PEDOMAN PENANGANAN INSIDEN SIBER

COMPUTER SECURITY INCIDENT RESPONSE TEAM

(MAGELANGKAB-CSIRT)

DINAS KOMUNIKASI DAN INFORMATIKA
KABUPATEN MAGELANG
2024

KATA PENGANTAR

Puji dan syukur kita panjatkan ke hadirat Tuhan Yang Maha Esa, atas rahmat dan karunia-Nya sehingga penyusunan Pedoman Penanganan Insiden Siber ini dapat diselesaikan. Di era digital saat ini, kemajuan teknologi informasi telah mengubah cara kita berinteraksi, bekerja, dan memberikan pelayanan kepada masyarakat. Namun demikian kemajuan ini juga disertai dengan tantangan besar dalam bentuk ancaman siber yang semakin kompleks dan beragam.

Sebagai bagian dari upaya menjaga integritas, kerahasiaan, dan ketersediaan informasi di lingkungan Pemerintah Kabupaten Magelang, pedoman ini disusun sebagai acuan resmi dalam penanganan insiden siber. Pedoman ini diharapkan dapat membantu setiap Perangkat Daerah dalam memahami langkah-langkah preventif serta responsif dalam menghadapi insiden siber.

Ucapan terima kasih kami sampaikan kepada seluruh pihak yang telah membantu dalam penyusunan Pedoman ini.

Magelang, Desember 2024

Ditandatangani secara elektronik oleh:

KEPALA DINAS KOMUNIKASI DAN INFORMATIKA
KABUPATEN MAGELANG

BUDI DARYANTO, S.STP., M.SI
Pembina Tingkat I
NIP. 19800501 199912 1 001

DAFTAR ISI

BAB I
PENDAHULUAN

A. LATAR BELAKANG

Kemajuan teknologi informasi dan komunikasi (TIK) telah membawa perubahan besar pada Pemerintah Kabupaten Magelang melalui Sistem Pemerintahan Berbasis Elektronik (SPBE). Sistem Pemerintahan Berbasis Elektronik telah banyak membawa manfaat dalam menyelenggarakan pelayanan publik dan menjalankan tata kelola pemerintahan. Selain itu dengan adanya SPBE mempermudah akses informasi dan layanan yang efisien bagi masyarakat. Namun demikian di balik manfaat yang ditawarkan oleh teknologi ini terdapat pula ancaman keamanan yang semakin komplek yaitu potensi serangan dan insiden siber.

Insiden siber yang mencakup berbagai bentuk serangan digital seperti peretasan, *Malware*, serangan *Denial of Service* (DoS), dan pencurian data berpotensi mengganggu kelangsungan operasional pemerintahan dan merugikan masyarakat. Oleh karena itu untuk memitigasi dampak dari ancaman keamanan informasi tersebut Pemerintah Kabupaten Magelang telah membentuk Tim Tanggap Insiden Siber atau *Computer Security Incident Response Team* (CSIRT) yang diberi nama MagelangKab-CSIRT.

MagelangKab-CSIRT beranggotakan personil pada Dinas Komunikasi dan Informatika serta perwakilan dari Perangkat Daerah di lingkungan Pemerintah Kabupaten Magelang. Dalam pelaksanaan penanganan insiden siber diperlukan panduan yang komprehensif bagi seluruh anggota Magelangkab-CSIRT dalam menangani dan merespons insiden siber. Oleh karena itu Tim Keamanan Informasi MagelangKab-CSIRT menyusun Pedoman Penanganan Insiden Siber Kabupaten Magelang yang dapat dijadikan sebagai rujukan bagi personil yang tergabung dalam MagelangKab-CSIRT dalam penanganan insiden siber.

B. DASAR HUKUM

1. Peraturan Pemerintah Nomor 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik;
2. Peraturan Presiden Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik;
3. Peraturan Badan Siber dan Sandi Negara Nomor 8 Tahun 2020 tentang Sistem Pengamanan Dalam Penyelenggaraan Sistem Elektronik;
4. Peraturan Badan Siber dan Sandi Negara Nomor 10 Tahun 2020 tentang Tim Tanggap Insiden Siber;
5. Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi Sistem Pemerintahan Berbasis Elektronik dan Standar Teknis dan Prosedur Keamanan Sistem Pemerintahan Berbasis Elekronik;
6. Peraturan Bupati Magelang Nomor 26 Tahun 2021 tentang Sistem Pemerintahan Berbasis Elektronik di Lingkungan Kabupaten Magelang;
7. Peraturan Badan Siber Dan Sandi Negara Nomor 1 Tahun 2024 Tentang Pengelolaan Insiden Siber;
8. Peraturan Bupati Magelang Nomor 69 Tahun 2023 tentang Tentang Kedudukan, Susunan Organisasi, Tugas dan Fungsi, serta Tata Kerja Dinas Komunikasi dan Informatika Kabupaten Magelang;
9. Surat Keputusan Bupati Magelang nomor: 180.182/90/KEP/15/2023 tanggal 14 April 2023 tentang Tim Tanggap Insiden Siber (*Computer Security Incident Response Team*) Kabupaten Magelang (MagelangKab-CSIRT);
10. Surat Tanda Registrasi Badan Siber dan Sandi Negara Nomor 355/CSIRT.01.02.01/BSSN/04/2024 tentang Registrasi Tim Tanggap Insiden Siber Kabupaten Magelang (MagelangKab-CSIRT);

C. RUANG LINGKUP

Pedoman Penanganan Insiden Siber Kabupaten Magelang ini berisi tata kelola dan kebijakan terkait penanganan insiden siber secara umum dan prosedur penanganan insiden yaitu langkah-langkah yang harus diambil apabila terjadi insiden siber berupa *Web Defacement*, *Phising, Malware* dan *Ransomware.* Langkah-langkah penanganan pada masing-masing insiden

dimulai dari tahap persiapan sampai dengan tahap pembuatan laporan penanganan insiden. Pedoman ini menjadi acuan bagi individual atau tim (administrator, pengelola TI, dan tim respon insiden keamanan siber) yang bertanggung jawab untuk mencegah, mempersiapkan, atau menanggapi insiden siber di lingkungan Pemerintah Kabupaten Magealang.

