DINAS KOMUNIKASI DAN INFORMATIKA
PROVINSI NUSA TENGGARA TIMUR

PANDUAN
PENANGANAN INSIDEN
WEB DEFACEMENT

Panduan praktis untuk mendeteksi, merespon, dan memulihkan insiden web defacement secara efektif dan terstruktur

BIDANG PERSANDIAN DAN PENGAMANAN INFORMASI

DETEKSI RESPON PENANGANAN PEMULIHAN

KATA PENGANTAR

Puji syukur kami panjatkan ke hadirat Allah SWT atas segala rahmat dan karunia-Nya sehingga penyusunan "Panduan Penanganan Insiden Web Defacement" ini dapat diselesaikan. Panduan ini disusun sebagai acuan bagi seluruh pihak yang berkepentingan dalam menghadapi insiden Web Defacement. 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 WEB DEFACEMENT

1. PENDAHULUAN

Web defacement merupakan salah satu bentuk serangan siber yang dilakukan dengan cara mengubah tampilan, isi, maupun struktur halaman website tanpa izin dari pemiliknya. Dalam praktiknya, pelaku biasanya mengganti halaman utama situs dengan pesan tertentu, gambar, propaganda, maupun identitas kelompok peretas sebagai bentuk unjuk kemampuan, protes politik, vandalisme digital, hingga penyebaran pesan ideologis. Serangan ini umumnya memanfaatkan celah keamanan pada aplikasi web, konfigurasi server yang lemah, kredensial administrator yang bocor, maupun kerentanan pada plugin dan Content Management System (CMS).

Dalam lanskap keamanan siber modern, web defacement menjadi salah satu ancaman yang cukup sering terjadi, khususnya terhadap website pemerintahan, institusi pendidikan, organisasi publik, dan perusahaan yang memiliki tingkat keamanan rendah. Meskipun tidak selalu menyebabkan kerusakan sistem secara langsung seperti malware, serangan ini dapat menimbulkan dampak serius terhadap reputasi organisasi, menurunkan tingkat kepercayaan publik, serta mengganggu layanan informasi yang seharusnya tersedia bagi masyarakat. Pada beberapa kasus, web defacement juga menjadi indikasi awal bahwa sistem telah berhasil ditembus dan berpotensi mengalami serangan lanjutan yang lebih berbahaya.

Perkembangan teknik serangan web saat ini menunjukkan bahwa pelaku tidak hanya menargetkan perubahan tampilan website semata, tetapi juga dapat menyisipkan script berbahaya, backdoor, maupun malware ke dalam sistem yang telah berhasil dikompromikan. Kondisi tersebut membuat web defacement tidak lagi dipandang sekadar aksi vandalisme digital, melainkan bagian dari ancaman keamanan informasi yang dapat berdampak pada kerahasiaan, integritas, dan ketersediaan data. Oleh karena itu, pengamanan website melalui penerapan patch keamanan, penguatan konfigurasi server, monitoring berkala, serta pengujian keamanan aplikasi web menjadi langkah penting dalam mencegah terjadinya serangan web defacement.

2. TUJUAN

Insiden web defacement memerlukan penanganan yang terencana dan terorganisir. Untuk mendukung hal tersebut, dibutuhkan prosedur standar yang dapat dijadikan acuan. Secara umum, prosedur ini bertujuan memberikan panduan berbasis praktik terbaik (best practices) dalam menangani insiden web defacement. Secara khusus, tujuannya adalah:

1. Memastikan ketersediaan sumber daya yang cukup untuk menangani insiden yang terjadi;
2. Menjamin seluruh pihak yang bertanggung jawab dalam penanganan insiden menjalankan tugas dan kewajibannya masing-masing;
3. Menjamin koordinasi penanganan insiden berjalan dengan baik dan efektif;
4. Memastikan pengumpulan informasi dilakukan secara akurat;
5. Mendorong berbagi pengetahuan dan pengalaman antar anggota tim penanganan insiden;
6. Menekan dampak insiden seminimal mungkin;
7. Mencegah serangan lanjutan dan menghalangi perluasan kerusakan yang lebih parah.

3. RUANG LINGKUP

Prosedur standar ini mencakup langkah-langkah yang perlu dilaksanakan saat terjadi insiden web defacement, dari fase persiapan hingga pelaporan akhir. Web defacement berpotensi terjadi pada seluruh halaman web, baik milik instansi pemerintah, infrastruktur informasi kritikal nasional, maupun pelaku ekonomi digital. Panduan ini berlaku bagi setiap individu atau tim yang mengemban tanggung jawab sebagai pengelola atau administrator suatu web server.

4. PROSEDUR PENANGANAN INSIDEN WEB DEFACEMENT

Penanganan terhadap insiden malware dilaksanakan melalui serangkaian tahapan yang saling berkesinambungan, sebagaimana diuraikan berikut ini:

Gambar 1. Alur Tahapan Penanganan Insiden Web Defacement

Terdapat dua cara bagi institusi atau perorangan dalam menempatkan halaman web: mengelola server secara mandiri, atau menggunakan layanan web hosting. Bagi yang menggunakan web hosting, koordinasi dengan pihak penyedia hosting wajib dilakukan saat terjadi web defacement, guna memudahkan dan mempercepat proses penanganan. Setiap pengelola web hosting seharusnya memiliki prosedur standar untuk menghadapi insiden semacam ini.

