DINAS PENGAMANAN DAN PERSANDIAN
SATUAN SIBER

STANDAR OPERASIONAL PROSEDUR
PENANGANAN INSIDEN SERANGAN *PHISHING*

TAHUN 2023

VERSI DOKUMEN

No	Tanggal	Versi Dokumen	Oleh	Keterangan
1.	November 2023	Versi 2.0	Satsiber Dispamsanau	

DAFTAR ISI

PROSEDUR PENANGANAN INSIDEN SERANGAN *PHISHING* DI LINGKUNGAN TNI AU

1. PENDAHULUAN

Perkembangan teknologi internet menjadikan dunia seakan-akan tidak memiliki batasan. Internet mampu menciptakan ruang atau dunia maya tersendiri yang terlihat jauh lebih aktif dari pada dunia nyata. Perkembangan dunia maya telah menciptakan berbagai macam fenomena siber. Keadaan ini menjadi titik rawan bahkan menjadi ancaman bagi negara karena bisa disalahgunakan oleh suatu pihak demi keuntungan pribadi maupun kelompok. Serangan siber adalah serangan pada sistem komputer atau jaringan komputer untuk mendapatkan kendali atau akses tanpa izin ke sistem komputer yang ditargetkan. Sementara kejahatan siber adalah aktivitas ilegal yang menggunakan dan menargetkan sistem atau jaringan komputer untuk menimbulkan kerugian materiil atau immateriil pada pihak yang menjadi target. Bagi korban korporasi, serangan siber dan kejahatan siber menyebabkan kerugian finasial, kerugian nilai pasar, tuntutan hukum, dan rusaknya reputasi. Bagi korban individu, kerugian dari serangan siber dan kejahatan siber menyebabkan dampak stres dan psikologis, pencurian identitas, dan kerugian finansial.

Serangan *phising* adalah serangan siber yang dilakukan untuk menipu/memancing korban agar mau mengklik link/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.

Agar penanganan serangan *phising* dapat dilaksanakan secara berdaya guna dan berhasil guna, maka perlu dibuatkan Standar Operasional Prosedur (SOP) Tentang Prosedur Penanganan Serangan *Phising*.

2. TUJUAN.

Mencegah kerugian yang ditimbulkan akibat serangan phising terhadap personel atau organisasi TNI AU.

3. RUANG LINGKUP

SOP penanganan insiden ini berisi langkah-langkah yang harus diambil apabila terjadi insiden serangan *phising* di lingkungan TNI AU, yang dimulai dari tahap persiapan sampai dengan tahap pembuatan laporan dari penanganan insiden.

4. PROSEDUR PENANGANAN SERANGAN *PHISING*

Prosedur penanganan insiden ini dapat dijadikan acuan bagi semua individual atau tim (*administrator*, pengelola TI, dan tim respon insiden keamanan siber) yang bertanggung jawab untuk mencegah, mempersiapkan, atau menanggapi insiden *phishing*. Proses penanganan insiden *phishing* dapat dilaksanakan dalam kurun waktu hingga 14 hari kerja. Penanganan serangan *phishing* ditujukan utuk mencapai hal-hal sebagai berikut:

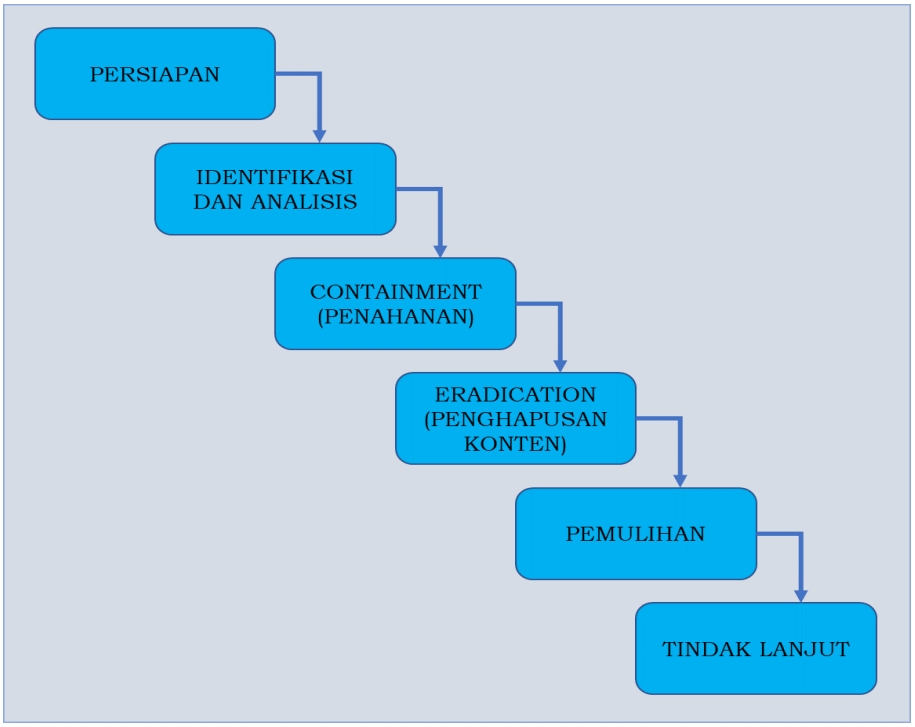
a. Mengumpulkan informasi sebanyak mungkin tentang serangan *phishing*.

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.

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



Gambar 1. Tahap Penanganan Insiden Serangan *Phising*

4.1. **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. 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*, dan Nasional CERT.

e. Meningkatkan kesadaran terhadap serangan *phishing*, diantaranya:

1) Tidak mengklik *link*/tautan yang mencurigakan.

2) Tidak memasukkan *username* dan *password* pada situs *web* yang alamat *web* nya meragukan.

3) Merubah penulisan alamat email yang di*publish*, dari bentuk @ menjadi "at" atau dalam bentuk gambar, untuk menghindari menjadi target *email phising*.

4) Menggunakan *Anti Virus* yang memiliki fitur *Anti Phising*.

4.2. Identifikasi dan Analisis

Tujuan dari proses identifikasi dan analisis adalah untuk mendeteksi adanya insiden serangan *phising*, menentukan ruang lingkup, dan melibatkan pihak-pihak yang tepat dalam menangani serangan *phising*. Tahap identifikasi dan analisis 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*, dan Nasional CERT.

d. Mengumpulkan bukti-bukti terkait adanya serangan *phising*. Contohnya *screenshot* halaman *web* yang terdampak.

4.3. *Containment* (Penahanan)

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*".

4.4. ***Eradication*** **(Penghapusan Konten)**

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.

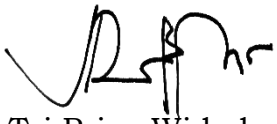
c. Berkolaborasi dengan tim hukum jika diperlukan tindakan hukum.

d. Membuat dokumentasi dan laporan terkait penanganan serangan *Phising*.

e. Membuat evaluasi dan rekomendasi.

Jakarta, November 2023

Kepala Satsiber,



Tri Priyo Widodo
Kolonel Sus NRP 525026