D. DEFINISI

1. Insiden Siber adalah satu atau serangkaian kejadian yang mengganggu atau mengancam berjalannya Sistem Elektronik.
2. Sistem Elektronik adalah serangkaian perangkat dan prosedur elektronik yang berfungsi mempersiapkan, mengumpulkan, mengolah, menganalisis, menyimpan, menampilkan, mengumumkan, mengirimkan, dan/atau menyebarkan informasi elektronik.
3. MagelangKab-CSIRT adalah sekelompok orang yang bertanggungjawab menangani Insiden Siber di lingkungan Pemerintah Kabupaten Magelang sesuai dengan Keputusan Bupati Magelang nomor 180.182/90/KEP/15/2023 tanggal 14 April 2023 tentang Tim Tanggap Insiden Siber (*Computer Security Incident Response Team*) Kabupaten Magelang (MagelangKab-CSIRT).
4. Tim Keamanan Informasi selanjutnya disebut Koordinator Insiden adalah sekelompok orang pada Bidang Statistik dan Persandian yang bertugas melaksanakan *helpdesk*, identifikasi, investigasi dan koordinasi penanganan Insiden Siber dan memberikan rekomendasi solusi Insiden Siber yang terjadi.
5. Perangkat Daerah adalah unsur pembantu Bupati dan Dewan Perwakilan Rakyat Daerah dalam penyelenggaraan urusan pemerintahan yang menjadi kewenangan daerah.
6. Agen Siber yang selanjutnya disebut Agen adalah personil pada Perangkat Daerah yang bertugas melakukan monitoring keamanan informasi Perangkat Daerah.
7. Sistem Manajemen Keamanan Informasi yang selanjutnya disingkat SMKI adalah sistem manajemen yang meliputi kebijakan, organisasi, perencanaan, penanggung jawab, proses, dan sumber daya yang mengacu pada pendekatan risiko bisnis untuk menetapkan, mengimplementasikan, mengoperasikan, memonitoring, mengevaluasi, mengelola, dan

meningkatkan keamanan informasi.

8. Sistem Pemerintahan Berbasis Elektronik yang selanjutnya disingkat SPBE adalah penyelenggaraan pemerintahan yang memanfaatkan teknologi informasi dan komunikasi untuk memberikan layanan kepada pengguna SPBE.

BAB II
KEBIJAKAN UMUM KEAMANAN SIBER

A. PENERAPAN KONTROL KEAMANAN SIBER

Penerapan kontrol keamanan siber adalah langkah-langkah teknis, administratif, dan operasional yang diterapkan untuk melindungi sistem informasi dan data dari ancaman siber, serta untuk meminimalkan risiko insiden. Tujuan utamanya adalah memastikan keamanan, kerahasiaan, integritas, dan ketersediaan informasi yang dikelola oleh Perangkat Daerah di lingkungan Pemerintah Kabupaten Magelang. Kebijakan penerapan kontrol keamanan siber meliputi:

1. Perangkat Daerah wajib menerapkan standar keamanan sesuai dengan standar SMKI dan standar keamanan SPBE sebagaimana diatur dalam peraturan perundang-undangan.
2. Dalam penerapan standar keamanan serta untuk mendukung penyediaan informasi awal dalam penanganan Insiden Siber, Perangkat Daerah melakukan:
   a. Kategorisasi Sistem Elektronik yang dikelola oleh Perangkat Daerah;
   b. Menyusun daftar aset berupa sumber daya manusia (SDM), perangkat keras, perangkat lunak termasuk lisensi, informasi yang dikelola dalam Sistem Elektornik, kebijakan dan prosedur, serta pihak ketiga yang terlibat dalam pengelolaan Sistem Elektronik; dan
   c. Menyusun daftar risiko keamanan informasi dari daftar aset.
3. Dalam hal Perangkat Daerah mengalami kendala dalam penerapan standar keamanan, maka Bidang Statistik dan Persandian Dinas Komunikasi dan Informatika Kabupaten Magelang dapat memberikan asistensi dan pendampingan.

B. PENANGANAN INSIDEN KEAMANAN SIBER

Penanganan Insiden Keamanan Siber merupakan proses terstruktur untuk merespons, mengatasi, dan memulihkan sistem dari insiden siber guna meminimalkan dampaknya terhadap layanan publik dan data pemerintah. Proses

ini mencakup identifikasi insiden, pelaporan, analisis, mitigasi, hingga pemulihan, dengan koordinasi yang melibatkan Tim Tanggap Insiden Siber (CSIRT) Kabupaten Magelang dan pihak terkait seperti BSSN. Penanganan ini bertujuan untuk memastikan kesinambungan operasional, mengurangi risiko insiden berulang, dan meningkatkan kesiapan menghadapi ancaman siber di masa depan. Dalam kebijakan umum Penanganan Insiden Keamanan Siber terdapat kebijakan Penanganan Insiden Siber Oleh Perangkat Daerah, Penanganan Insiden Siber oleh Magelangkab-CSIRT, dan Kebijakan Penanganan Pasca Insiden Siber.

1. PENANGANAN INSIDEN SIBER OLEH PERANGKAT DAERAH

Kebijakan penanganan insiden siber oleh Perangkat Daerah merupakan langkah-langkah yang harus dilakukan oleh Perangkat Daerah dalam mencegah dan menangani insiden siber pada masing-masing Perangkat Daerah. Kebijakan penanganan insiden siber oleh Perangkat Daerah adalah:

a. Perangkat Daerah wajib untuk menunjuk personil sebagai Agen Siber.
b. Penunjukan Agen Siber ditetapkan dengan Surat Keputusan Bupati.
c. Agen bertugas:
    1). melakukan pemantauan lalu lintas jaringan di Perangkat Daerah dan memeriksa apabila terdapat anomali di jaringan;
    2). melakukan tindakan korektif pada jaringan dan server di Perangkat Daerah sebagai solusi atas insiden siber maupun temuan celah kerentanan;
    3). melakukan pemantauan terhadap aplikasi di Perangkat Daerah dan memeriksa apabila terdapat anomali di aplikasi;
    4). melakukan *backup* aplikasi, konfigurasi aplikasi dan database di Perangkat Daerah secara berkala;
    5). melakukan deteksi dan identifikasi serangan siber di Perangkat Daerah; dan
    6). melakukan edukasi dan Literasi di Lingkup Perangkat Daerah.
d. Pemantauan keamanan informasi dapat menggunakan sumber data yang diperoleh dari daftar risiko keamanan informasi, patroli siber,

pengujian keamanan secara mandiri terhadap infrastruktur maupun Sistem Elektronik milik Perangkat Daerah.

e. Apabila terjadi insiden siber, Agen Siber wajib melaporkan dan berkoordinasi dengan koordinator insiden.

f. Agen siber wajib menindaklanjuti hasil rekomendasi penanganan insiden dari koordinator insiden.

g. Prosedur penanganan Insiden Siber untuk internal Perangkat Daerah sekurang-kurangnya memuat:

   1). Alur penetapan Insiden Siber;

   2). Petunjuk teknis dari setiap Insiden Siber yang ditangani oleh Perangkat Daerah;

   3). Alur penyampaian Insiden Siber pada Perangkat Daerah yang penanganannya dikoordinir oleh Koordinator insiden; dan

   4). Pengakhiran masa Insiden Siber.

