PEMERINTAH KOTA BANJARBARU

BUKU PANDUAN DUNIA CYBER

SIAGA DAN CERMAT

diskominfo KOTA BANJARBARU

Telp/Fax.(0511)6749126 kominfobjb@banjarbarukota.go.id Diskominfo Kota Banjarbaru DiskominfoBanjarbaru banjarbaru.tv diskominfo.banjarbarukota.go.id

KATA PENGANTAR

Selamat membuka buku panduan "Dunia Siber" Buku ini adalah kompas yang akan membimbing Anda melalui kerumitan dunia digital yang terus berkembang. Dalam zaman di mana teknologi mendefinisikan kehidupan kita, penting bagi kita untuk memahami, mengendalikan, dan memanfaatkan dengan bijak kecanggihan yang tersedia.

Buku ini mengajak Anda untuk menjelajahi berbagai aspek dunia siber, termasuk keamanan, privasi, etika digital, dan literasi informasi. Dengan pengetahuan yang didapat dari buku ini, Anda akan dapat menjalani kehidupan online dengan lebih cerdas, aman, dan bertanggung jawab.

Mari bersama-sama membangun kesadaran dan keterampilan untuk menghadapi dunia siber dengan penuh keyakinan dan pemahaman. Selamat membaca dan semoga buku ini membantu Anda memahami dan meraih manfaat penuh dari era digital yang begitu dinamis ini.

Ditandatangani secara elektronik oleh :
Kepala Dinas Komunikasi dan Informatika
Kota Banjarbaru

ASEP SAPUTRA, S.Kom, MM
Pembina Tingkat I
NIP. 19770909 200604 1 006

DAFTAR ISI

Apa Sih Tanda Tangan Elektronik Itu ?

Tanda Tangan Elektronik adalah tanda tangan yang terdiri atas Informasi Elektronik yang dilekatkan , terasosiasi atau terkait dengan Informasi Elektronik lainnya yang digunakan sebagai alat verifikasi dan autentikasi.
(UU ITE No. 11 Tahun 2008)

Berdasarkan PPSTE Pasal 60 Ayat 2
TTE itu dibagi jadi 2 jenis

Tersertifikasi

TTE tersertifikasi dibuat menggunakan Sertifikat Elektronik dari PSrE yang terdaftar di Kominfo.

Tidak Tersertifikasi

TTE tidak tersertifikasi merupakan TTe yang dibuat tanpa menggunakan jasa PSrEyang sudah diakui oleh Kominfo.

Apa Saja Sih Dokumen yang Bisa di- TTE?

Semua Dokumen Bisa di-TTE Lohh.....!!

Kecuali...

Surat yang menurut undang-undang harus dibuat dalam bentuk tertulis.

Surat beserta dokumennya yang menurut undang-undang harus dibuat dalam bentuk akta notaril atau akta yang dibuat oleh pejabat pembuat akta.

Format Dokumen Apa Saja yang Bisa di-TTE?

Semua format dokumen bisa di-TTE loh...
Seperti PDF, .doc, .docx, .xls, .jpg, .png, .gif, .mp3, .exe dan masih banyak lagi....

TAPIII.....!!!
Kalau kalian TTE menggunakan aplikasi BSrE seperti BeSign dan Panter hanya bisa TTE dengan format file **PDF** saja....

Kenapa Gitu Ya Sob?

Karena dokumen dengan format PDF memiliki beberapa keunggulan dibandingkan format lainnya, yaitu :

- Dapat dibuka dan ditampilkan secara konsisten di berbagai perangkat.
- Dapat memuat berbagai konten.
- Memungkinkan kompresi data , sehingga ukuran file dapat menjadi lebih kecil.
- Memungkinkan pengguna untuk melakukan pencarian teks di dalam dokumen.

Kenapa Pakai Tanda tangan Elektronik?

1. Dapat dilakukan dimana pun dan kapan pun
2. Pengambilan keputusan lebih cepat
3. Sah di mata hukum
4. Hemat sumber daya dan waktu
5. Meminimalisir penggunaan kertas
6. Tidak bisa dipalsukan
7. Mengurangi praktik korupsi

3 Aplikasi Untuk
Tanda Tangan Elektronik

BeSign

Panter

Website :
http:/tte.kominfo.go.id/verifyPDF

Panduan Pelaporan Insiden Siber

1. Laporan Insiden Siber

Pelapor yang dalam hal ini pengelola IT yang terkena insiden ataupun pengguna yang menemukan adanya insiden, dapat dilakukan melalui alamat email pusopskamsinas@bssn.go.id atau bantuan70@bssn.go.id atau dapat menghubungi via telepon di (021)78833610. Pelapor dapat melampirkan bukti insiden, berupa screenshot insiden.

2. Verifikasi Insiden Siber

Berdasarkan laporan insiden siber tersebut, Pusopskamsinas akan melakukan verifikasi insiden tersebut. Tahap verifikasi dilakukan dengan cara pihak pengelola website tersebut mengisi data-data lengkap seperti identitas lengkap pengelola website, jenis insiden, sistem log aplikasi, dan dampak terkait insiden tersebut.

Tujuan dari tahap Verifikasi ini adalah melakukan identifikasi dari insiden yang terjadi dan melakukan dokumentasi terhadap insiden tersebut.

3. Approvement

Laporan insiden siber yang telah diverifikasi akan dilakukan approvement guna untuk penanganan insiden selanjutnya. Approvement dilakukan oleh pimpinan pada Pusopskamsinas.

4. Open Ticket

Setelah dilakukan verifikasi dan dinyatakan valid, maka akan diberlakukan sistem *open ticket*. Tiket tersebut berisi informasi mengenai nomor tiket insiden dan informasi terkait penanganan insiden. Tiket yang telah dibuat, nantinya akan dilanjutkan ke tim *Response Incident* BSSN.

Tiket ini bertujuan untuk melakukan manajemen laporan insiden dan dapat sebagai monitoring pelapor insiden terkait sejauh mana insiden tersebut ditangani oleh BSSN.

