand is key to containing the incident and limiting the damage and disruption to business operations.

This Incident Response Checklist is structured around the IPDRR (Identify, Protect, Detect, Response, Recover) framework developed by the U.S. National Institute of Standards and Technology (NIST), and adpted by Bidang Siber dan Sandi (BSS) Diskominfotik Pemerintah Provinsi DKI Jakarta is intended to guide organisations in preparedness, response and recovery to cyber incidents.

Broadly, there are four stages to an incident response plan:

1. Preparations Preparations for an incident response is not just about preparing to handle an incident when it happens. It also entails the prevention of incidents by ensuring that systems, networks and applications are sufficiently secure.	
Preparing to handle incidents	Identify key contact information
	☐ Designate an incident response handler within your organisation
	☐ Appoint a third-party incident response provider
	☐ Contacts for product/service vendor(s)

Gambar 7.1 Daftar periksa tanggap insiden



Broadly, there are four stages to an incident response plan:

1. Preparations Preparations for an incident response is not just about preparing to handle an incident when it happens. It also entails the prevention of incidents by ensuring that systems, networks and applications are sufficiently secure.	
Preparing to handle incidents	Identify key contact information
	☐ Designate an incident response handler within your organisation
	☐ Appoint a third-party incident response provider
	☐ Contacts for product/service vendor(s)
	☐ Regulatory bodies
	☐ Law enforcement agencies
	☐ SingCERT
	☐ Clients
	☐ Others: _____
	Identify investigation resources
	☐ List of key assets and data and where they are located/hosted
	☐ Network diagrams
	☐ Current baseline of IT systems' activities
	☐ Documentation of IT systems and software versions
	☐ Back-ups of important data
	☐ Others: _____

Gambar 7.2 Daftar periksa tanggap insiden

Memiliki rencana tanggap insiden yang kuat yang siap sebelum insiden dapat membantu organisasi dengan cepat dan lebih efektif mengatasi ancaman dan pulih, alih-alih hanya bereaksi ketika insiden terjadi dan mencoba membuat rencana dengan cepat. Rencana tanggap insiden yang telah dipikirkan dan dilatih sebelumnya adalah kunci untuk menahan insiden dan membatasi kerusakan dan gangguan pada operasi bisnis.

SIMPULAN DAN SARAN

Pengelolaan pengetahuan penanganan insiden keamanan informasi membantu Bidang Siber dan Sandi Dinas Komunikasi Informatika dan Statistik DKI Jakarta dalam peningkatan efisiensi cara kerja dan proses, dimana organisasi dapat mengelola setiap pengetahuan dari tenaga ahli atau sumber daya yang lain untuk meningkatkan efisiensi organisasi. Daftar periksa *Insiden Response* dapat memandu organisasi dalam kesiapsiagaan, tanggap, dan pemulihan pasca insiden.

Untuk pengembangan manajemen pengetahuan dalam menangani insiden keamanan informasi perlu dibuatkan buku pedoman perencanaan penanganan insiden atau Incident Response Plan Playbook yang disusun berdasarkan prosedur dan langkah standar untuk merespon dan menyelesaikan insiden secara realtime. Buku pedoman juga harus mencakup *peacetime training*, dan pelatihan untuk mempersiapkan tim untuk insiden berikutnya.

Perencanaan penanganan insiden menjadi sangat penting karena dapat menguraikan cara meminimalkan durasi dan kerusakan insiden keamanan, mengidentifikasi pemangku kepentingan, merampingkan forensik digital, meningkatkan waktu pemulihan, mengurangi publisitas negatif, dan churn pelanggan. Bahkan insiden keamanan siber kecil, seperti infeksi malware, dapat menjadi masalah yang lebih besar yang pada akhirnya menyebabkan pelanggaran data, kehilangan data, dan operasi bisnis yang terganggu.

UCAPAN TERIMA KASIH

Terima kasih kepada seluruh jajaran di Dinas Komunikasi, Informatika dan Statistik Pemerintah Provinsi DKI Jakarta.

DAFTAR PUSTAKA

Andrie Yuswanto, B. W. (2020). *Pembangunan Pusat Pengendalian Operasional Keamanan Informasi (Pusdalops Kami) guna Meningkatkan Pelayanan E-Gov dari Ancaman Kejahatan Siber*.

