DINAS KOMUNIKASI DAN INFORMATIKA
PROVINSI NUSA TENGGARA TIMUR
BIDANG PERSANDIAN DAN PENGAMANAN INFORMASI

PANDUAN PENANGANAN INSIDEN SERANGAN PHISING

Langkah Cepat, Tepat, dan Terkoordinasi untuk Melindungi Informasi dan Layanan Pemerintah

WASPADA | DETEKSI | TANGANI | LAPORKAN

AMAN INFORMASI TERLINDUNGI NTT

KATA PENGANTAR

Puji syukur kami panjatkan ke hadirat Allah SWT atas segala rahmat dan karunia-Nya sehingga penyusunan "Panduan Penanganan Insiden Serangan Phishing" ini dapat diselesaikan. Panduan ini disusun sebagai acuan bagi seluruh pihak yang berkepentingan dalam menghadapi insiden Serangan Phishing. Di dalamnya tertuang langkah-langkah konkret yang perlu ditempuh saat serangan terjadi, mulai dari kesiapan awal hingga pelaporan akhir pasca penanganan.

Kami menyadari bahwa panduan ini masih memiliki ruang untuk penyempurnaan. Oleh karena itu, evaluasi dan pembaruan berkala akan terus dilakukan demi meningkatkan kualitasnya.

Ucapan terima kasih kami sampaikan kepada semua pihak yang telah berkontribusi dalam penyusunan panduan ini.

Kupang, 08 Mei 2026
Kepala Dinas Komunikasi dan Informatika
Provinsi Nusa Tenggara Timur,

Drs. Ady Endezon Mandala, M.Si
Pembina Utama Muda
NIP. 197001231990091002

DAFTAR ISI

PROSEDUR PENANGANAN INSIDEN SERANGAN PHISHING

1. PENDAHULUAN

Phishing merupakan bentuk serangan siber yang dirancang untuk mengelabui korban agar bersedia mengklik tautan tertentu dan memasukkan data kredensial seperti nama pengguna dan kata sandi. Modus operandi phishing umumnya menggunakan email palsu yang mengatasnamakan pihak berwenang, atau membuat situs web tiruan yang secara visual hampir identik dengan situs resmi.

2. TUJUAN

Panduan ini bertujuan membantu organisasi memahami dan menjalankan penanganan insiden phishing secara efektif. Secara spesifik, panduan ini ditujukan untuk:

1. Menghimpun data dan informasi yang akurat terkait insiden;
2. Menekan dampak kerugian yang timbul akibat serangan seminimal mungkin;
3. Mencegah terjadinya eskalasi serangan dan membatasi kerusakan yang lebih luas..

3. RUANG LINGKUP

Panduan ini mencakup prosedur yang harus dilaksanakan saat terjadi serangan phishing, dari tahap kesiapan hingga pelaporan akhir. Panduan ini dapat digunakan sebagai rujukan oleh seluruh individu maupun tim yang bertanggung jawab dalam mencegah, mempersiapkan, atau menangani serangan phishing, termasuk administrator sistem, pengelola TI, dan tim respons insiden keamanan komputer.

4. PROSEDUR PENANGANAN INSIDEN PHISHING

Penanganan insiden phishing diarahkan untuk mencapai sasaran berikut:

1. Mengumpulkan informasi selengkap mungkin mengenai serangan yang terjadi;
2. Mencegah dampak serangan agar tidak berkembang menjadi lebih parah;
3. Mengamankan bukti-bukti yang berkaitan dengan insiden phishing;
4. Menerapkan langkah-langkah proaktif guna menurunkan risiko serangan serupa di kemudian hari.

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

Gambar 1. Alur Tahapan Penanganan Insiden PHISHING

4.1. Persiapan

Tahap persiapan bertujuan membangun kontak, menetapkan prosedur, dan mengumpulkan informasi awal terkait potensi serangan. Langkah-langkah yang perlu dilakukan:

1. Menyusun inventaris seluruh domain resmi yang dimiliki organisasi;
2. Mempersiapkan halaman peringatan khusus pada website untuk menginformasikan pengguna tentang adanya serangan phishing;
3. Menyiapkan formulir pelaporan penyalahgunaan domain;
4. Membangun dan memperbarui kontak dengan pihak-pihak terkait, meliputi perusahaan hosting, penyedia layanan domain, penyedia email, dan Nasional CERT;
5. Meningkatkan kesadaran seluruh pengguna terhadap ancaman phishing, antara lain melalui imbauan:
   - Tidak mengklik tautan yang tidak dikenal atau mencurigakan;

- Tidak memasukkan kredensial akun pada situs dengan alamat yang meragukan;
- Mengubah format penulisan alamat email yang dipublikasikan dari simbol @ menjadi kata 'at' atau representasi gambar, guna menghindari jadi sasaran email phishing;
- Menggunakan perangkat lunak antivirus yang dilengkapi fitur perlindungan terhadap phishing.