5. Respon Insiden

Tim respon insiden akan melakukan koordinasi dengan pihak pengelola IT terkait dengan tiket tersebut. Tim respon insiden akan memberikan panduan terkait mekanisme penanggulangan dan pemulihan website tersebut. Jika diperlukan penanganan khusus, maka tim dapat melakukan penanggulangan dan pemulihan website tersebut secara on-site. Pada tahapan ini, akan dihasilkan berupa rekomendasi penanggulangan dan pemulihan terkait insiden yang terjadi.

6. Close Ticket

Selanjutnya, pihak pengelola website dapat melakukan penanggulangan dan pemulihan sesuai dengan rekomendasi yang telah diberikan. Tim akan melakukan pantauan terhadap website yang terkena insiden tersebut. Jika insiden telah dapat diatasi, maka akan dilakukan Close Ticket

Panduan Penanganan Insiden SERANGAN PHISING

1. Persiapan

Tujuan tahap persiapan pada penanganan serangan *phishing* adalah untuk membangun kontak, menentukan prosedur dan mengumpulkan informasi serangan. Tahap persiapan penanganan serangan *phishing*, dilakukan dengan prosedur sebagai berikut:

a) Membuat daftar semua domain sah yang dimiliki organisasi.
b) Mempersiapkan satu buah halaman website untuk memperingatkan pengguna tentang terjadinya serangan *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 :
- Tidak mengklik *link* yang mencurigakan
- Tidak memasukan *username* dan *password* pada situs web yang alamat web nya meragukan.
- Merubah penulisan alamat *email* yang dipublish, dari bentuk @ menjadi “at” atau dalam bentuk gambar, untuk menghindari menjadi target *email phising*.
- Menggunakan *Anti Virus* yang memiliki fitur Anti *Phising*.

2. Identifikasi

Tujuan dari proses identifikasi adalah untuk mendeteksi adanya insiden serangan phising, menentukan ruang lingkup, dan melibatkan pihak-pihak yang tepat dalam menangani serangan phising. Tahap identifikasi penanganan serangan phishing adalah sebagai berikut:

a) Memonitor 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. Agar bisa segera dilakukan takedown terhadap web phising. Seperti perusahaan hosting, penyedia domain, penyedia jasa email, Nasional CERT.
d. Mengumpulkan bukti bukti terkait adanya serangan phising. Contohnya screenshot halaman web yang terdampak.

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 spamreporting 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. Pemulihan

Pemulihan merupakan tahap untuk mengembalikan seluruh sistem bekerja normal seperti semula. Prosedur yang dapat dilakukan sebagai berikut:

a. Memastikan bahwa halaman website penipuan sudah tidak dapat diakses;
b. Tetap Memantau URL palsu, untuk memastikan URL palsu tersebut tidak dapat diakses;
c. Menghapus halaman peringatan dari website.

6. Tindak Lanjut

Tahap ini adalah fase di mana semua dokumentasi kegiatan yang dilakukan dicatat sebagai referensi untuk di masa mendatang. Tujuan dari tahap ini adalah untuk:

a. Pelaporan, membuat laporan mengenai langkah-langkah dan hasil yang telah didapatkan pada penanganan serangan phising;
b. Mengambil pelajaran dan membuat rekomendasi untuk mencegah terjadi lagi.

Prosedur yang dapat dilakukan adalah sebagai berikut:

a. Menyempurnakan langkah-langkah respon, prosedur penanganan serangan yang diambil selama 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 hokum;
d. Membuat dokumentasi dan laporan terkait penanganan serangan Phising;
e. Membuat evaluasi dan rekomendasi

Panduan Penanganan Insiden RANSOMWARE

Penanganan terhadap insiden Ransomware dapat dilakukandalam beberapa tahap seperti pada gambar berikut:

1. Persiapan

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 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

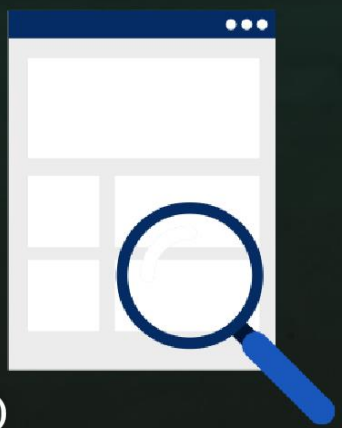
a) Evidence Collection

- *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.html

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

c) 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/installationguide/virtual-machine.html)



d) Ransomware Decryptor URL

- **Nomoreransom** : (https://nomoreransom.org)
- **Emsisoft** : (https://blog.emsisoft.com)

e) Malware Analysis

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

2. Identifikasi 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. Containment (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.*

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.

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.

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.

Panduan Penanganan Serangan *SQL INJECTION*

Penanganan serangan *SQL Injection* ditujukan utukmencapai hal-hal sebagai berikut:

a. Mengumpulkan informasi sebanyak mungkin tentang serangan *SQL Injection.*
b. Menghalangi atau mencegah eskalasi kerusakan yang disebabkan oleh serangan tersebut.
c. Mengumpulkan bukti terkait serangan *SQL Injection.*
d. Mengambil langkah-langkah proaktif untuk mengurangi kemungkinan terjadinya serangan SQL Injection di masa depan.

Supaya tujuan di atas dapat terlaksana dengan baik, maka penanganan terhadapserangan *SQL Injection* dilakukan dalam beberapa tahap sebagai berikut:

1. Persiapan

Dalam melakukan penanganan serangan *SQL Injection*, perlu adanya tahappersiapan dengan prosedur sebagai berikut :

a) Pembentukan tim respon. Tim dapat berasal dari institusi yang mengalami serangan (internal) atau juga bisa berasal dari luar institusi (eksternal) jika memang diperlukan. Anggota tim memiliki pengetahuan tentang *SQL Injection* dan memiliki kemampuan penanganannya.
b) Menyiapkan dokumen yang dibutuhkan dalam proses penanganan serangan *SQL Injection*. Dokumen ini antara lain adalah :
   - Panduan penanganan insiden serangan siber;
   - Formulir penanganan insiden serangan siber;
   - Diagram yang menggambarkan hubungan antar komponen-komponen

   aplikasi yang membangun website (web server, aplikasi web, daftar user, diagram network).
c) Menyiapkan tool dan media yang dibutuhkan untuk penanganan. Misalnya Notepad ++ untuk membaca log, IDS/IPS, SQL Map, Accunetix /Nessus.