2. PENANGANAN INSIDEN SIBER OLEH MAGELANGKAB-CSIRT

Kebijakan penanganan insiden siber oleh Magelangkab-CSIRT merupakan kebijakan yang dilakukan oleh Tim Tanggap Insiden Siber Kabupaten Magelang dalam mengelola insiden keamanan siber secara cepat dan efektif yaitu:

a. Penanganan Insiden Siber oleh MagelangKab-CSIRT dikoordinir oleh Koordinator Insiden.

b. Insiden Siber yang ditangani oleh MagelangKab-CSIRT terdiri dari:

   1). Insiden Siber pada Perangkat Daerah yang dilaporkan oleh agen siber;

   2). Insiden Siber di lingkungan Pemerintah Kabupaten Magelang yang berdampak signifikan terhadap berjalannya administrasi pemerintahan dan dapat mengganggu kepentingan layanan publik.

c. Jenis Insiden Siber yang berdampak signifikan dan dapat mengganggu layanan publik disusun oleh Koordinator Insiden dan ditetapkan oleh Kepala Dinas Komunikasi dan Informatika selaku Ketua MagelangKab-CSIRT.

d. Dalam mendukung penanganan Insiden Siber, Koordinator Insiden menyusun prosedur penanganan Insiden Siber dan petunjuk teknis penanganan Insiden Siber sesuai dengan jenisnya.

e. Prosedur penanganan Insiden Siber sekurang-kurangnya memuat:

1). Petunjuk teknis pelaksanaan *helpdesk*;

2). Alur identifikasi jenis, sumber, dan informasi lainnya terkait Insiden Siber;

3). Alur koordinasi dan penyampaian penangananInsiden Siber yang melibatkan Agen Siber, dan tim penanganan insiden pada Dinas Komunikasi dan Informatika.

4). Alur pelibatan JatengProv-CSIRT dan *Government*–CSIRT di Badan Siber dan Sandi Negara maupun pihak lain yang sah atau resmi dalam penanganan Insiden Siber di lingkungan Pemerintah Kabupaten Magelang.

3. PENANGANAN PASCA INSIDEN SIBER

Kebijakan Penanganan Pasca Insiden Siber merupakan rangkaian langkah yang dilakukan setelah insiden siber berakhir untuk memastikan pemulihan penuh, mencegah insiden serupa, dan meningkatkan kesiapan menghadapi ancaman berikutnya. Kebijakan Penanganan Pasca Insiden Siber meliputi:

a. Penanganan pasca Insiden Siber merupakan kegiatan yang dilaksanakan setelah berakhirnya masa Insiden Siber.

b. Maksud dari penanganan pasca Insiden Siber adalah untuk meminimalisir Insiden Siber serupa tidak terjadi kembali di lingkungan Pemerintah Kabupaten Magelang.

c. Kegiatan penanganan pasca Insiden Siber tidak terbatas pada kegiatan:

1). Berbagi informasi dalam proses penanganan Insiden Siber, sehingga hal ini dapat menjadi media pembelajaran bagi Tim MagelangKab-CSIRT.

2). Evaluasi daftar risiko keamanan informasi.

3). Penerapan rencana tindak lanjut hasil evaluasi risiko keamanan informasi.

4). Penguatan Sistem Elektronik yang terdampak Insiden Siber.

5). Peningkatan kompetensi pengelola Sistem Elektronik.

C. PEMBINAAN

Kebijakan Pembinaan Magelangkab-CSIRT bertujuan untuk membentuk, mengembangkan, dan memastikan kesiapan tim tanggap insiden siber dalam menangani ancaman keamanan informasi secara efektif. Kebijakan Pembinaan Magelangkab-CSIRT adalah sebagai berikut:

1. Merupakan kegiatan untuk menjaga kemampuan MagelangKab-CSIRT dalam penanganan Insiden Siber.
2. Kegiatan pembinaan dikoordinir oleh Koordinator Insiden.
3. Kegiatan pembinaan dilaksanakan tidak terbatas pada kegiatan:
   a. Rapat Koordinasi yang dilakukan secara berkala (minimal 1 Tahun sekali atau insidental).
   b. Bimbingan teknis, *workshop* penanganan Insiden Siber.
   c. Simulasi penanganan Insiden Siber bagi kepala Perangkat Daerah, Agen, dan tim penanganan Insiden Siber pada MagelangKab-CSIRT.
   d. Asistensi penyusunan kebijakan dan prosedur keamanan informasi.
   e. Asisten penerapan kebijakan dan prosedur keamanan informasi.

D. EVALUASI PENANGANAN INSIDEN SIBER

Kebijakan Evaluasi Penanganan Insiden Siber merupakan panduan untuk menilai efektivitas proses penanganan insiden siber yang telah dilakukan, dengan tujuan meningkatkan kesiapan dan respons terhadap ancaman yang akan mendatang. Kebijakan Evaluasi Penanganan Insiden Siber meliputi:

1. Evaluasi penanganan Insiden Siber merupakan kegiatan untuk memastikan bahwa penanganan Insiden Siber sesuai dengan kebijakan, prosedur, dan petunjuk teknis yang terkait.
2. Evaluasi penanganan Insiden Siber dilakukan untuk setiap penanganan Insiden Siber dan menjadi satu kesatuan dengan laporan penanganan Insiden Siber.
3. Evaluasi penanganan Insiden Siber oleh Perangkat Daerah dilaksanakan oleh Agen Siber dan dilaporkan kepada kepalaPerangkat Daerah dan ketua

MagelangKab-CSIRT.

4. Evaluasi penanganan Insiden Siber oleh MagelangKab-CSIRT dilaksanakan oleh Koordinator Insiden dan dilaporkan kepada ketua MagelangKab-CSIRT.

BAB III

PROSEDUR PENANGANAN INSIDEN SIBER

A. PROSEDUR PENANGANAN INSIDEN *WEB DEFACEMENT*

Web Defacement merupakan insiden yang menyebabkan perubahan tampilan tidak wajar pada suatu sistem elektronik. Prosedur penanganan insiden *web defacement* dapat diuraikan sebagai berikut :

1. Persiapan

Tahap ini adalah tahap dimana kebijakan, prosedur, teknologi, dan sumber daya manusia harus disiapkan secara matang, dimana akan digunakan pada proses penanganan terhadap insiden. Dalam suatu organisasi/institusi, kemampuan melakukan respon yang cepat terhadap suatu insiden, merupakan persiapan yang mendasar bagi penanganan insiden *Web Defacement*.

Langkah-langkah yang diambil pada tahap ini antara lain:

a. Menyiapkan dokumen yang dibutuhkan dalam proses penanganan insiden. Dokumen ini antara lain adalah:
   1). *Standar Operation Procedure*;
   2). Form-form yang akan digunakan: form penanganan insiden, form *chain of custody*;
   3). Gambaran diagram terbaru yang menggambarkan hubungan antar komponen- komponen aplikasi yang membangun *website* (web server, aplikasi web, para user, diagram *network*);
   4). Dokumentasi dari sistem operasi, aplikasi, protokol dan anti virus yang terdapat pada web server.

b. Lakukan koordinasi insiden dengan tim yang dapat menangani secara teknis, koordinasi dengan tim CSIRT ataupun *Point of Contact* untuk mendapatkan informasi tambahan dalam penanangan insiden;

c. Menyimpan bukti insiden antara lain *screenshot* insiden *web defacement*, log server ataupun log perangkat pendukung server. Jika menemukan file yang mencurigakan dapat dilakukan pendokumentasian file tersebut. Untuk kegiatan forensik, dapat juga dilakukan proses

imaging baik seluruh storage server ataupun memori (RAM) yang digunakan;

d. Menentukan tempat (ruangan) untuk menangani insiden baik kegiatan rapat tim maupun kegiatan analisis insiden;

e. Menyiapkan tool dan media yang dibutuhkan untuk menangani insiden. *Tools* yang dapatdisiapkan antara lain *Scanning Tools, ForensicTools*, dan Monitoring *Tools*. Media dapat berupa *storage external*.

