PANDUAN PENANGANAN INSIDEN PHISING

MAHKAMAH AGUNG
COMPUTER SECURITY INCIDENT RESPONSE TEAM
[MA-CSIRT]

KATA PENGANTAR

Puji syukur kehadirat Allah SWT, 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 Phising". Panduan ini disusun dalam rangka memberikan acuan bagi pihak yang berkepentingan dalam penanganan insiden serangan Phising. Panduan ini berisikan langkah-langkah yang harus diambil apabila terjadi serangan Phising, 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 penduan ini.

Jakarta, Maret 2023

MA-CSIRT,

KEPALA MA-CSIRT

DAFTAR ISI

PANDUAN PENANGANAN INSIDEN SERANGAN PHISHING

1. PENDAHULUAN

Serangan *phising* adalah serangan yang dilakukan untuk menipu /memancing korban agar mau mengklik tautan serta menginput informasi kredential seperti *username* dan *password.* Cara kerja phising umumnya dilakukan melalui penggunaan *email* palsu mengatasnamakan *admin,* atau melalui situs web palsu yang sangat mirip dengan situs web yang asli.

2. TUJUAN

Secara umum, tujuan panduan ini dimaksudkan untuk membantu organisasi memahami tentang penanganan serangan *phishing.* Sedangkan secara khusus adalah sebagai berikut:

a) Melakukan pengumpulan informasi yang akurat;
b) Meminimalisir dampak dari serangan siber yang terjadi;
c) Mencegah adanya serangan lanjutan dan mencegah kerusakan agar tidak lebih meluas.

3. RUANG LINGKUP

Panduan ini berisi langkah-langkah yang harus diambil apabila terjadi serangan *phishing,* yang dimulai dari tahap persiapan sampai dengan tahap pembuatan laporan dari penanganan serangan. Panduan ini dapat dijadikan acuan bagi semua individu atau tim *(administrator,* pengelola TI, tim respon insiden keamanan komputer) yang bertanggung jawab untuk mencegah, mempersiapkan atau menangani serangan *phishing*.

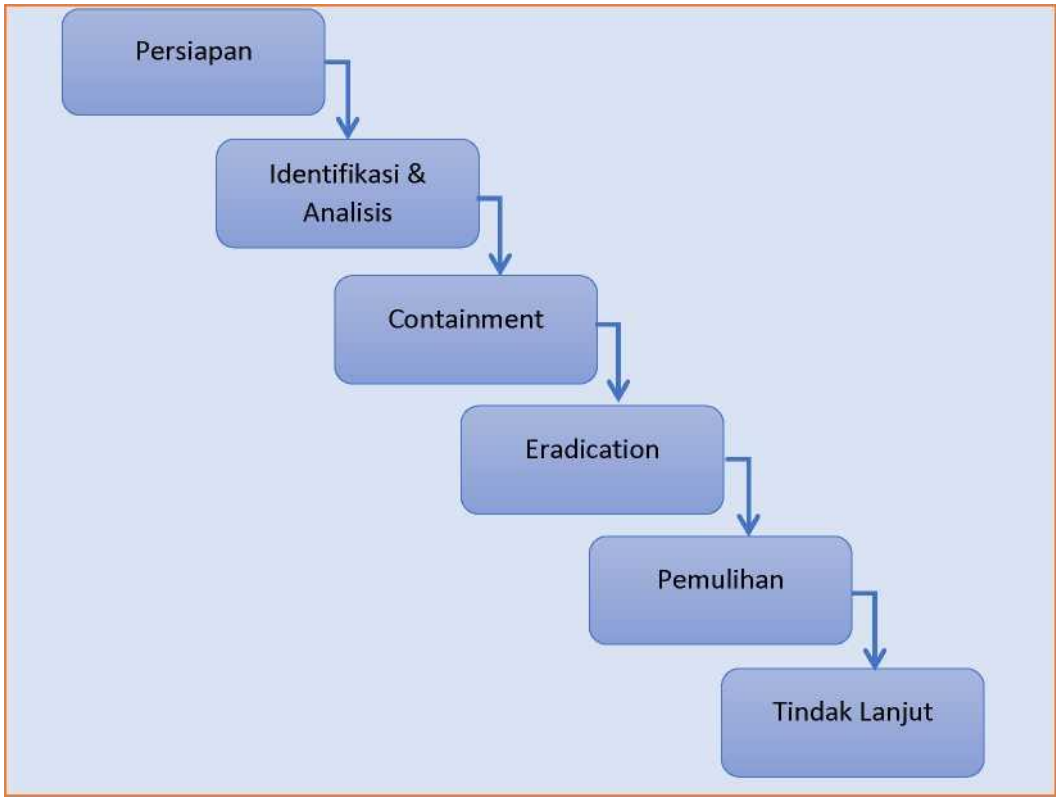
4. PROSEDUR PENANGANAN SERANGAN *PHISHING*

Penanganan serangan phishing ditujukan utuk mencapai hal-hal sebagai berikut:

a) Mengumpulkan informasi sebanyak mungkin tentang serangan *phishing*;

b) Menghalangi atau mencegah eskalasi kerusakan yang disebabkan oleh serangan tersebut;
c) Mengumpulkan bukti terkait serangan *phising*;
d) Mengambil langkah-langkah proaktif untuk mengurangi kemungkinan terjadinya serangan *phishing* di masa depan.

Supaya tujuan di atas dapat terlaksana dengan baik, maka penanganan terhadap serangan *phishing* dilakukan dalam beberapa tahap sebagai berikut:



Gambar 1. Tahap Penanganan Serangan Phising

4.1. 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. Membangun kontak dengan pihak-pihak terkait, seperti perusahaan *hosting*, penyedia domain, penyedia jasa *email*, asional CERT;

d) 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.*

4.2. 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 di lakukan *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.

4.3. 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".

4.4. 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.*

4.5. 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.*

4.6. 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.