PANDUAN PENANGANAN INSIDEN RANSOMWARE

DINAS KOMUNIKASI, INFORMATIKA DAN STATISTIK
PROVINSI BALI

csirt.baliprov.go.id aduancsirt.baliprov.go.id

Versi Dokumen

No	Tanggal	Versi Dokumen	Oleh	Keterangan
1	Desember 2021	Versi 1.0	Diskominfos Prov. Bali	-

Kata Pengantar

Puji syukur kehadirat Tuhan Yang Maha Esa, atas segala limpahan rahmat, nikmat serta karunia-Nya yang tak ternilai dan tak dapat dihitung sehingga kami dapat menyelesaikan penyusunan “Panduan Penanganan Insiden *Ransomware*”. Panduan ini disusun dalam rangka memberikan acuan bagi pihak yang berkepentingan dalam pelaporan insiden siber. Panduan ini berisikan langkah-langkah yang harus diambil apabila terjadi serangan *Ransomware*, yang dimulai dari tahap persiapan sampai dengan tahap pembuatan laporan dari penanganan serangan. Panduan ini tentu saja masih banyak kekurangan dan masih jauh dari kesempurnaan karena keterbatasan ilmu dan referensi kami. Untuk itu, kami selalu berusaha melakukan evaluasi dan perbaikan secara berkala agar bisa mencapai hasil yang lebih baik lagi.

Akhir kata, kami ucapkan terima kasih kepada segala pihak yang telah membantu dalam penyusunan panduan ini.

Bali, 2 Desember 2021

Ditandatangani secara elektronik oleh :
KEPALA DINAS
Gede Pramana
NIP. 19680531 199703 1 002

Daftar Isi

Pendahuluan

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.

Beberapa jenis *Ransomware* adalah *Crypto Ransomware* (melakukan enkripsi pada dokumen), *Locker Ransomware* (melakukan enkripsi pada seluruh sistem), *Scareware* (memunculkan *popup* untuk menawarkan solusi terkait data terenkripsi), dan *Doxware* (melakukan pencurian data dan mengancam akan dipublikasikan).

Panduan Penanganan Insiden *Ransomware*

1. TUJUAN

Secara umum, tujuan panduan ini dimaksudkan untuk membantu organisasi memahami tentang penanganan suatu insiden *Ransomware*. Penanganan insiden yang dilakukan dengan tepat dan cepat, akan sangat bermanfaat untuk mengurangi resiko yang diakibatkan oleh *Ransomware* tersebut. Sedangkan secara khusus adalah sebagai berikut:

a. Memastikan adanya sumber daya yang memadai untuk menangani insiden yang terjadi
b. Melakukan pengumpulan informasi yang akurat
c. Meminimalisir dampak dari insiden yang terjadi.
d. Mencegah adanya serangan lanjutan dan mencegah kerusakan agar tidak lebih meluas

2. RUANG LINGKUP

Panduan ini berisi langkah-langkah yang harus diambil apabila terjadi insiden *Ransomware*, yang dimulai dari tahap persiapan sampai dengan tahap pembuatan laporan dari penanganan insiden. Panduan ini dapat dijadikan acuan bagi individual atau tim (administrator, pengelola TI, dan tim respon insiden keamanan siber) yang bertanggung jawab untuk mencegah, mempersiapkan, atau menanggapi insiden *Ransomware*.

3. PROSEDUR PENANGANAN *RANSOMWARE*

Penanganan terhadap insiden *ransomware* dapat dilakukan dalam beberapa tahap seperti pada gambar berikut:

Gambar 1. Tahap Penanganan Insiden

3.1. 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*.

Langkah-langkah yang diambil pada tahap ini antara lain:

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 *ransomware*. Dokumen ini antara lain:

- Panduan/Formulir Penanganan Insiden Siber
- Dokumen Kebijakan, diantaranya kebijakan keamanan, kebijakan pengunaan laptop, antivirus, internet dan *email*, serta kebijakan *backup*.
- Dokumen *Baseline Performance*, Audit Sistem, Topologi Jaringan
- *Database* penanganan insiden yang pernah terjadi sebelumnya
- Daftar yang memuat jenis dan tipe *ransomware*.

c. Melakukan koordinasi dengan pihak terkait :

- Pihak Korban
- Pihak Pengelola Sistem Jaring Komunikasi
- Tim CSIRT Lain
- Tim Pakar/Praktisi

d. Penyiapan *Tools*

- *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
- *Pcap Capture* yang digunakan untuk menangkap jaringan *inbound* dan *outbound* pada sistem, misal Wireshark.
- *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-guide/virtual-machine.html)
- *Ransomware Decryptor* URL
  - *Nomoreransom* : (https://nomoreransom.org)
  - *Emsisoft* : (https://blog.emsisoft.com)
- *Malware Analysis*
  - *VirusTotal* : (https://virustotal.com)
  - *Hybrid-Analysis* : (https://www.hybrid-analysis.com/)
  - *Cuckoo Sandbox* : (https://cuckoosandbox.org/download)

3.2. Indentifikasi dan Analisis

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

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 Nomoreransom 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 :
   - Identifikasi dan analisis proses berjalan

- Identifikasi dan analisis jaringan komunikasi (*pcap analysis*)
- Identifikasi dan analisis *registry*
- Identifikasi dan analisis aplikasi *startup*
- Identifikasi dan analisis layanan/aplikasi terjadwal
- Identifikasi dan analisis *browser history*
- 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.

3.3. *Containtment* (Penahanan)

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 juga harus dilakukan proses *containment*.

3.4. *Eradication* (Penghapusan Konten)

Tahap ini merupakan tahapan dimana beberapa teknik yang berbeda-beda digunakan untuk melakukan analisa terhadap *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 :
   - Tidak melakukan *kill* / *end process* terhadap *malicious process* tersebut. Hal ini dikarenakan *malware* akan melakukan *autostart process* ketika prosesnya terhenti.
   - Lakukan *suspend* terhadap proses tersebut, kemudian lakukan *record* pada *path* EXE proses tersebut dan *file* DLL yang dipanggil oleh proses tersebut.

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

3.5. 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 :
   - Memantau proses dan servis yang berjalan menggunakan *Process Monitor* dan *Process Explorer*.
   - 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* biasanya melakukan 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.

3.6. 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:
    - Peningkatan pengetahuan tentang penanganan insiden *ransomware*, misalnya melalui pelatihan, *cyber exercise*.
    - Implementasikan sistem *monitoring* untuk pendeteksian dini serangan ataupun insiden.
    - Meningkatkan pertahanan sistem
e. Melakukan penyempurnaan prosedur penanganan insiden berdasarkan insiden yang terjadi.

Referensi

1. Enterprise Survival Guide for *Ransomware* Attacks : https://www.sans.org/reading-room/whitepapers/incident/enterprise-survival-guide-*ransomware*- attacks-36962
2. *Ransomware* Incident Handling and Mitigation : https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Africa_Cyberdrill_18/Presentations/2 018-10-03_CS_*Ransomware*_incident_handling_mitigation_ITU_GrandB assam.pdf