2. Identifikasi dan Analisis

Pada tahap ini dilakukan proses identifikasi untuk memastikan bahwa insiden yang telah terjadi dapatdiketahui sumber serangannya. Selain itu juga untuk mengumpulkan informasi yang cukup tentang insiden tersebut sehingga tim dapat memprioritaskan langkah selanjutnya dalam menangani insiden. Dalam proses identifikasi, prosedur yang dilakukan adalah sebagai berikut:

a. Memeriksa file-file yang bersifat statis, apakah terjadi perubahan dan kapan perubahan itu terjadi. Memeriksa semua link yang ada pada halaman web (*src, meta, css, script*);

b. Memeriksa semua *log file. File log* yang dapat diperiksa antara *lain Error Log, Access Log, Database Log, Auth Log, Install Log, Event Log, Firewall Log, IDS/IPS Log, Switch/Router Log*;

c. Memeriksa folder pada *website* yang bersifat publik (akses *write*, biasanya untuk menyimpan *file upload*) untuk indikasi *file backdoor*, *Malware*, *trojan*, atau *maliciuous file* lainnya;

d. Memeriksa kembali kode sql yang digunakan pada web aplikasi, apakah terdapat *bug* pada *code* tersebut. Memeriksa pada implementasi fitur *Login/Logout*, Koneksi Database, dan Menampilkan Isi *Database*;

e. Memeriksa *version* setiap aplikasi/*library* yang digunakan. Periksa versi web server, versi aplikasi dan versi database;

f. Memeriksa setiap koneksi yang terhubung ke server tersebut;

g. Memeriksa layanan/service yang sedang berjalan. Periksa semua port yang terbuka, periksa *cronjob* (service otomatis harian), periksa *last login* untuk user, periksa *history*;

h. Dalam melakukan tahapan ini, *tools* yang dapat digunakan antara lain:

NMap, Nikto, Accunetic,Nessus.

3. *Containment*

Untuk mengurangi dampak peningkatan resiko (mitigasi) perlu dilakukan hal-hal sebagai berikut :

a. Perlu dilakukan pembangunan website sementara agar publikasi informasi pada website tetap berjalan. Atau dapat juga dilakukan pembangunan *site under maintenance*;
b. Lakukan *backup* sistem, untuk keperluan forensik ataupun untuk mengumpulkan bukti-bukti insiden;
c. Pembatasan akses terhadap sumber serangan yang ditemukan antara lain sumber IP, sumber port, serta akun user yang digunakan oleh penyerang.

4. *Eradication*

Setelah ditemukan aplikasi ataupun file yang bersifat *malicious*, maka tahap selanjutnya adalah melakukan penghapusan konten tersebut. Adapun tahapannya adalah sebagai berikut:

a. Lakukan hapus *file malicious*, antara lain: *file defacement*, *file backdoor*, *file rootkit* ataupun *file Malware*;
b. Lakukan *uninstall* aplikasi yang ditemukan sebagai aplikasi *malicious*;

5. *Recovery*

Pada tahapan ini bertujuan untuh memulihkan kembali halaman web kepada keadaan semula. Prosedur yang dapat dilakukan adalah sebagai berikut:

a. Mengaktifkan (*me-restore*) file-file yang telah di- *backup*. File dapat berupa file pada *web server*, *file database*. Dan gunakan aplikasi checksum sebagai data *integrity checker* pada *file backup* tersebut;
b. Lakukan *update/upgrade/patch* semua aplikasi yang digunakan pada web server. Jika menggunakan CMS, *update* versi web aplikasi, *plugins*, *themes* yang digunakan. Jika menggunakan API dapat melakukan *update library* yang digunakan. Selain itu perlu dilakukan *update rules* pada konfigurasi keamanan yang digunakan;
c. Lakukan *automatic updates* pada setiap aplikasi yang digunakan;

d. Lakukan pembaruan seluruh akun yang digunakan baik pada sistem operasi, web aplikasi;
e. Lakukan *hardening* server ataupun aplikasi yang digunakan seperti memasang *Web Application Firewall* (WAF), memasang aplikasi *anti-defacement (DotDefender, Nagios, Webguard)*;
f. Pisahkan antara *file webserver* dengan *file database* pada partisi yang digunakan.

6. Tindak Lanjut

Sebagai tindak lanjut penanganan insiden, perlu dilakukan hal-hal sebagai berikut:

a. Lakukan uji keamanan web server dan aplikasi;
b. Memetakan kerentanan yang ditemukan, baik rentan terhadap serangan *SQL Injection, XSS, Misconfiguration*, atau sudah *deprecated* /usangnya versi aplilkasi yang digunakan;
c. Membuat semua dokumentasi dan laporan terkait kegiatan dan waktu yang dibutuhkan pada proses *incident handling* yang telah dilakukan;
d. Menuliskan *tools* apa saja yang digunakan dalam membatu proses *incident handling*;
e. Menuliskan bukti-bukti yang ditemukan, hal ini terkait dengan proses hukum kedepannya;
f. Memberikan analisa dan penjelasan apa yang harus dilakukan sehingga insiden serupa tidak terulang kembali;
g. Membuat evaluasi dan rekomendasi.

B. PROSEDUR PENANGANAN INSIDEN *PHISING*

Insiden *phising* adalah insiden yang diakibatkan dengan melakukan serangan untuk menipu/memancing korban agar mau mengklik tautan serta menginput informasi kredential seperti *username* dan *password*. Prosedur penanganan insiden *phising* dijabarkan sebagai berikut :

1. Persiapan

Tahap persiapan penangan *phising* dijabarkan sebagai berikut:

a. Membuat daftar semua domain sah yang dimiliki organisasi;

b. Mempersiapkan satu buah halaman website untuk memperingatkan pengguna tentang terjadinyaserangan *phising*;
c. Mempersiapkan formulir untuk informasi laporan penyalahgunaan domain.
d. Membangun kontak dengan pihak-pihak terkait, seperti perusahaan *hosting*, penyedia domain, penyedia jasa email, Nasional CERT;
e. Meningkatkan kesadaran terhadap serangan phishing, diantaranya :
    1). Tidak mengklik link yang mencurigakan;
    2). Tidak memasukan *username* dan *password* pada situs web yang alamat web nyameragukan;
    3). Merubah penulisan alamat email yang dipublish, dari bentuk @ menjadi “at” atau dalam bentuk gambar, untuk menghindari menjadi target email *phising*;
    4). Menggunakan Anti Virus yang memiliki fitur Anti *Phising*.

