DISKOMINFO BATAM

G20 INDONESIA 2022

BerAKHLAK
Berorientasi Pelayanan Akuntabel Kompeten Harmonis Loyal Adaptif Kolaboratif

PANDUAN PENANGANAN
INSIDEN RANSOMWARE

Dinas Komunikasi dan Informatika Kota Batam

DISKOMINFO BATAM

G20 INDONESIA 2022

BerAKHLAK
Berorientasi Pelayanan Akuntabel Kompeten Harmonis Loyal Adaptif Kolaboratif

PENDAHULUAN

Ransomware merupakan jenis malicious software tertentu yang menuntut tebusan finansial dari seorang korban dengan melakukan penahanan pada aset atau data yang bersifat pribadi.

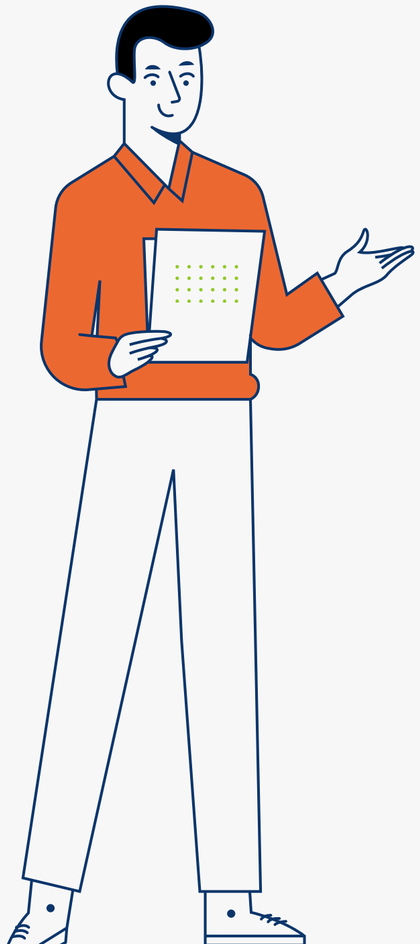
Indikasi utama adanya ransomware adalah terdapatnya file baik dokumen atau gambar yang dienkripsi, terdapatnya file pesan (Readme File) yang mencantumkan alamat finansial dan alamat email penyerang.

DISKOMINFO BATAM

G20 INDONESIA 2022

BerAKHLAK
Berorientasi Pelayanan Akuntabel Kompeten Harmonis Loyal Adaptif Kolaboratif

PROSEDUR PENANGANAN RANSOMWARE



STEP 06 — TINDAK LANJUT

STEP 05 — PEMULIHAN

STEP 04 — ERADICATION

STEP 03 — CONTAINMENT

STEP 02 — IDENTIFIKASI DAN ANALISIS

STEP 01 — PERSIAPAN

DISKOMINFO BATAM

G20 INDONESIA 2022

BerAKHLAK
Berorientasi Pelayanan Akuntabel Kompeten Harmonis Loyal Adaptif Kolaboratif

PERSIAPAN

1. Pembentukan tim respon, anggota tim memiliki pengetahuan tentang Ransomware dan memiliki kemampuan penanganan insiden Ransomware.

2. Penyiapan Dokumen Legal, dokumen ini antara lain adalah :
   - 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

3. Melakukan koordinasi dengan pihak terkait, diantaranya pihak korban, pihak pengelola sistem jaring komunikasi, tim CSIRT lain, tim pakar/praktisi.

4

Penyiapan Tools

1) Evidence Collection
   Windows Evidence Collection
- Brimorlabs : https://www.brimorlabs.com/tools/
- Incident Rescue : https://github.com/diogo-fernan/irrescue
- 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.ht ml

2) Pcap Capture digunakan untuk menangkap jaringan inbound dan outbound pada sistem, misal Wireshark.

3) Endpoint Security Tools 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/installationguide/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)

DISKOMINFO BATAM

G20 INDONESIA 2022

BerAKHLAK
Berorientasi Pelayanan Akuntabel Kompeten Harmonis Loyal Adaptif Kolaboratif

IDENTIFIKASI DAN ANALISIS

1

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

- Temukan pesan yang disampaikan oleh aplikasi Ransomware (README File). Dalam file pesan tersebut berisi mengenai alamat email penyerang, string pesan, interface dari malware tersebut.
- Temukan jenis ekstensi dari file yang terkena insiden ransomware (misalkan *.crypt, *.cry, *.locked, dst).
- Gunakan file Readme, Email Penyerang, dan Sampel File yang terkena insiden untuk mendapatkan jenis Ransomware.
- Upload file pada poin 3 pada beberapa penyedia decryption tools seperti Nomoreransom dan Emsisoft.