2. Identifikasi dan Analisis

Tujuan dari proses identifikasi dan analis adalah:
a. Memahami sifat dan ruang lingkup kejadian;
b. Mengumpulkan informasi yang cukup tentang serangan *SQL Injection* sehingga

tim respon dapat memprioritaskan langkah selanjutnya dalam menangani serangan tersebut, yang biasanya diikuti dengan penahanan sistem.

Pada tahap ini dilakukan proses identifikasi untuk memastikan telah terjadi serangan *SQL Injection* dan mendeteksi sumbernya. Langkah-langkah yang dapat diambil pada tahap identifikasi dan analisis antara lain:
a. Memeriksa alert dan anomalies dari perangkat IDS atau IPS;
b. Melakukan error checking melalui form atau url dengan memberikan karakter atau sebuah simbol. Misalnya :

• Melalui form login, memasukan pada username dan password berupa karakter-karakter yang digunakan SQL Injection, seperti:

OR 1=1 –
OR 1=2 --
OR 'a'='a'

• Melalui url, menambahkan karakter-karakter yang digunakan SQL Injection, seperti single quote, double minus.

c. Memeriksa semua log (error log, access log, database log, firewall log). Lokasi log file secara default berada pada var/log, log tersebut menyimpan seluruh aktivitas yang terjadi pada sistem.
d. Memeriksa adanya command line, string-string yang digunakan untuk menyerang.
e. Memeriksa isi database untuk mencari script yang berbahaya, dan mengecek apakah ada penambahan user secara tidak sah.
f. Memeriksa apakah ada file atau script berbahaya (trojan, malicious file, backdoor) yang ditanamkan pada web server.
g. Menggunakan tool untuk memeriksa kerentanan. Tool yang dapat digunakan diantaranya Acunetix, SQLMap, SQL Injection tools.

Mengukur dampak dari terjadinya SQL Injection adalah
a. Terhadap kelangsungan proses bisnis, indikatornya adalah seberapa besar dari fungsi-fungsi bisnis yang terdapat pada website mengalami gangguan.
b. Terhadap sistem dan informasi, apakah penyerang melakukan distribusi malware, membuat backdoor atau melakukan web defacement. Selain itu, apakah ada data dan informasi yang berubah atau terhapus.

3. Containment

Setelah dipastikan bahwa memang benar telah terjadi serangan SQL Injection, maka dilakukan proses berikutnya dengan tujuan:

1. Tidak terjadi kerusakan lebih dalam.
2. Mencegah penyerang masuk lebih dalam ke sistem yang terkena dampak.
3. Melindungi server-server lain yang terhubung dengan aplikasi web.

Prosedur yang dilakukan pada tahap ini adalah:

a. Melakukan proses backup semua data yang terdapat pada web server. untuk keperluan forensik dan pengumpulan bukti-bukti. Backup sebaiknya ditempatkanpada hard disk eksternal

b. Jika sumber penyerangan berasal dari sistem lain pada jaringan, maka putuskan secara fisik koneksi tersebut dan lakukan investigasi sumber tersebut.

4. Eradication

Tahap Eradication pada penanganan serangan SQL Injection adalah untuk menghapus file /script serta menutup sumber serangan. Prosedur untuk melakukan proses ini dapat dilakukan dengan cara berikut:

a. Memeriksa apakah terdapat malicious file, backdoor, rootkit atau kode-kode berbahaya lainnya yang berhasil ditanamkan pada server dan segera menghapusnya.

b. Jika terdapat kode SQL yang mengakses IP tertentu maka perlu melakukan block /menutup sumber serangan (block IP dan Port).

5. Pemulihan

Pemulihan merupakan tahap untuk mengembalikan seluruh sistem bekerjanormal seperti semula. Prosedur yang dapat dilakukan sebagai berikut:

a. Mengubah kredential password pengguna. Hal ini untuk mengantisipasi apabila password pengguna telah diketahui oleh penyerang.

b. Melakukan recovery database pada aplikasi web.

c. Jika SQL Injection menyebabkan web defacement, gunakan panduan penangananinsiden web defacement.

d. Jika SQL Injection menyebabkan insiden malware, gunakan panduan penangananinsiden malware;

e. Menutup semua kerentanan yang telah diketahui.

f. Membatasi akses root langsung ke database.

g. Melakukan filter terhadap input yang dimasukkan oleh pengguna.

h. Mematikan atau menyembunyikan pesan-pesan error yang keluar dari SQLServer yang berjalan.

i. Patching terhadap aplikasi yang rentan, melakukan upgrade terhadap aplikasi web yang masih memiliki kerentanan.

j. Melakukan penetration testing untuk mengetahui celah-celah keamanan yangmungkin masih terdapat pada website.

6. Tindak Lanjut

Tahap ini adalah fase di mana semua dokumentasi kegiatan yang dilakukan dicatat sebagai referensi untuk di masa mendatang. Tujuan dari tahap ini adalah untuk :

a. Pelaporan, membuat laporan mengenai langkah-langkah dan hasil yang telah didapatkan pada penanganan serangan SQL Injection.

b. Mengambil pelajaran dan membuat rekomendasi untuk mencegah terjadi lagi.Prosedur yang dapat dilakukan adalah sebagai berikut:

a. Membuat dokumentasi dan laporan terkait penanganan serangan SQL Injection.

b. Menuliskan tools apa saja yang digunakan dalam penanganan serangan injeksisql.

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

d. Memberikan analisa dan penjelasan apa yang harus dilakukan sehinggaserangan serupa tidak terulang kembali.

e. Membuat evaluasi dan rekomendasi.

Panduan Penanganan Serangan *DISTRIBUTED DENIAL OF SERVICE (DDoS)*

PROSEDUR PENANGANAN SERANGAN DDoS

Serangan DDoS pada prinsipnya sama seperti serangan DoS, akan tetapi trafik serangan DDoS yang dikirim berasal dari berbagai sumber yang berbeda. Oleh karena itu, dalam penanganan serangan DDoS perlu melibatkan Internet Service Provider (ISP). Penanganan terhadap serangan DDoS dilakukan dalam beberapa tahap sebagai berikut:

1. Tahap Persiapan

Tujuan tahap persiapan pada penanganan serangan DDoS adalah untuk membangun kontak dan mempersiapkan sumber daya yang dibutuhkan untuk penanganan serangan DDoS.