2. Identifikasi dan Analisis

Pada tahap ini dilakukan proses identifikasi untuk memastikan bahwa insiden yang telah terjadi dapatdiketahui sumber serangannya. Selain itu juga untuk mengumpulkan informasi yang cukup tentang insiden tersebut sehingga tim dapat memprioritaskan langkah selanjutnya dalam menangani insiden. Prosedur yang dilakukan dalam proses identifikasi penanganan serangan *phising* adalah sebagai berikut:

a. Memonitoring *email, social media, web forms* dsb pada Organisasi untuk mencari informasi *Phising*;
b. Memeriksa URL *phising* dan *hyperlink* yang mencurigakan menggunakan *www.virustotal.com, www.urlvoid.com,* serta *www.phishtank.com*
c. Melibatkan pihak yang tepat terkait serangan *phising* seperti perusahaan *hosting*, penyedia domain, penyedia jasa email, Nasional CERT agar dapat segera di lakukan *takedown* terhadap web *phising*.
d. Mengumpulkan bukti bukti terkait adanya serangan *phising*.

3. *Containment*

Setelah dipastikan bahwa memang benar telah terjadi serangan phishing, maka dilakukan proses mitigasi serangan, agar tidak terjadi

kerusakan lebih dalam. Prosedur yang dilakukan pada tahap ini adalah:

a. Menyebarkan URL *phising* dan konten dari email *phising* pada pihak *spam- reporting website*, misalnya *www.phishtank.com*;
b. Menginformasikan serangan *phising* kepada pengguna, agar pengguna mengetahui dan tidak terkena dampak dari serangan tersebut;
c. Memeriksa *source code* dari website *phising*, jika menggunakan gambar dari website yang anda miliki, anda dapat mengganti gambar dengan tampilan "*PHISING WEBSITE*".

4. *Eradication*

Proses ini bertujuan untuk mengambil tindakan dalam menghentikan serangan *phising*. Prosedur untuk melakukan proses ini dapat dilakukan dengan cara berikut:

a. Jika halaman *phising* di *hosting* di situs web yang telah disusupi, maka hubungi pemilik dari website tersebut, agar halaman *phising* dihapus dan dilakukan *update* security;
b. Untuk percepatan penanganan, hubungi perusahaan *hosting* dengan mengirim email berisikan informasi *phising*, serta lakukan kontak telepon perusahaan *hosting* yang tersedia;
c. Menghubungi perusahaan *hosting* untuk melakukan *takedown*/penutupan alamat website palsu;
d. Jika *takedown* terlalu lama, maka hubungi Nasional CERT untuk mengontak CERT lokal yang berada di negara tersebut untuk membantu proses *takedown*.

5. Tindak Lanjut

Sebagai tindak lanjut penanganan insiden, perlu dilakukan hal-hal sebagai berikut:

a. Membuat evaluasi dan rekomendasi. Menyempurnakan langkah-langkah respon, prosedur penanganan serangan yang diambilselama insiden agar kedepannya dapat menangani insiden secara lebih cepat dan efisien;
b. Memperbaharui daftar kontak yang dimiliki, disertai catatan cara paling efektif untuk menghubungi setiap pihak yang terlibat;
c. Berkolaborasi dengan tim hukum jika diperlukan tindakan hukum;

d. Membuat dokumentasi dan laporan terkait penanganan serangan *Phising*;
e. Membuat evaluasi dan rekomendasi.

C. PROSEDUR PENANGANAN INSIDEN *MALWARE*

Malware, atau *Malicious Software*, merupakan suatu definisi yang diberikan untuk setiap program atau file atau kode yang dapat membahayakan suatu sistem. *Malware* berusaha menyerang, merusak, atau menonaktifkan komputer, sistem komputer, jaringan, tablet, dan perangkat seluler, sering kali dengan mengambil sebagian kendali atas operasi perangkat.

1. Persiapan

Tahap ini adalah tahap dimana kebijakan, prosedur, teknologi, dan sumber daya manusia harus disiapkan secara matang, dimana akan digunakan pada proses penanganan terhadap insiden. Dalam suatu organisasi/institusi, kemampuan melakukan respon yang cepat terhadap suatu insiden, merupakan persiapan yang mendasar bagi penanganan insiden yang disebabkan oleh *Malware*. Langkah-langkah yang diambil pada tahap ini antara lain:

a. Pembentukan Tim Respon

Tim dapat berasal dari internal organisasi/institusi atau jika memang diperlukan dapat berasal dari luar organisasi/institusi (eksternal). Anggota tim memiliki pengetahuan tentang *Malware* dan memiliki kemampuan penanganan insiden *Malware*.

b. Penyiapan Dokumen

Menyiapkan dokumen yang dibutuhkan dalam proses penanganan insiden *Malware*. Dokumen ini antara lain:

1). Panduan Penanganan Insiden Siber
2). Formulir Penanganan Insiden Siber
3). Dokumen Kebijakan, diantaranya: kebijakan keamanan kebijakan pengunaan laptop, antivirus, internet dan email, serta kebijakan *backup*.
4). Dokumen Profil dari semua perangkat lunak dan proses-proses yang harus berjalan pada sistem berdasarkan proses bisnis

organisasi.

5). Database penanganan insiden yang pernah terjadi sebelumnya.

6). Daftar yang memuat indikasi-indikasi suatu komputer atau jaringan terkena *Malware*, misalkan daftar aplikasi yang telah terindikasi terkena *Malware*, alamat IP terkait dengan *Command and Control* (C&C).

c. Menentukan tempat (ruangan) untuk penanganan.

d. Menentukan lingkungan yang aman untuk analisa *Malware*.

e. Menyiapkan *tools* yang akan digunakan, diantaranya:

1). *Tools* untuk penyaringan, misalnya:

a). *Squid* merupakan perangkat lunak *open source* pada *web proxy* yang mendukung filter URL;

b). *Squid Guard* adalah *tools* yang dapat digunakan untuk menyederhanakan tugas filter URL yang merupakan plug-in untuk squid yang merupakan kombinasi dari *filter, redirector*, dan akses kontrol, yang dapat digunakan untuk membuat aturan akses berdasarkan pada waktu, kelompok pengguna, dan URL.

c). *Tools* untuk menghitung nilai *hash*.

d). *Tools* untuk deteksi virus baik berbasis *host* maupun online, misalnya antivirus dan website *www.virustotal.com*

e). *Tools* pendeteksi berbasis *host*, misalnya *Samhain*, OSSEC dan Osiris.

2). *Tools* untuk analisa *Malware*, meliputi :

a). Mesin uji, merupakan mesin virtual untuk melakukan analisis terhadap *Malware*, misalnya VMWare, MS VPC, dan Xen. Mesin uji ini diperlukan dalam melakukan analisa *Malware* menggunakan metode analisadinamis.

b). *Utility toolkit*, *tools* ini digunakan untuk mengumpulkan sampel untuk analisis *Malware* atau untuk mengidentifikasi, menampung, dan memberantas *Malware*, misalnya *SysInternals*.

c). *Reverse Engineering tools*, merupakan *tools* yang digunakan untuk melakukan analisa lebih lanjut terkait *source code* dari sampel *Malware*, misalnya *IDA-Pro, CFF Explorer,* dan *WinHex*.

