**PROSEDUR MONITORING KEAMANAN APLIKASI BERBASIS WEB**

**{{nama organisasi}}**

**{{logo organisasi}}**

|  |  |
| --- | --- |
| No Dokumen | : 0.1 (Draft) |
| Revisi | : 00 |
| Tanggal Terbit | : |

|  |  |  |
| --- | --- | --- |
| Disusun  oleh : | Diketetahui  oleh: | Disetujui / Disahkan  oleh : |
|  |  |  |
| **NN**  NN | **NN**  NN | **NN**  NN |

**Riwayat Dokumen**

|  |  |  |
| --- | --- | --- |
| **Versi** | **Tanggal** | **Perubahan** |
| 0.1 (Draft) | 28/02/2023 | Rilis draft awal dengan hanya menyalin sepenuhnya konten dari **PEDOMAN TATA KELOLA KEAMANAN APLIKASI BERBASIS WEB - BSSN** |
| … | … | … |
|  |  |  |

1. **TUJUAN:**
   1. Memberikan referensi panduan kegiatan monitoring keamanan Aplikasi Berbasis Web yang secara berkelanjutan memantau suatu sistem Aplikasi Berbasis Web dari kemungkinan adanya potensi risiko keamanan atau terjadinya suatu serangan siber.
   2. Memastikan bahwa setiap petugas/tim keamanan informasi dan Aplikasi Berbasis Web, tanggap dalam melakukan langkah untuk mengurangi risiko keamanan yang terdeteksi dalam kegiata monitoring keamanan suatu sistem Aplikasi Berbasis Web.
   3. Memastikan Aplikasi Berbasis Web beserta datanya aman dari kemungkinan berbagai tindakan yang tidak sah (unauthorized action).
   4. Memastikan kegiatan monitoring keamanan Aplikasi Berbasis Web berjalan dengan baik dan efektif.
   5. Memastikan adanya pencatatan semua kejadian dalam aktivitas monitoring keamanan Aplikasi Berbasis Web.
2. **RUANG LINGKUP:**

Prosedur ini mencakup langkah-langkah monitoring keamanan suatu sistem Aplikasi Berbasis Web atas risiko keamanan dengan adanya potensi masalah keamanan ataupun serangan siber yang terjadi.

1. **REFERENSI:**
   1. OWASP Testing Guide version 4.0
   2. OWASP Top 10 - 2017: The Ten Most Critical Web Application Security Risks
2. **DEFINISI/ SINGKATAN:**
   1. TIK (Teknologi Informasi dan Komunikasi) adalah istilah dalam sistem komputer yang meliputi perangkat keras (hardware), perangkat lunak (software), jaringan data dan suara, aplikasi sistem informasi dan database, dan lain sebagainya.
   2. Pengguna (User) adalah akun yang digunakan untuk mengakses suatu aplikasi atau sistem TIK.
   3. Hak akses adalah hak akses suatu akun Pengguna terhadap suatu aplikasi atau sistem TIK (misal: read, write, delete, upload, download, dll).
   4. *Vulnerability* (Kerentanan) adalah suatu kelemahan berkaitan dengan keamanan sistem komputer (Aplikasi Berbasis Web), yang dapat dieksploitasi oleh suatu sumber ancaman (threat source), untuk melakukan suatu tindakan yang tidak sah (unauthorized action) dalam sistem komputer (Aplikasi Berbasis Web) tersebut.
   5. *Exploit* (Eksploitasi) adalah cara di mana suatu kerentanan dapat dimanfaatkan untuk melakukan aktivitas yang berbahaya (malicious activity) oleh peretas. Eksploitasi adalah langkah selanjutnya dari si penyerang setelah menemukan sebuah kerentanan dalam sistem komputer (Aplikasi Berbasis Web).
   6. *Vulnerability Scanning* adalah pemindaian terhadap suatu sistem komputer berbasis jaringan (misal: Aplikasi Berbasis Web) dengan menggunakan suatu program komputer yang dirancang untuk mencari berbagai kelemahan atau kerentanan yang terdapat dalam sistem komputer tersebut.
   7. *Penetration Testing* adalah simulasi serangan siber yang secara resmi dilakukan pada suatu sistem komputer (Aplikasi Berbasis Web) untuk mengevaluasi keamanan sistemnya. Pengujian ini dilakukan dengan mengeksploitasi kelemahan atau kerentanan sistem komputer yang teridentifikasi, khususnya terhadap potensi pihak yang tidak berwenang untuk bisa mendapatkan akses ke fitur dan data sistem komputer.
3. **PENANGGUNGJAWAB:**
   1. Penanggungjawab Monitoring Keamanan Aplikasi Berbasis Web, adalah unit kerja dalam organisasi atau pihak ketiga yang bertindak sebagai Penanggungjawab atas pelaksanaan kegiatan monitoring keamanan pada sistem Aplikasi Berbasis Web.
   2. Tim Teknis adalah Penanggungjawab atas semua hal teknis yang berkaitan dengan sistem Aplikasi Berbasis Web, yang umumnya terdiri dari:
      1. Fungsi Pengaturan Pengguna dan Hak Akses TIK bertindak sebagai Penanggungjawab atas pengaturan pengguna dan pengendalian hak akses pada sistem aplikasi dan database.
      2. Fungsi Pengembang Aplikasi TIK bertindak sebagai Penanggungjawab atas pengembangan dan pemeliharaan sistem aplikasi dan database.
      3. Fungsi Pengembangan Infrastruktur dan Jaringan TIK bertindak sebagai Penanggungjawab atas pengembangan dan pemeliharaan perangkat keras, LAN, WAN, jaringan internet, administrasi database dan administrasi sistem operasi server.
      4. Fungsi Pengendali Keamanan TIK bertindak sebagai pelaksana pengendalian keamanan sistem infrastruktur dan sistem aplikasi.
      5. Fungsi Operasional TIK bertindak sebagai pelaksana operasional harian atas sistem infrastruktur dan sistem aplikasi.
4. **LANGKAH – LANGKAH:**
5. **Aktivitas Monitoring Keamanan Aplikasi Berbasis Web**