Tahap persiapan penanganan serangan DDoS, dilakukan dengan prosedur sebagai berikut:

a) Pembentukan tim respon. Tim dapat berasal dari institusi yang mengalami serangan (internal) atau juga bisa berasal dari luar institusi (eksternal) jika memang diperlukan. Anggota tim memiliki pengetahuan tentang DDoS dan memiliki kemampuan penanganannya.
b) Membangun kontak dengan ISP. Menentukan metode koordinasi dan komunikasi antara tim, penanggung jawab server, ISP dan pihak terkait. Kapan koordinasi harus dilakukan, dan melalui media komunikasi apa yang akan digunakan, misalkan telepon dan email.
c) Menyiapkan dokumen yang dibutuhkan dalam proses penanganan serangan DDoS. Dokumen ini antara lain adalah :
   - Panduan penanganan insiden siber
   - Formulir penanganan insiden siber
   - Dokumen yang berisi daftar dari alamat IP yang diprioritaskan untuk diperbolehkan melewati jaringan selama penanganan
   - Dokumen topologi jaringan, termasuk semua alamat IP yang paling up to date.
   - Dokumen Baseline Performance.
d) Menyiapkan tools yang diperlukan dalam proses penanganan, antara lain:
   - Perangkat Analisa Jaringan, misalnya wireshark, kfsensor, dll.
   - Perangkat Analisa Log, misalnya Notepad++/EmEditor, dll.
e) Mempersiapkan desain jaringan dengan menggunakan redundan di sisi perangkat, server, dan interkoneksi.
f) Melakukan backup secara berkala.

2. Identifikasi dan Analisis

Tujuan dari proses identifikasi adalah:

a. Memahami sifat dan ruang lingkup serangan.
b. Mengumpulkan informasi yang cukup tentang serangan sehingga tim respon dapat memprioritaskan langkah selanjutnya dalam menangani serangan tersebut. Kemampuan untuk mengidentifikasi dan memahami sifat dari serangan dan target akan membantu dalam proses containment dan pemulihan.

Langkah-langkah yang dapat diambil pada tahap identifikasi dan analisis antara lain :

a. Mengetahui perilaku "normal" dari lalu lintas jaringan, penggunaan CPU, penggunaan memori dari host, sehingga alat monitoring jaringan akan memberikan informasi berupa peringatan terhadap perubahan abnormal. Beberapa indikasi bahwa telah terjadi serangan DDoS 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.
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 atau penyedia hosting).
d. Memeriksa lalu lintas jaringan, seperti source IP address, destination port, URLs, protocol, TCP sysnc, UDP, ICMP dan traffic Netflow misalnya menggunakan tcpdump, wireshark, snort dan membandingkannya 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 yang terkena dampak) untuk mengetahui jenis serangan, sumber serangan, apa yang menjadi sasaran, dan bagaimana masuknya serangan.
f. Menentukan dampak dari tingkat keparahan yang terjadi, yaitu seberapa besar sistem dan layanan mengalami gangguan, serta kemungkinan motif yang dilakukan oleh penyerang.

3. Containment

Tahap containment bertujuan untuk meminimalisir efek/dampak serangan pada sistem yang ditargetkan dan mencegah kerusakan lebih lanjut. Prosedur yang 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 sementara aplikasi tersebut.
b. Jika bottleneck 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, dll).
e. Mengontrol lalu lintas data dengan menghentikan koneksi atau proses yang tidak diinginkan pada server/router.
f. Melakukan filter sesuai karakteristik serangan, misalnya memblokir paket echo ICMP.
g. Menerapkan rate limiting untuk protokol tertentu, mengijinkan dan membatasi jumlah paket per detik untuk protokol tertentu dalam mengakses suatu host.

4. Eradication

Eradication pada penanganan serangan DDoS yaitu mengambil tindakan untuk menghentikan kondisi denial of service. Tindakan ini sebagaian besar melibatkan peran ISP.

Prosedur untuk melakukan proses ini dapat dilakukan dengan cara menghubungi penyedia layanan internet (ISP) untuk meminta bantuan, terkait :

- Pemblokiran jaringan (source IP address)
- Pemfilteran (membatasi jumlah lalu lintas)
- Traffic-scrubbing/shinkhole/clean-pipe
- Blackhole routing

5. Pemulihan

Pemulihan merupakan tahap untuk mengembalikan seluruh sistem bekerja normal seperti 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 DDoS pada jaringan telah selesai dan layanan bisa dilakukan kembali.
b. Memastikan bahwa jaringan telah kembali ke kinerja semula
c. Memastikan bahwa layanan yang terkena dampak dapat dijangkau lagi/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 kembali lalu lintas ke jaringan asli.

6. Tindak Lanjut

Tahap ini adalah fase di mana semua dokumentasi kegiatan yang dilakukan dicatat sebagai referensi untuk di masa mendatang. Tujuan dari tahap ini adalah untuk:

a. Pelaporan, membuat laporan mengenai langkah-langkah dan hasil yang telah didapatkan pada penanganan serangan DDoS.
b. Mengambil pelajaran dan membuat rekomendasi untuk mencegah terjadi lagi.