Reverse Engineering tools diperlukan dalam melakukan analisa *Malware* menggunakan metode analisa statis.

2. Identifikasi dan Analisis

Tahap ini merupakan tahap identifikasi adanya *Malware*. Proses-proses yang dilakukan dalam tahap identifikasi adalah sebagai berikut :

a. Memeriksa apakah antivirus berfungsi normal atau tidak. Hal ini karena ada *Malware* yang dapat menghancurkan instalasi antivirus dengan merusak *executable file*, mengubah kunci registri atau merusak file definisi, maupun menonaktifkan *update* dari *signature* suatu file.
b. Mengecek file yang tidak dikenal pada *root* atau *system directory*.
c. Memeriksa file dengan ekstensi ganda. Sangat disarankan untuk menonaktifkan opsi fitur 'sembunyikan ekstensi' pada *file explorer* untuk mengetahui ekstensi yang sebenarnya dari suatu file.
d. Memeriksa proses dan *service* yang tidak dikenal dalam sistem menggunakan *Task Manager*.
e. Memeriksa utilitas sistem, misalnya *Task Manager* atau *SysInternals Process Explorer*. Terdapat *Malware* yang menonaktifkan utilitas ini sehingga tidak dapat dijalankan.
f. Memeriksa penggunaan memory CPU menggunakan *Task Manager*.
g. Memeriksa anomali pada *Registry Key*.
h. Memeriksa anomali pada traffic jaringan. *Malware* modern saat ini kebanyakan memiliki fitur "*Command and Control*" dimana biasanya setiap *Malware* yang sudah menginfeksi suatu sistem, akan mengirimkan sinyal kepada induk *Malware* melalui aktivitas "*Command and Control*" tersebut.
i. Identifikasi anomali proses dan service yang dibuat pada Task Scheduler
j. Identifikasi *user account* pada sistem. Beberapa *Malware* mempunyai kemampuan untuk membuat *user account* baru pada sistem operasi yang terinfeksi.
k. Identifikasi *entry log* pada sistem operasi menggunakan *Event Viewer*.
l. Identifikasi proses yang mencurigakan menggunakan *SysInternals Tools*. SysInternal *Tools* merupakan salah satu kumpulan *tools* utilitas

milik Microsoft.

3. *Containment*

Tahap ini bertujuan untuk menghentikan atau mencegah penyebaran *Malware*. Prosedur yang dilakukan pada tahap *containment* adalah sebagai berikut:

a. Meminta izin kepada pemilik sistem untuk memutus sistem yang terinfeksi *Malware* dari jaringan.
b. Isolasi sistem yang terinfeksi *Malware*. Hal ini dapat dilakukan dengan cara mencabut kabel LAN atau memindahkan sistem tersebut ke VLAN khusus.
c. Namun, perlu menyimpan informasi koneksi jaringan pada sistem sebelum memutuskan hubungan dari jaringan yang mungkin akan dibutuhkan dalam melakukan analisa selanjutnya.
d. Mengubah konfigurasi routing table pada Firewall untuk memisahkan sistem yang terinfeksi *Malware* dengan sistem lainnya.
e. Melakukan *backup* data pada sistem yang terinfeksi *Malware*.
f. Identifikasi gejala kemiripan pada sistem lain untuk mencegah penyebaran *Malware*. Jika terdapat kemiripan, maka sistem tersebut juga harus dilakukan proses *containment*.

4. *Eradication*

Tahap ini merupakan tahapan dimana beberapa teknik yang berbeda-beda digunakan untuk melakukan analisa terhadap *Malware* dan menghapus *Malware* dari sistem yang telah terinfeksi. Setelah file yang terinfeksi diidentifikasi, gejala *Malware* dicatat dan executable *Malware* diidentifikasi dan dianalisis, kemudian semua *file executables Malware* dan artefak yang ditinggalkan oleh *Malware* akan dihapus, serta menutup port yang terindikasi sebagai lubang masuknya *Malware*.

Proses-proses yang dilakukan dalam tahap ini adalah sebagai berikut:

a. Menghentikan proses yang terindikasi sebagai proses yang *malicious*, dengan cara sebagai berikut:
    1). Tidak melakukan *kill / end process* terhadap *malicious process* tersebut. Hal ini dikarenakan *Malware* akan melakukan *autostart process* ketika prosesnya terhenti.

2). Lakukan *suspend* terhadap proses tersebut, kemudian lakukan record pada path EXE proses tersebut dan file DLL yang dipanggil oleh proses tersebut.

3). Dalam kondisi *sleep* (proses di *suspend*), kemudian satu persatu lakukan *kill process* dari kumpulan *malicious process* tersebut dimulai dari child *process* ke *parent process*.

4). Jika *malicious process* masih melakukan *autostart* atau mengganti Namanya dengan nama proses baru, maka perlu didokumentasikan lebih lanjut dan simpan *malicious* program tersebut ke media lain untuk proses analisa yang lebih mendetail.

b. Menghapus *autostart process* yang mencurigakan dari hasil analisa aplikasi *autostart*.

c. Jika proses tersebut kembali lagi, jalankan *Process* Monitor untuk mengidentifikasi apakah ada lokasi lain dimana *Malware* tersebut bersembunyi.

d. Lakukan proses di atas secara berulang hingga dapat dipastikan semua *malicious* program telah dihapus dan prosesnya sudah di *kill process*.

e. Setelah program *Malware* dihapus dan *malicious process* di *kill process*, lakukan full *scanning* terhadap sistem menggunakan signature antivirus yang sudah diperbaharui.

f. Jika proses *scanning* antivirus tidak dapat dilakukan karena telah diblokir oleh *Malware*, maka lakukan proses sebagai berikut :

1). *Booting* sistem melalui *Live usb rescue disk*, misalnya *Hiren Boot CD, FalconFour's Ultimate Boot CD, Kaspersky Rescue Disk*, dll.

2). Live usb tersebut dapat berupa sistemoperasi Linux ataupun miniXP yang berisi beberapa *tools* seperti *defragment tools, driver tools*, *backup* dan recover data *tools*, antivirus dan anti-*Malware tools*, rootkit detection *tools*, *secure* data wiping *tools*, partitioning *tools*, *password* recovery *tools*, network *tools*, recover/repair broken partitions *tools*, dll. Lakukan proses mountingsistem operasi yang terinfeksi ke dalam *Live usb* yang sedang berjalan.

3). Lakukan proses *scanning* antivirus dan anti *Malware* pada Live usb yang sedang berjalan

g. Jika terdapat user-user yang dibuat oleh *Malware*,maka hapus user-user yang tidak dikenali tersebut untuk menghindari masuknya kembali *Malware* melalui user yang tidak dikenal tersebut.