# Tabel 4.10 Aktivitas Monitoring Keamanan Aplikasi Berbasis Web

|  |  |  |
| --- | --- | --- |
| **LANGKAH** | **AKTIVITAS** | **AKTOR** |
| 1 | Melaksanakan kegiatan monitoring keamanan terhadap suatu Aplikasi Berbasis Websecara berkesinambungan. Berbagai aktivitas monitoring tersebut dapat mencakup, antara lain:   * Monitoring kerentanan (vulnerability) * Monitoring sertifikat SSL/TLS * Monitoring lama hidup server/ service (up-time) * Monitoring masa berlaku domain * Monitoring Aplikasi Berbasis Webdari daftar blacklist * Monitoring DNS terkait Aplikasi Berbasis Web | Penanggungjawab Monitoring Keamanan Aplikasi Berbasis Web |
| 2 | Jika dalam kegiatan monitoring terdeteksi suatu masalah keamanan, maka:   * Melakukan pemeriksaan dan validasi terhadap masalah keamanan yang terdeteksi untuk mem-validasi masalah keamanan tersebut, dan apakah berpotensi untuk terjadinya suatu pelanggaran keamanan terhadap Aplikasi Berbasis   Webyang dimonitor | Penanggungjawab Monitoring Keamanan Aplikasi Berbasis Web |
| 3 | Melakukan penilaian tingkat potensi masalah keamanan yang terdeteksi dalam salah satu tingkatan (level) sebagai acuan prioritas penanganan, diantaranya:   * Normal, jika hasil pemeriksaaan dan validasi menunjukkan (false positive) sehingga dapat diabaikan. * Rendah (low) * Medium (med) * Tinggi (high) * Parah (severe) | Penanggungjawab Monitoring Keamanan Aplikasi Berbasis Web |
| 4 | Untuk tingkatan low, med, high, dan severe, melakukan pelaporan kepada “Tim Teknis” terkait untuk permintaan tindak lanjut atas masalah keamanan Aplikasi Berbasis  Webtersebut | Penanggungjawab Monitoring Keamanan Aplikasi Berbasis Web |
| 5 | Melakukan pencatatan kejadian (log event) secara terstruktur dan rinci atas semua masalah keamanan Aplikasi  Berbasis Webyang terdeteksi | Penanggungjawab Monitoring Keamanan  Aplikasi Berbasis Web |

1. **Diagram Alir Aktivitas Monitoring Keamanan Aplikasi Berbasis Web**

**Gambar 4.11 Diagram Alir Aktivitas Monitoring Keamanan Aplikasi Berbasis Web**

**Penanggungjawab Monitoring Keamanan Aplikasi Berbasis Web**

**Tim Teknis**

Monitoring Keamanan Website

Masalah Keamanan Terdeteksi?

Ya

Pemeriksaan & Verifikasi

False Positive (Normal)

Tidak

Potensi

Pelanggaran Keamanan?

Ya

Laporan Permintaan Tindak Lanjut

Pelaporan Untuk Permintaan Tindak Lanjut

Pencatatan (Log Event)