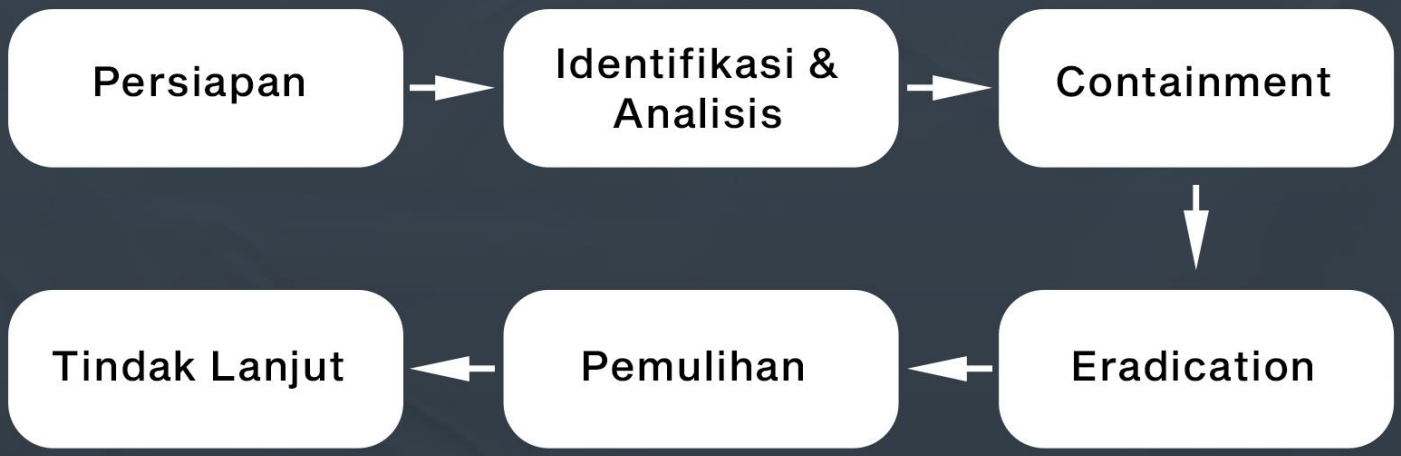
Prosedur yang dapat dilakukan adalah sebagai berikut:

a. Membuat dokumentasi dan laporan terkait penanganan serangan DDoS, yang berisi langkah-langkah dan hasil yang telah didapatkan pada penanganan serangan DDoS. Mendokumentasikan dampak dan biaya dari terjadinya serangan tersebut.
b. Evaluasi efektivitas respon
c. Menyempurnakan langkah-langkah respon, prosedur penanganan serangan yang diambil selama insiden
d. Mencatat tools apa saja yang digunakan dalam penanganan.
e. Mendokumentasikan bukti-bukti yang ditemukan, hal ini terkait dengan proses hukum kedepannya.
f. Memberikan analisa dan penjelasan apa yang harus dilakukan sehingga serangan serupa tidak terulang kembali.
g. Membuat evaluasi dan rekomendasi.

Pedoman Penanganan Insiden Malicious Software (MALWARE)

PROSEDUR PENANGANAN INSIDEN MALWARE

Penanganan terhadap insiden malware dapat dilakukan dalam beberapa tahap seperti pada gambar 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 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 Legal***
Menyiapkan dokumen yang dibutuhkan dalam proses penanganan insiden malware. Dokumen ini antara lain:
- Panduan Penanganan Insiden Siber
- Formulir Penanganan Insiden Siber
- Dokumen Kebijakan, diantaranya kebijakan keamanan, kebijakan pengunaan laptop, antivirus, internet dan email, serta kebijakan backup.
- Dokumen Baseline Performance.
- Dokumen Audit Sistem.
- Dokumen Profil dari semua perangkat lunak dan proses-proses yang harus berjalan pada sistem berdasarkan proses bisnis organisasi.
- Database penanganan insiden yang pernah terjadi sebelumnya.
- 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 agar dampak malware tidak menyebar ke sistem yang lain.***

e) ***Menyiapkan tools yang akan digunakan, diantaranya:***
- 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.
- Tools untuk menghitung nilai hash.
- Tools untuk deteksi virus baik berbasis host maupun online, misalnya antivirus dan website www.virustotal.com
- Tools pendeteksi berbasis host, misalnya Samhain, OSSEC dan Osiris.
- Tools untuk analisa malware, meliputi : *(halaman berikutnya)*

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 analisa dinamis.
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. *(halaman berikutnya)*

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 yang bertujuan untuk mengidentifikasi sistem lebih mendetail. Beberapa Aplikasi SysInternal tools yang paling banyak digunakan untuk melakukan identifikasi dan analisa malware adalah Process Explorer, Autoruns, dan Process Monitor.

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. Namun, perlu menyimpan informasi koneksi jaringan pada sistem sebelum
c. 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.
- 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 :

i. Tidak melakukan kill / end process terhadap malicious process tersebut. Hal ini dikarenakan malware akan melakukan autostart process ketika prosesnya terhenti.
ii. Lakukan suspend terhadap proses tersebut, kemudian lakukan record pada path EXE proses tersebut dan file DLL yang dipanggil oleh proses tersebut.
iii. Dalam kondisi sleep (proses di suspend), kemudian satu persatu lakukan kill process dari kumpulan malicious process tersebut dimulai dari child process ke parent process.
iv. 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 :

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

ii. Live usb tersebut dapat berupa sistem operasi 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 mounting sistem operasi yang terinfeksi ke dalam Live usb yang sedang berjalan.

iii. Lakukan proses scanning antivirus dan antimalware 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 ada aplikasi 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 :

i. Memantau proses dan servis yang berjalan menggunakan Process Monitor dan Process Explorer.

ii. 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 malware yang memiliki kemampuan Command and Control biasanya melakukan kontak dengan induknya.

c. 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.
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 untuk masa mendatang. Prosedur yang dapat dilakukan adalah sebagai berikut:

a. Membuat dokumentasi dan laporan terkait penanganan 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:
    - Penambahan pengetahuan tentang penanganan insiden malware, misalnya melalui pelatihan
    - Memperbaharui anti malware dengan signature file yang baru, dengan harapan dapat berhasil dalam mendeteksi dan menghapus malware
    - Meningkatkan pertahanan sistem terhadap malware
e. Mendokumentasikan malware terkait jalan masuk, perilaku, dampak kerusakan, dll yang terkait malware ke dalam database malware.
f. Menyempurnakan langkah-langkah respon atau prosedur penanganan insiden malware yang ada.