Ashenden, D. (2008). Information Security

management: A human challenge? *Information Security Technical Report*, *13*(4), 195–201. https://doi.org/10.1016/j.istr.2008.10.006

Bidang Siber dan Sandi DKI. (2021). *BIDANG SIBER & SANDI*. https://diskominfotik.jakarta.go.id/bidang-siber-sandi

CSIRT, J. P. (2021). *Jakarta Prov CSIRT*. https://csirt.jakarta.go.id/profile

Dey, M. (2007). Information security management - A practical approach. *IEEE AFRICON Conference*, 7–12. https://doi.org/10.1109/AFRCON.2007.4401528

Halim, M. A., Abdullah, A., & Ariffin, K. A. Z. (2019). Recurrent neural network for malware detection. *International Journal of Advances in Soft Computing and Its Applications*, *11*(1), 46–63.

Jakarta Prov CSIRT. (n.d.). *Jakarta Prov CSIRT*. Retrieved July 4, 2022, from https://csirt.jakarta.go.id/info-grafis

Kusuma, E. A., Widiarto, H., & Efendi, D. (2021). The Role of Knowledge Management and Sustainable Competitive advantage. *Intergrated Journal of Business and Economics*, 47–60.

Majid, M., & Ariffi, K. (2019). *Success Factors for Cyber Security Operation Center (SOC) Establishment*. https://doi.org/10.4108/eai.18-7-2019.2287841

Mariki Eloff, & Jan Eloff. (2003). Information security management: a new paradigm. *Information Security Management – A New Paradigm*, 130–136. http://dl.acm.org/citation.cfm?id=954014.954028

Mitropoulos, S., Patsos, D., & Douligeris, C. (2006). On Incident Handling and Response: A state-of-the-art approach. *Computers and Security*, *25*(5), 351–370. https://doi.org/10.1016/j.cose.2005.09.006

Novian Nur Cahya, D., & Operasi Keamanan Siber. (2022). *Novian Nur Cahya , S . S . T ., M . Kom . Sandiman Muda* (Issue April). https://csirt.kemhan.go.id/assets/event/April---Incident-Response.pdf

Nur Dwi Muryanto, S. P. B. (2019). *Penanganan Insiden Keamanan Informasi*, *DIREKTORAT PENANGGULANGAN DAN PEMULIHAN PEMERINTAH BADAN SIBER DAN SANDI NEGARA*.

Paul Cichonski, Tom Millar, Tim Grance, K. S. (2012). Computer Security Incident Handling Guide : Recommendations of the National Institute of Standards and Technology. *NIST Special Publication*, *800–61*, 79. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Pham, H. C., Ulhaq, I., Nguyen, M. N., & Nkhoma, M. (2021). An Exploratory Study of the Effects of Knowledge Sharing Methods on Cyber Security Practice. *Australasian Journal of Information Systems*, *25*(2017), 1–23. https://doi.org/10.3127/ajis.v25i0.2177

Prosise, C., & Mandia, K. (2001). *Incident response: investigating computer crime* (p. 509).

Ryan, J. J. C. H. (2015). Review of: Computer Incident Response and Forensics Team Management: Conducting a Successful Incident Response . In *Journal of Forensic Sciences* (Vol. 60, Issue 1). https://doi.org/10.1111/1556-4029.12646

Safa, N. S., & Von Solms, R. (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57*(February 2016), 442–451. https://doi.org/10.1016/j.chb.2015.12.037

Saif, M. R., & Yeop, N. K. Bin. (2020). Measuring the Organizational Performance in the Government Departments of Dubai Using the Knowledge Management Process. *European Journal of Social Science Education and Research*, *7*(1), 33. https://doi.org/10.26417/ejser.v7i1.p33-40

Sindiren, E., & Ciylan, B. (2018). Privileged Account Management Approach for Preventing Insider Attacks. *International Journal of Computer Science and Network Security*, *18*(1), 33–42.

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy

compliance: A systematic review of quantitative studies. *Information Management and Computer Security*, *22*(1), 42–75. https://doi.org/10.1108/IMCS-08-2012-0045

Yasinsac, A., & Manzano, Y. (2001). Policies to Enhance Computer and Network Forensics. *Proceedings of the 2001 IEEE*, 5–6.