4.2. Identifikasi dan Analisis

Tujuan tahap identifikasi adalah mendeteksi keberadaan insiden phishing, memetakan cakupannya, dan menggerakkan pihak-pihak yang tepat untuk turut serta dalam penanganan. Langkah-langkah yang dilakukan:

1. Memantau secara aktif email, media sosial, dan formulir web organisasi untuk mendeteksi indikasi phishing;
2. Memeriksa URL mencurigakan dan hyperlink menggunakan layanan seperti virustotal.com, urlvoid.com, dan phishtank.com;
3. Melibatkan pihak-pihak yang relevan seperti perusahaan hosting, penyedia domain, penyedia email, dan Nasional CERT agar proses takedown website phishing dapat segera dilakukan;
4. Mengumpulkan bukti-bukti yang mendukung, antara lain berupa tangkapan layar (screenshot) halaman web yang terdampak.

4.3. Containment

Setelah dipastikan bahwa serangan phishing benar-benar terjadi, dilakukan langkah mitigasi untuk mencegah kerusakan yang lebih dalam. Prosedur yang diterapkan:

1. Melaporkan URL phishing beserta konten email terkait ke layanan pelaporan spam seperti phishtank.com;
2. Menginformasikan kepada seluruh pengguna mengenai insiden yang terjadi agar mereka tidak menjadi korban;
3. Memeriksa source code website phishing; jika menggunakan gambar dari website resmi organisasi, segera ganti gambar tersebut dengan tampilan penanda 'PHISHING WEBSITE'.

4.4. Eradication

Tahap ini bertujuan mengambil tindakan nyata untuk menghentikan operasi phishing. Prosedur yang dilakukan:

1. Jika halaman phishing dihosting di website yang telah dikompromikan, hubungi pemilik website tersebut untuk meminta penghapusan halaman palsu dan pelaksanaan pembaruan keamanan;
2. Hubungi perusahaan hosting secara tertulis (email) maupun lisan (telepon) dengan menyertakan informasi lengkap mengenai konten phishing, guna mempercepat penanganan;
3. Minta perusahaan hosting untuk melakukan takedown atau penutupan akses terhadap website palsu tersebut;
4. Apabila proses takedown berlangsung terlalu lama, koordinasikan dengan Nasional CERT untuk menghubungi CERT lokal di negara yang bersangkutan guna membantu akselerasi proses takedown.
5.

4.5. Pemulihan

Pemulihan merupakan tahap pengembalian kondisi ke keadaan normal sebelum insiden. Prosedur yang dilakukan:

1. Memverifikasi bahwa halaman website phishing sudah tidak dapat diakses oleh siapapun;
2. Terus memantau URL palsu secara berkala untuk memastikan tidak ada akses yang masih bisa dilakukan;
3. Menghapus halaman peringatan dari website resmi setelah dipastikan ancaman telah sepenuhnya ditangani.

4.6. Tindak Lanjut

Tindak lanjut adalah fase akhir yang berfokus pada pendokumentasian seluruh kegiatan sebagai bahan pembelajaran dan referensi ke depan. Prosedur yang dilakukan meliputi:

1. Menyempurnakan prosedur dan langkah-langkah respons insiden berdasarkan pengalaman yang diperoleh, sehingga penanganan serupa di masa mendatang dapat dilakukan lebih cepat dan efisien;
2. Memperbarui daftar kontak yang dimiliki beserta catatan mengenai cara paling efektif untuk menghubungi setiap pihak yang terlibat;
3. Berkoordinasi dengan tim hukum apabila diperlukan tindakan hukum terhadap pelaku;
4. Menyusun dokumentasi dan laporan lengkap mengenai seluruh proses penanganan insiden phishing;
5. Membuat evaluasi menyeluruh dan merumuskan rekomendasi peningkatan keamanan.