Panduan Penanganan Insiden WEB DEFACEMENT

1. Persiapan

Dalam melakukan penanganan insiden, perlu dilakukannya tahapan persiapan yang bertujuan untuk mempersiapkan segala sesuatu yang dibutuhkan pada saat penanganan insiden web defacement. Adapun prosedur sebagai berikut :

a) Pembentukan tim penanganan insiden perlu dilakukan baik ber asal dari institusi yang mengalami insiden (internal) atau juga bisa berasal dari luarinstitusi (eksternal) jika memang sangat diperlukan;

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

c) 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

d) Menyimpan bukti insiden antara lain screenshot insiden web defacement,log server ataupun log perangkat pendukung server. Jika menemukan fileyang mencurigakan dapat dilakukan pendokumentasian file tersebut. Untuk kegiatan forensik, dapat juga dilakukan proses imaging baik seluruh storage server ataupun memori (RAM) yang digunakan.
e) Menentukan tempat (ruangan) untuk menangani insiden baik kegiatan rapat tim maupun kegiatan analisis insiden.
f) Menyiapkan tool dan media yang dibutuhkan untuk menangani insiden. Tools yang dapat disiapkan antara lain Scanning Tools, Forensic Tools, 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 dapat diketahui sumber serangannya. Selain itu jugauntuk mengumpulkan informasi yang cukup tentang insiden tersebut sehinggatim 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 halamanweb (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, biasanyauntuk 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 loginuntuk user, periksa history;
h) Dalam melakukan tahapan ini, tools yang dapat digunakan antara lain : NMap, Nikto, Accunetic, Nessus.

3. Mitigasi

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

a) Perlu dilakukan pembangunan website sementara agar publikasi informasipada website tetap berjalan. Atau dapat juga dilakukan pembangunan siteunder 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. Penghapusan Konten

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. Pemulihan

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 checksumsebagai 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 yangdibutuhkan pada proses incident handling yang telah dilakukan.
d) Menuliskan tools apa saja yang digunakan dalam membatu prosesincidenthandling.
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.

Modus Penipuan Terbaru :

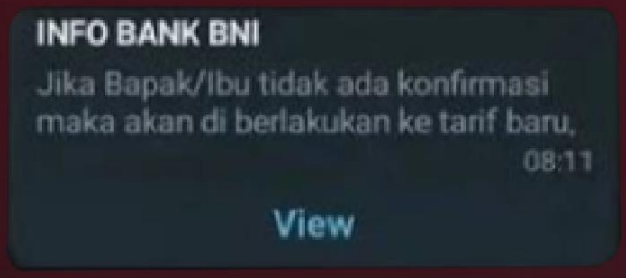
Pakai Button “View”

Modus Phising Terbaru Muncul Lagi!

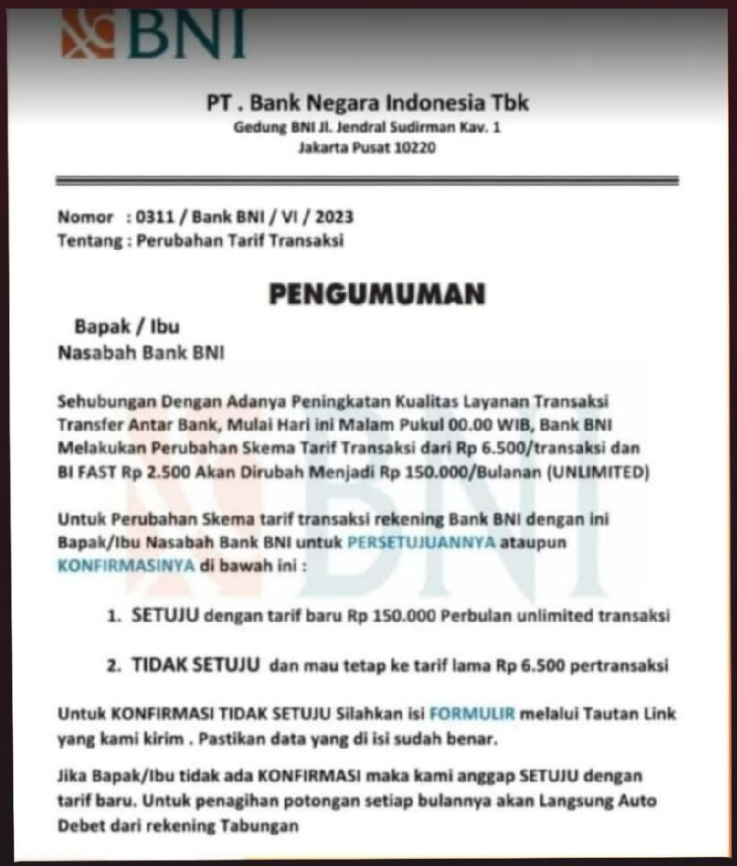
Penipuan ini mengatasnamakan **Bank Negara Indonesia (BNI)** dimana penipu mengirimkan pesan WhatsApp dilengkapi action button "View" atau "Lihat" dimana di dalamnya berisi link yang jika di klik bisa mengarahkan korban ke malicious website.

Gini Cara Kerja Phising

Berdasarkan pakar keamanan siber dari Vaksincom, Alfons Tanujaya



Korban klik tombol "View" atau "Lihat"



BNI

PT . Bank Negara Indonesia Tbk
Gedung BNI Jl. Jendral Sudirman Kav. 1
Jakarta Pusat 10220

Nomor : 0311 / Bank BNI / VI / 2023
Tentang : Perubahan Tarif Transaksi

PENGUMUMAN

Bapak / Ibu
Nasabah Bank BNI

Sehubungan Dengan Adanya Peningkatan Kualitas Layanan Transaksi Transfer Antar Bank, Mulai Hari ini Malam Pukul 00.00 WIB, Bank BNI Melakukan Perubahan Skema Tarif Transaksi dari Rp 6.500/transaksi dan BI FAST Rp 2.500 Akan Dirubah Menjadi Rp 150.000/Bulanan (UNLIMITED)