5. Pemulihan

Pemulihan merupakan tahap untuk mamulihkan data sistem yang terinfeksi *Malware* serta mengembalikan seluruh sistem bekerja normal seperti semula. Langkah yang dilakukan terhadap pemulihan sistem, diantaranya:

a. Validasi sistem untuk memastikan sudah tidak adaaplikasi atau file yang rusak atau terinfeksi *Malware*. Begitu pula kesalahan atau kekurangan konfigurasi sistem untuk kemudian disesuaikan kembali.

b. Melakukan aktivitas monitoring untuk memastikan apakah *Malware* masih ada atau kembali lagi setelah proses eradication dengan malakukan hal- hal sebagai berikut :

   1) Memantau proses dan servis yang berjalan menggunakan *Process* Monitor dan *Process* Explorer.

   2) Memantau aktivitas traffic jaringan menggunakan *tools* wireshark atau *tcpdump* untuk memantau apakah ada *request outgoing* atau *traffic incoming* yang mencurigakan, serta *request query* DNSkarena *Malware* yang memiliki kemampuan *Command and Control* biasanya melakukan kontak dengan induknya.

c. Jika terjadi kerusakan yang cukup parah, maka sistem dibangun ulang dengan file *backup* terakhir yang dimiliki.

d. Melakukan *patching* sistem.

e. Melakukan *hardening* terhadap sistem.

f. Menambahkan signature dari *Malware* ke sistem monitoring atau database antivirus.

6. Tindak Lanjut

Tahap ini adalah fase di mana semua dokumentasi kegiatan yang dilakukan dicatat sebagai referensi untukmasa mendatang. Prosedur yang dapat dilakukan adalah sebagai berikut:

a. Membuat dokumentasi dan laporan terkaitpenanganan insiden *Malware*, yang berisi langkah-langkah dan hasil yang telah didapatkan.

b. Memberikan analisa dan penjelasan apa yang harus dilakukan, sehingga meminimalisir insiden serupa tidak terulang kembali.
c. Menuliskan bukti-bukti yang ditemukan, hal ini terkait dengan proses hukum kedepannya.
d. Membuat evaluasi dan rekomendasi. Rekomendasi yang dapat diberikan diantaranya:
    1). Penambahan pengetahuan tentang penanganan insiden *Malware*, misalnyamelalui petatihan
    2). Memperbaharui anti *Malware* dengan signature file yang baru, dengan harapan dapat berhasil dalam mendeteksi danmenghapus *Malware*
    3). Meningkatkan pertahanan sistem terhadap *Malware*
e. Mendokumentasikan *Malware* terkait jalan masuk, perilaku, dampak kerusakan, dan lain lain yang terkait *Malware* ke dalam database *Malware*.
f. Menyempurnakan langkah-langkah respon atau prosedur penanganan insiden *Malware* yang ada.

D. PROSEDUR PENANGANAN INSIDEN *RANSOMWARE*

Ransomware merupakan jenis *Malicious Software* tertentu yang menuntut tebusan finansial dari seorang korban dengan melakukan penahanan pada aset atau data yang bersifat pribadi. Kegiatan penyebaran *ransomware* dilakukan oleh penyerang atau Threat Actor dengan tujuan utama adalah finansial, oleh karenanya Threat Actor menjadikan data pribadi sebagai ancamannya. Indikasi utama adanya *ransomware* adalah terdapatnya file baik dokumen atau gambar yang dienkripsi, terdapatnya file pesan (Readme File) yang mencantumkan alamat finansial dan alamat email penyerang.

Prosedur penanganan insiden *ransomware* dijabarkan sebagai berikut:

1. Persiapan

Tahap ini adalah tahap dimana kebijakan, prosedur, teknologi, dan sumber daya manusia harus disiapkan secara matang, dimana akan digunakan pada proses penanganan terhadap insiden. Dalam suatu organisasi/institusi, kemampuan melakukan respon yang cepat terhadap

suatu insiden, merupakan persiapan yang mendasar bagi penanganan insiden *Ransomware*. Tahap persiapan penangan *ransomware* dijabarkan sebagai berikut:

a. Pembentukan Tim

Tim dapat berasal dari internal organisasi/institusi atau jika memang diperlukan dapat berasal dari luar organisasi/institusi (eksternal). Anggota tim memiliki pengetahuan tentang *Ransomware* dan memiliki kemampuan penanganan insiden *Ransomware*.

b. Penyiapan Dokumen Legal

Menyiapkan dokumen yang dibutuhkan dalam proses penanganan insiden *Malware*. Dokumen iniantara lain:

1). Panduan/Formulir Penanganan Insiden Siber
2). Dokumen Kebijakan
3). Dokumen *Base line Performance*, Audit Sistem, Topologi Jaringan
4). Database penanganan insiden yang pernah terjadi sebelumnya
5). Daftar yang memuat jenis dan tipe *ransomware*

c. Melakukan koordinasi dengan pihak terkait

1). pihak Korban
2). Pihak Pengelola Sistem Jaring Komunikasi
3). Tim CSIRT Lain
4). Tim Pakar / Praktisi

d. Penyiapan *Tools*

1). Evidence Collection

- Windows Evidence Collection
  Brimorlabs: https://www.brimorlabs.com/*tools*/
- Incident Rescue:
  https://github.com/diogo-fernan/ir-rescue
- X-Way Forensics :
  http://www.x-ways.net/forensics/
- Fast IR Collection:
  https://github.com/SekoiaLab/Fastir_Collector/releases
- Redline:
  https://www.fireeye.com/services/freeware/redline.html

2). Pcap capture yang digunakan untuk menangkap jaringan inbound dan outbond pada sistem, misal: Wireshark.

3). Endpoint Security *Tools* yang digunakan sebagai *Host* Intrusion Detection System (HIDS) seperti:

- ❖ OSSEC https://www.ossec.net/downloads
- ❖ OSSIM https://www.alienvault.com/products/ossim
- ❖ Wazuh https://documentation.wazuh.com/3.12/installation-uide/virtual-machine.html

4). *Ransomware* Decryptor URL:

- ❖ Nomoreransom: https://nomoreransom.org
- ❖ Emsisoft: https://blog.emsisoft.com

5). *Malware* Analysis

- ❖ VirusTotal : https://virustotal.com
- ❖ Hybrid-Analysis: https://www.hybrid-analysis.com/
- ❖ Cuckoo Sandbox: https://cuckoosandbox.org/download

2. Identifikasi

Melakukan identifikasi dan analisis terhadap sistem terdampak guna mendapatkan akar permasalahan dari insiden yang terjadi. Langkah yang dapat dilakukan adalah sebagai berikut:

a. Melakukan identifikasi jenis *ransomware* untuk melakukan analisis lebih lanjut. Adapun langkah-langkah yang dilakukan sebagai berikut:

1). Temukan pesan yang disampaikan oleh aplikasi *Ransomware* (README File). Dalam file pesan tersebut berisi mengenai alamat email penyerang, string pesan, interface dari *Malware* tersebut;

2). Temukan jenis ekstensi dari file yang terkena insiden *ransomware* (misalkan *.crypt, *.cry,*.locked, dst)

3). Gunakan file Readme, Email Penyerang, dan Sampel File yang terkena insiden untuk mendapatkan jenis *Ransomware*.

