**PROSEDUR MANAJEMEN KERENTANAN KEAMANAN APLIKASI BERBASIS WEB**

**DI LINGKUNGAN**

**BADAN PENGUSAHAAN BATAM**

**Logo

Description automatically generated**

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

|  |  |  |
| --- | --- | --- |
| Disusun  oleh : | Diketetahui  oleh: | Disetujui / Disahkan  oleh : |
|  |  |  |
| **Yogi Kortisa**  Analis Keamanan TI | **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 bagi aktivitas manajemen kerentanan Aplikasi Berbasis Web yang secara bertahap dengan skala prioritas dan berkelanjutan, untuk mengurangi ancaman keamanan yang mungkin terjadi akibat adanya kerentanan dalam sebuah Aplikasi Berbasis Web.
   2. Memastikan bahwa Penanggungjawab manajemen kerentanan Aplikasi Berbasis Web, tanggap dalam melakukan langkah-langkah untuk meminimalkan risiko keamanan atas suatu sistem Aplikasi Berbasis Web.
   3. Memastikan Aplikasi Berbasis Web beserta datanya menjadi lebih aman dari kemungkinan berbagai tindakan yang tidak sah (unauthorized action).
   4. Memastikan kegiatan manajemen kerentanan Aplikasi Berbasis Web berjalan dengan baik dan efektif.
   5. Memastikan adanya dokumentasi dari setiap kegiatan dalam aktivitas manajemen kerentanan Aplikasi Berbasis Web.
2. **RUANG LINGKUP:**

Prosedur ini mencakup langkah-langkah secara umum untuk meminimalkan ancaman keamanan yang mungkin terjadi akibat terdapatnya kerentanan-kerentanan dalam suatu sistem Aplikasi Berbasis Web, melalui kegiatan manajemen kerentanan Aplikasi Berbasis Web.

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 Manajemen Kerentanan Aplikasi Berbasis Web, adalah unit kerja dalam organisasi atau pihak ketiga yang bertindak sebagai Penanggung jawab atas pelaksanaan kegiatan manajemen kerentanan pada sistem Aplikasi Berbasis Web.
   2. Tim Teknis adalah Penanggung jawab 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 Manajemen Kerentanan Aplikasi Berbasis Web**

# Tabel 4.11 Aktivitas manajemen Kerentanan Aplikasi Berbasis Web

|  |  |  |  |
| --- | --- | --- | --- |
| **LANGKAH** | | **AKTIVITAS** | **AKTOR** |
| 1 | | Melaksanakan inventarisir terhadap data-data teknis dalam Aplikasi Berbasis Web, meliputi: alamat IP, DNS, sistem operasi, alamat MAC, port, layanan, software, proses, hardware, event log, dan lainnya | Penanggungjawab Manajemen Kerentanan Aplikasi Berbasis Web |
| 2 | | Melakukan identifikasi dan pengujian kerentanan Aplikasi Berbasis Web, baik secara manual maupun dengan menggunakan tool. Rincian item-item yang diuji secara umum adalah mengacu pada dokumen *“Standar Pengujian Kerentanan Aplikasi Web, BSSN – 2019”*, diantaranya berkaitan dengan komponen penting Aplikasi Berbasis Webberikut: server, aplikasi web, kode statis, middleware, dan database | Penanggungjawab Manajemen Kerentanan Aplikasi Berbasis Web |
| 3 | | Melakukan identifikasi risiko berdasarkan potensi ancaman dan risiko keamanan aplikasi web (misalnya: berdasarkan OWASP Top 10), serta menentukan prioritas pemulihan kerentanan sesuai tingkat risikonya.  Selanjutnya informasi dan data kerentanan berikut prioritas pemulihannya diserahkan pada “Tim Teknis” terkait untuk ditindaklanjuti. | Penanggungjawab Manajemen Kerentanan Aplikasi Berbasis Web |
| 4 | | Melakukan langkah pemulihan kerentanan Aplikasi Berbasis Web |  |
|  | 4.1 | Melakukan ujicoba pemulihan kerentanan dengan melakukan berbagai langkah untuk bisa menutup suatu celah keamanan. | Tim Teknis |

|  |  |  |  |
| --- | --- | --- | --- |
|  | 4.2 | Melakukan verifikasi dan melakukan pengujian atas hasil ujicoba pemulihan kerentanan Aplikasi Berbasis Webyang telah dilakukan oleh Tim Teknis | Penanggungjawab Manajemen Kerentanan Aplikasi Berbasis Web |
| 4.3 | Jika ujicoba pemulihan kerentanan Aplikasi Berbasis Webdinyatakan berhasil untuk menutup celah keamanan, maka langkah pemulihan kerentanan diterapkan di Aplikasi Berbasis Web“Production”. | Tim Teknis |
| 5 | | Melakukan pendokumentasian untuk setiap kegiatan yang berkaitan dengan aktivitas manajemen kerentanan Aplikasi Berbasis Web, sebagai bahan untuk analisis kedepan terkait keamanan Aplikasi Berbasis Webdan knowledge repository.  Secara periodik membuat “Laporan Manajemen Kerentanan Aplikasi Berbasis Web”. | Penanggungjawab Manajemen Kerentanan Aplikasi Berbasis Web |

1. **Diagram Alir Aktivitas Manajemen Kerentanan Aplikasi Berbasis Web**

**Gambar 4.12 Diagram Alir Aktivitas Manajemen Kerentanan Aplikasi Berbasis Web**

|  |  |  |  |
| --- | --- | --- | --- |
| **Penanggungjawab Manajemen Kerentanan Aplikasi Berbasis Web** | | | **Tim Teknis** |
|  | Inventarisir Data Teknis |  |  |
|  | & Komponen Website |  |  |
|  |  |  |  |
|  | Identifikasi & Pengujian |  |  |
|  | Kerentanan Website |  |  |
|  |  |  |  |
|  | Identifikasi Risiko |  | Data |
|  | Keamanan & Menentukan Prioritas Pemulihan |  | Prioritas |
|  |  |  | Ujicoba |
|  |  |  | Pemulihan Kerentanan |
|  | Verifikasi & Pengujian |  |  |
|  | Hasil Ujicoba Pemulihan |  |  |
|  | Kerentanan Website |  |  |
|  |  |  |  |
|  | Ujicoba Pemulihan | Ya | Memulihkan Kerentanan di Aplikasi Berbasis |
| Tidak | Berhasil? |  | Web“Production” |
|  | Menyusun |  |  |
|  | Dokumentasi |  |  |
|  |  |  |  |
|  | Laporan Manajemen Kerentanan  Website |  |  |