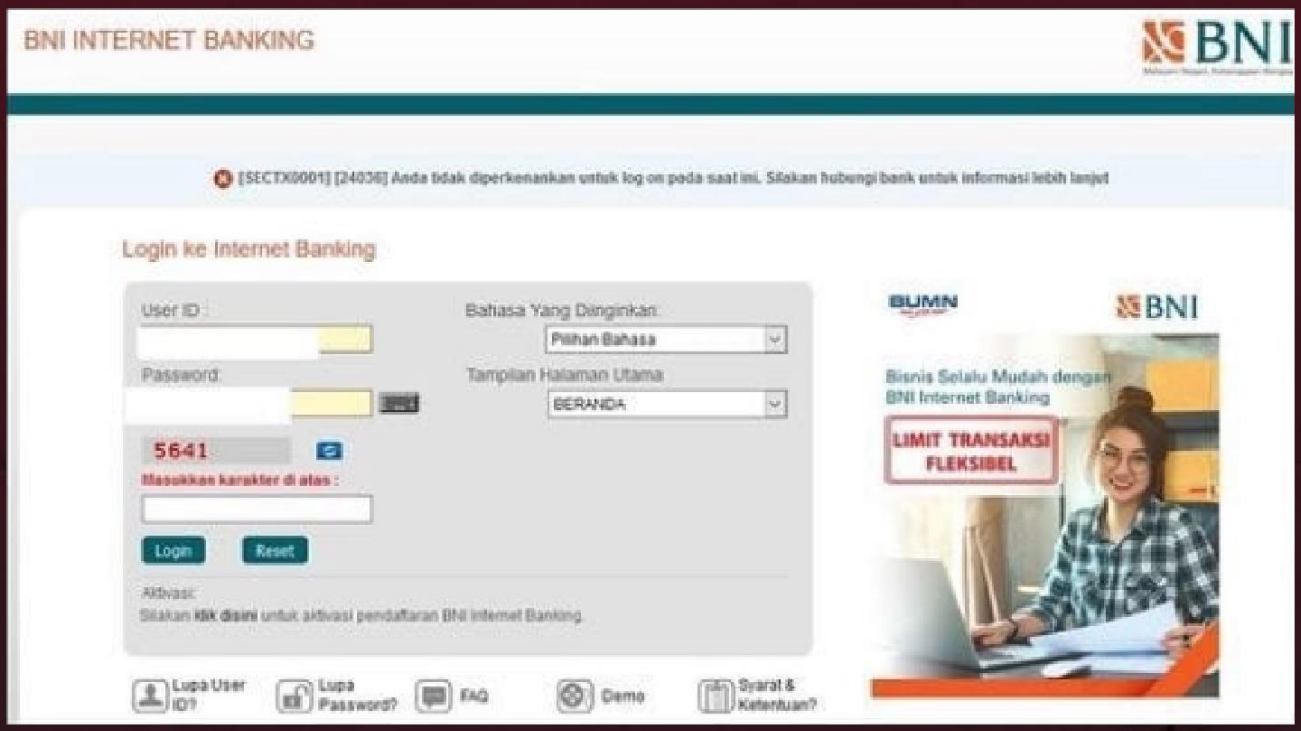
Untuk Perubahan Skema tarif transaksi rekening Bank BNI dengan ini Bapak/Ibu Nasabah Bank BNI untuk PERSETUJUANNYA ataupun KONFIRMASINYA di bawah ini :

1. SETUJU dengan tarif baru Rp 150.000 Perbulan unlimited transaksi
2. TIDAK SETUJU dan mau tetap ke tarif lama Rp 6.500 pertransaksi

Untuk KONFIRMASI TIDAK SETUJU Silahkan isi FORMULIR melalui Tautan Link yang kami kirim . Pastikan data yang di isi sudah benar.

Jika Bapak/Ibu tidak ada KONFIRMASI maka kami anggap SETUJU dengan tarif baru. Untuk penagihan potongan setiap bulannya akan Langsung Auto Debet dari rekening Tabungan

Halaman WhatsApp akan menampilkan surat yang berisi informasi perubahan tarif transaksi antarbank yakni dari Rp 6.500 per transaksi menjadi Rp 150.000 per bulan untuk bebas biaya transfer.



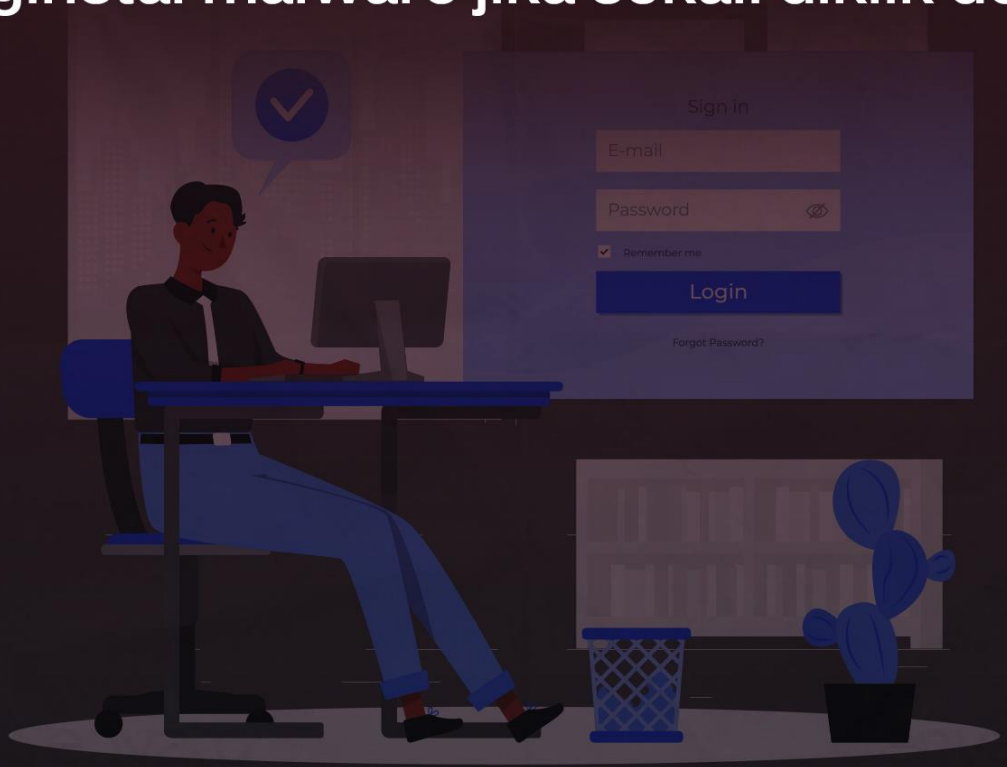
Korban akan diarahkan untuk klik link phising berkedok bank dan meminta kredensial m-banking serta OTP (One -Time Password).

Jangan Sampai
Saldo Terkuras !!

Dari link tersebut ketika akan dimintai beberapa data yang perlu diisi . Jika kalian isi, saldo akan terkuras.

Jangan masukan data apapun agar AMAN!!