4.1. Persiapan

Tahap persiapan bertujuan memastikan semua kebutuhan penanganan insiden web defacement tersedia sebelum dan saat insiden terjadi. Prosedur yang dilakukan:

1. Membentuk tim penanganan insiden, baik dari internal organisasi maupun dari pihak eksternal apabila sangat diperlukan;
2. Menyiapkan dokumen-dokumen pendukung yang dibutuhkan, antara lain:

- Standard Operation Procedure (SOP);
- Formulir yang diperlukan: formulir penanganan insiden dan formulir chain of custody;
- Diagram terbaru yang menggambarkan hubungan antar komponen aplikasi website (web server, aplikasi web, pengguna, dan topologi jaringan);
- Dokumentasi sistem operasi, aplikasi, protokol, dan antivirus yang terpasang pada web server.

3. Berkoordinasi dengan tim teknis, tim CSIRT, maupun Point of Contact untuk mendapatkan informasi tambahan yang diperlukan dalam penanganan insiden;
4. Mengamankan bukti insiden, termasuk screenshot tampilan defacement, log server, dan log perangkat pendukung. Jika ditemukan file mencurigakan, dokumentasikan file tersebut. Untuk keperluan forensik, dapat dilakukan imaging terhadap seluruh storage server maupun memori (RAM);
5. Menentukan ruang atau lokasi yang akan digunakan sebagai pusat koordinasi tim, baik untuk rapat maupun kegiatan analisis insiden;
6. Menyiapkan tools dan media yang diperlukan untuk penanganan insiden, seperti Scanning Tools, Forensic Tools, dan Monitoring Tools, serta media penyimpanan eksternal.

4.2. Identifikasi dan Analisis

Pada tahap ini dilakukan proses identifikasi untuk menelusuri sumber serangan dan mengumpulkan cukup informasi agar tim dapat menentukan prioritas tindakan selanjutnya. Prosedur yang dilakukan:

1. Memeriksa file-file statis di website, apakah terdapat perubahan dan kapan perubahan tersebut terjadi. Periksa juga seluruh link pada halaman web (src, meta, CSS, script);
2. Memeriksa semua file log yang tersedia, meliputi Error Log, Access Log, Database Log, Auth Log, Install Log, Event Log, Firewall Log, IDS/IPS Log, serta Switch/Router Log;
3. Memeriksa folder publik di website (yang memiliki akses write, umumnya digunakan untuk menyimpan file upload) untuk mendeteksi indikasi file backdoor, malware, trojan, atau file berbahaya lainnya;
4. Meninjau kembali kode SQL yang digunakan pada aplikasi web, apakah terdapat celah/bug terutama pada implementasi fitur Login/Logout, koneksi database, dan tampilan isi database;
5. Memeriksa versi setiap aplikasi dan library yang digunakan: web server, aplikasi, dan database;

6. Memeriksa seluruh koneksi yang terhubung ke server;
7. Memeriksa layanan yang sedang berjalan, meliputi port yang terbuka, cronjob, riwayat login pengguna, dan history sistem;
8. Tools yang dapat digunakan pada tahap ini antara lain: NMap, Nikto, Acunetix, dan Nessus.

4.3. Containment

Langkah containment dilakukan untuk mengurangi dampak dan menekan peningkatan risiko lebih lanjut. Prosedur yang dilakukan:

1. Membangun website sementara agar publikasi informasi organisasi tetap dapat berjalan, atau menampilkan halaman 'Site Under Maintenance' selama proses penanganan berlangsung;
2. Melakukan backup sistem untuk keperluan forensik dan pengumpulan bukti insiden;
3. Membatasi akses dari sumber serangan yang telah teridentifikasi, mencakup pemblokiran source IP, port, serta akun pengguna yang digunakan penyerang.

4.4. Eradication

Setelah aplikasi atau file berbahaya berhasil ditemukan, tahap selanjutnya adalah melakukan pembersihan konten tersebut. Prosedur yang dilakukan:

1. Menghapus seluruh file berbahaya yang ditemukan, meliputi file defacement, backdoor, rootkit, dan malware;
2. Melakukan uninstall terhadap aplikasi yang teridentifikasi sebagai malicious.

4.5. Pemulihan

Tahap pemulihan bertujuan mengembalikan halaman web ke kondisi semula sebelum insiden terjadi. Prosedur yang dilakukan:

1. Mengaktifkan kembali (restore) file-file yang telah dibackup sebelumnya, baik file web server maupun file database. Gunakan aplikasi checksum sebagai alat verifikasi integritas data pada file backup;
2. Melakukan update, upgrade, atau patching terhadap seluruh aplikasi yang digunakan pada web server, termasuk CMS, plugin, tema, library, dan modul keamanan;
3. Mengaktifkan pembaruan otomatis (automatic updates) pada setiap aplikasi yang digunakan;
4. Memperbarui semua akun pengguna baik pada sistem operasi maupun aplikasi web;

5. Melakukan hardening server dan aplikasi, termasuk pemasangan Web Application Firewall (WAF) dan aplikasi anti-defacement seperti DotDefender, Nagios, atau Webguard;
6. Memisahkan file web server dari file database pada partisi yang berbeda.

4.6. Tindak Lanjut

Sebagai tindak lanjut penanganan insiden, perlu dilakukan hal-hal berikut:

1. Melakukan uji keamanan menyeluruh terhadap web server dan aplikasi;
2. Memetakan seluruh kerentanan yang ditemukan, baik terkait SQL Injection, XSS, misconfiguration, maupun versi aplikasi yang sudah usang/deprecated;
3. Menyusun dokumentasi dan laporan lengkap mengenai kegiatan dan waktu yang dibutuhkan dalam proses penanganan insiden;
4. Mencatat seluruh tools yang digunakan selama proses penanganan berlangsung;
5. Mendokumentasikan bukti-bukti yang ditemukan untuk keperluan proses hukum di masa mendatang;
6. Memberikan analisis dan rekomendasi konkret agar insiden serupa tidak terulang kembali;
7. Menyusun evaluasi menyeluruh dan rekomendasi peningkatan keamanan sistem.