4). Upload file pada poin 3 pada beberapa penyedia *decryption tools* seperti No more ransom dan Emsisoft.

b. Memeriksa apakah antivirus berfungsi normal atau tidak. Hal ini karena ada *Malware* yang dapat menghancurkan instalasi antivirus dengan

merusak executable file, mengubah kunci registri atau merusak file definisi, maupun menonaktifkan *update* dari signature suatu file.

c. Melakukan identifikasi dan analisis pada environment sistem terdampak guna mencari persistent mechanism penyerang atau artefak hasil penyerangan yang dilakukan. Proses yang dilakukan adalah sebagai berikut:
   1). Identifikasi dan analisis proses berjalan
   2). Identifikasi dan analisis jaringan komunikasi (pcap analysis)
   3). Identifikasi dan analisis registry
   4). Identifikasi dan analisis aplikasi startup
   5). Identifikasi dan analisis layanan/aplikasi terjadwal
   6). Identifikasi dan analisis browser history
   7). Identifikasi dan analisis sistem log
d. Melakukan identifikasi dan analisis pada sistem jaringan komunikasi untuk mengetahui Lateral Movement dari penyerang dengan melakukan implementasi daftar indikasi kebocoran (indicator of compromise) pada perimeter keamanan seperti Firewall, Network IDS, *Host* IDS.

3. *Containment*

Tahap ini bertujuan untuk menghentikan atau mencegah penyebaran APT. Prosedur yang dilakukan pada tahap *containment* adalah sebagai berikut :

a. Melakukan isolasi sistem terdampak.
b. Menutup akses ke jaringan.
c. Mengubah konfigurasi routing table pada Firewall untuk memisahkan sistem yang terinfeksi dengan sistem lainnya.
d. Melakukan *backup* data pada sistem yang terdampak.
e. Identifikasi gejala kemiripan pada sistem lain untuk mencegah penyebaran serangan. Jika terdapat kemiripan, maka sistem tersebut jugaharus dilakukan proses *containment*.

4. *Eradication*

Tahap ini merupakan tahapan dimana beberapa teknik yang berbeda-beda digunakan untuk melakukan analisaterhadap *malicious activity* dan menghapusnya dari sistem yang telah terinfeksi. Proses-proses yang

dilakukan dalam tahap ini adalah sebagai berikut:

a. Menghentikan proses yang terindikasi sebagai proses yang *malicious*, dengan cara sebagai berikut:
   1). Tidak melakukan *kill / end process* terhadap *malicious process* tersebut. Hal ini dikarenakan *Malware* akan melakukan *autostart process* ketika prosesnya terhenti.
   2). Lakukan *suspend* terhadap proses tersebut, kemudian lakukan record pada path EXE proses tersebut dan file DLL yang dipanggil oleh proses tersebut.
   3). Dalam kondisi *sleep* (proses di *suspend*), kemudian satu persatu lakukan *kill process* dari kumpulan *malicious process* tersebut dimulai dari child *process* ke *parent process*.
   4). Jika *malicious process* masih melakukan *autostart* atau mengganti namanya dengan nama proses baru, maka perlu didokumentasikan lebih lanjut dan simpan *malicious* program tersebut ke media lain untuk proses analisa yang lebih mendetail.
b. Menghapus *autostart process* yang mencurigakan dari hasil analisa aplikasi *autostart*.
c. Setelah program *Malware* dihapus dan *malicious process* di *kill process*, lakukan full *scanning* terhadap sistem menggunakan signature antivirus yang sudah diperbaharui.

5. Pemulihan

Tahap pemulihan merupakan tahap mengembalikan sistem terdampak pada kondisi normal seperti semula. Proses yang dilakukan adalah sebagai berikut:

a. Melakukan dekripsi file yang terkena dampak dengan menggunakan *decryption tools* yang tersedia;
b. Melakukan validasi sistem untuk memastikan sudah tidak ada aplikasi atau file yang rusak atau terinfeksi. Begitu pula kesalahan atau kekurangan konfigurasi sistem untuk kemudian disesuaikan kembali.
c. Melakukan aktivitas monitoring untuk memastikan apakah *malicious activity* masih ada atau kembali lagi setelah proses eradication dengan melakukan hal-hal sebagai berikut:

1). Memantau proses dan servis yang berjalan menggunakan *Process* Monitor dan *Process* Explorer.

2). Memantau aktivitas traffic jaringan menggunakan *tools* wireshark atau *tcpdump* untuk memantau apakah ada *request outgoing* atau *traffic incoming* yang mencurigakan, serta *request query* DNS karena *malicious activity* yang memiliki kemampuan *Command and Control* biasanyamelakukan kontak dengan induknya.

d. Jika terjadi kerusakan yang cukup parah (file sistem terhapus, data penting hilang, menyebabkan kegagalan *Booting* pada sistem operasi), maka sistem dibangun ulang dari file *backup* terakhir sistem yang dimiliki.

e. Melakukan *update*/*patching* sistem.

f. Melakukan *update*/*patching* antivirus.

6. Tindak Lanjut

Tahap ini adalah fase di mana semua dokumentasi kegiatan yang dilakukan dicatat sebagai referensi untuk masa mendatang. Prosedur yang dapat dilakukan adalah sebagai berikut:

a. Membuat dokumentasi dan laporan terkait penanganan insiden *Ransomware*, yang berisi langkah-langkah dan hasil yang telah didapatkan.

b. Memberikan analisa dan penjelasan apa yang harus dilakukan, sehingga meminimalisir insiden serupa tidak terulang kembali.

c. Menuliskan bukti-bukti yang ditemukan, hal ini terkait dengan proses hukum kedepannya.

d. Membuat evaluasi dan rekomendasi. Rekomendasi yang dapat diberikan diantaranya:

1). Peningkatan pengetahuan tentang penanganan insiden *Ransomware*, misalnya melalui pelatihan, *cyber exercise*.

2). Implementasikan sistem monitoring untuk pendeteksian dini serangan ataupun insiden.

3). Meningkatkan pertahanan sistem.

e. Melakukan penyempurnaan prosedur penanganan insiden berdasarkan insiden yang terjadi.

BAB IV
PENUTUP

Penyelenggaraan pelayanan publik dan tata kelola pemerintahan berbasis elektronik banyak membawa manfaat, mempermudah akses informasi serta meningkatkan efisiensi pelayanan pada masyarakat. Namun demikian terdapat ancaman keamanan pada sistem elektronik yang digunakan baik berupa potensi serangan maupun insiden siber.

Pedoman Penanganan Insiden Siber Kabupaten Magelang disusun sebagai rujukan bagi personil yang tergabung dalam MagelangKab-CSIRT atau Tim Tanggap Insiden Siber (TTIS) Kabupaten Magelang dalam menangani insiden siber pada sistem elektronik Pemerintah Kabupaten Magelang.