Penipuan Phising dengan tombol “View” atau “Lihat” ini berbeda dengan file APK yang bisa menginstal malware jika sekali diklik download.



Inilah Bahaya Pencurian Identitas Digital

Apa itu pencurian identitas?

Pencurian identitas adalah tindak kriminal dengan menggunakan identitas korban untuk melakukan aktivitas ilegal atau mendapatkan keuntungan finansial. Pencurian identitas dapat terjadi secara langsung melalui pencurian kartu identitas maupun secara siber melalui data breaching dan hacking.

Cara Mewaspadai Pencurian Identitas

- Bacalah statement bank, kartu kredit, dan asuransi kesehatan sesering mungkin untuk memastikan semua tagihan atau klaim sudah diketahui.
- Ketahui kapan jadwal tagihan masuk melalui tanggal jatuh tempo pembayaran.
- Rusak semua dokumen pembelian yang berisi informasi pribadi atau informasi keuangan kamu.
- Periksa askses aplikasi atau pihak ketiga terhadap smartphone, email dan akun media sosial kamu.

5 Cara Lindungi Data Pribadi di Medsos

Gunakan password dengan beragam karakter

Autentikasi dua faktor

Hapus informasi pribadi dari profil media sosial

Selalu pantau pengaturan keamanan di media sosial

Berhati-hatilah dengan email yang tidak dikenal

5 Jurus Menghindari Jebakan Scam & Situs Palsu

1 Cek URL situs

Website yang palsu memiliki nama URL yang tidak sama dengan aslinya, misalnya salah satu hurufnnya hilang atau diganti untuk mengecoh pengguna.

2 Periksa protokol HTTPS

Situs yang sah harus memiliki protokol HTTPS dalam alamat web dan bukan hanya http:/

3 Perhatikan susunan kalimat yang digunakan

Jika website menggunakan tata bahasa yang salah , frasa yang aneh , atau ada kata-kata yang hilang, kemungkinan itu situs scam.

4 Perhatikan iklan yang bermunculan (pop-up ads)

Jika website menggunakan tata bahasa yang salah , frasa yang aneh , atau ada kata-kata yang hilang, kemungkinan itu situs scam.

5 Verifikasi dengan pemilik situs

Kontak nomor telepon atau email pada situs untuk memverifikasi apakah situs itu kredibel atau tidak

KENALI MODUS PENIPUAN REKAYASA SOSIAL DI DUNIA SIBER AGAR TIDAK TERKECOH

Sosial engineering atau rekayasa sosial, adalah sebuah teknik manipulasi yang memanfaatkan kesalahan manusia untuk mendapatkan akses pada informasi pribadi atau data data berharga.

4 BENTUK SOSIAL ENGINEERING

Baiting
Serangan umpan dalam bentuk janji palsu memancing keserakahan dan keingintahuan korban.

Pretexting
Serangakian informasi menipulatif untuk meminta informasi sensitif dari korban dengan dalil tugas penting.

Phishing
Serangan *email* dan pesan teks untuk menciptaka urgensi, keingintahuan dan ketakutan korban dan memancing korban mengungkap informasi data pribadi atau membuka tautan berisi *malware.*

Spear Phishing
Seperti phishing namun dilakukan secara terstruktur dengan memilih individu atau lembaga tertentu, melakukan profilling dan menjaga kontak dalam waktu panjang untuk meraih kepercayaan.

PASSWORD

Dan Bagaimana Menjaganya

- Ubah password secara berkala minimal 3 bulan satu kali.
- Gunakanlah password dengan menggunakan kombinasi angka,huruf dan simbol.
- Jangan login akun anda di sembarang perangkat.
- Gunakanlah password yang berbeda untuk setiap akun yang anda gunakan.
- Berhati-hati ketika menggunakan WIFI publik.

Tips Bertransaksi Aman

Melalui Mobile Banking & Internet Banking

1. Gunakanlah aplikasi perbankan yang resmi
2. Jangan pernah gunakan fitur save password pada komputer
3. jaga rahasia id dan password anda, pihak bank tidak pernah meminta informasi ini
4. Gunakan fitur notifikasi e-mail dan SMS untuk memonitor aktifitas rekening
5. Gunakanlah antivirus yang resmi
6. Hapus history dan bersihkan cache ketika selesai melakukan transaksi

Cara Aman Menggunakan

WIFI PUBLIK

1. Menyambungkan Wifi secara manual
2. Hindari mengakses informasi sensitif
3. Perhatikan Nama Jaringan WiFi
4. Perhatikan HTTPS
5. Gunakan keamanan tambahan dan enkripsi kata sandi
6. Aktifkan firewall dan antivirus

LAKUKAN 3 HAL INI SEBELUM MEMBAGIKAN INFORMASI DI MEDIA SOSIAL

01 Cari tahu kebenaran informasi atau konten

02 Pelajari apakah informasi atau konten tersebut bermanfaat

03 Pikirkan apakah informasi atau konten pantas disebarluaskan

Mengenal Data Pribadi dan Jenisnya

01 Data Pribadi Umum

- Nama lengkap
- Jenis kelamin
- Kewarganegaraan
- Agama
- Data pribadi yang dikombinasikan untuk mengidentifikasi seseorang

02 Data Pribadi Spesifik

- Data informasi kesehatan
- Data biometrik
- Data genetika
- Kehidupan / orientasi seksual

03 Data Pribadi Spesifik

- Pandangan politik
- Catatan kejahatan
- Data anak
- Data keuangan pribadi
- Data lain sesuai peraturan perundang-undangan

Bicaralah Pada Anak Anda Tentang Pelecehan dan Intimidasi Siber (CYBERBULLYING)

Anjurkan anak untuk berani bercerita jika dirinya atau temannya mengalami pelecehan atau intimidasi.

Ajukan pertanyaan kepada anak dengan lemah lembut untuk mengetahui kondisi sebenarnya dan penyebabnya.

Ajari anak tentang dampak dari pelecehan atau intimidasi siber.

Anjurkan akan untuk berani memberikan dukungan kepada anak yang diganggu.

Terima kasih sudah membaca buku panduan pengamanan dari serangan siber! Sekarang, Anda adalah 'Ninja Siber' yang siap menghadapi ancaman digital.