2

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.

IDENTIFIKASI DAN ANALISIS

3

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) 8 Panduan Penanganan Insiden Ransomware Badan Siber dan Sandi Negara
- 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

4

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.

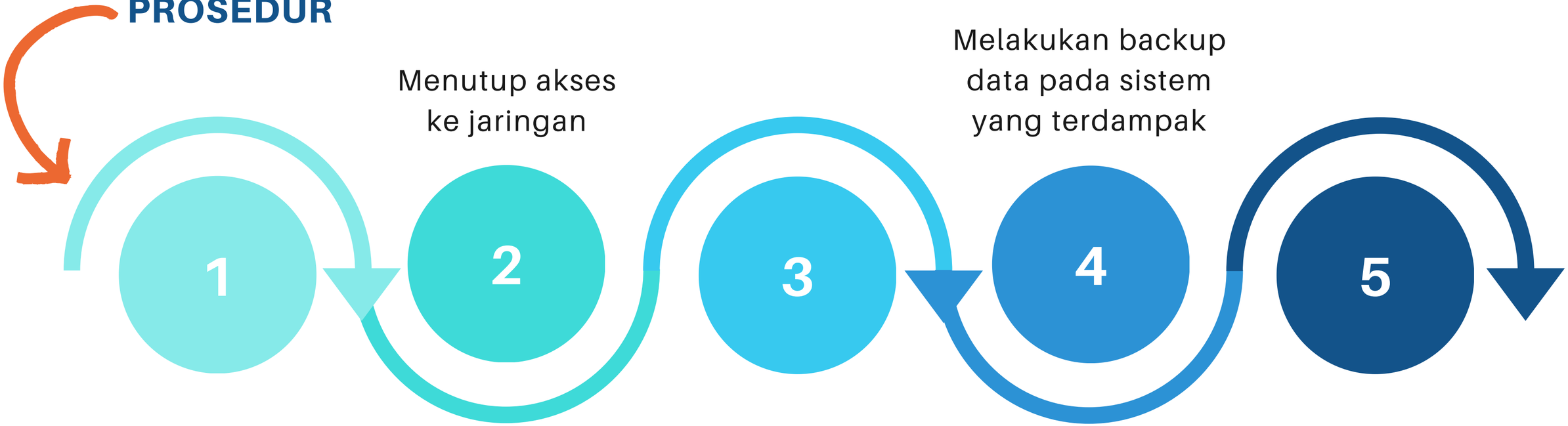
DISKOMINFO BATAM

G20 INDONESIA 2022 BerAKHLAK

CONTAINMENT

Containment (penahanan) tahap ini bertujuan untuk menghentikan atau mencegah penyebaran APT

PROSEDUR



1. Melakukan isolasi sistem terdampak
2. Menutup akses ke jaringan
3. Mengubah konfigurasi routing table pada Firewall untuk memisahkan sistem yang terinfeksi dengan sistem lainnya
4. Melakukan backup data pada sistem yang terdampak
5. Identifikasi gejala kemiripan pada sistem lain untuk mencegah penyebaran serangan

ERADICATION

Eradication (Penghapusan Konten) merupakan tahapan dimana beberapa teknik yang berbeda-beda digunakan untuk melakukan analisa terhadap malicious activity dan menghapusnya dari sistem yang telah terinfeksi

PROSES

1

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.**

DISKOMINFO BATAM

G20 INDONESIA 2022

BerAKHLAK
Berorientasi Pelayanan Akuntabel Kompeten Harmonis Loyal Adaptif Kolaboratif

ERADICATION

2

Menghapus autostart process yang mencurigakan dari hasil analisa aplikasi autostart.

3

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

PEMULIHAN

PROSES

1. Melakukan dekripsi file yang terkena dampak dengan menggunakan decryption tools yang tersedia

2. 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.

3. 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.

PEMULIHAN

4

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.

5

Melakukan update/patching sistem

6

Melakukan update/patching antivirus.

DISKOMINFO BATAM

TINDAK LANJUT

PROSEDUR

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

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

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

TINDAK LANJUT

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

Melakukan penyempurnaan prosedur penanganan insiden berdasarkan insiden yang terjadi.

DISKOMINFO BATAM

G20 INDONESIA 2022

BerAKHLAK
Berorientasi Pelayanan Akuntabel Kompeten Harmonis Loyal Adaptif Kolaboratif

PANDUAN PENANGANAN
INSIDEN RANSOMWARE

Dinas Komunikasi dan Informatika Kota Batam