**PROSEDUR PENGENDALIAN INSIDEN 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. Memitigasi risiko insiden keamanan Aplikasi Berbasis Web
   2. Memastikan bahwa setiap petugas/tim keamanan informasi dan Aplikasi Berbasis Web, tanggap terhadap insiden keamanan informasi/Aplikasi Berbasis Webyang terjadi.
   3. Memastikan penanganan insiden keamanan Aplikasi Berbasis Webdengan cepat dan tepat.
   4. Memastikan adanya knowledge management dan repository yang berkelanjutan dalam menangani insiden keamanan Aplikasi Berbasis Web
2. **RUANG LINGKUP**

Prosedur ini hanya berlaku untuk pengendalian insiden yang dikarenakan oleh:

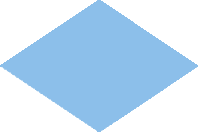
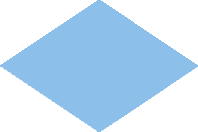
1. DoS/DDoS
2. Malware
3. Web defacement
4. Phishing
5. **REFERENSI**
   1. NIST Special Publication 800-61 Revision 2: Computer Security Incident Handling Guide
6. **DEFINISI/SINGKATAN**
   1. Pemohon adalah pengguna TIK yang mengirim permintaan pengendalian insiden dan/atau layanan TIK.
   2. TIK (Teknologi Informasi dan Komunikasi) adalah meliputi perangkat keras, perangkat lunak dan sistem operasi PC (*Personal Computer*) dan *Server*, Jaringan Komunikasi Data dan Suara, Aplikasi Sistem Informasi dan *Database* Sistem Informasi.
   3. User adalah akun yang digunakan untuk mengakses suatu aplikasi atau sistem
   4. Hak akses adalah hak akses suatu akun terhadap suatu aplikasi atau sistem (read, update, write, upload, download, dll)
7. **PENANGGUNGJAWAB**
   1. Tim Security Incident Respon bertindak dan bertanggungjawab atas penanganan insiden keamanan Aplikasi Berbasis Webdan mencari breakthrough agar kondisi setelah insiden tersebut dapat kembali ke kondisi normal secepat - cepatnya
   2. Tim Teknis bertindak dan bertanggungjawab atas proses perbaikan karena insiden sehingga sistem dapat beroperasi secara nomal kembali.
8. **LANGKAH – LANGKAH**
9. **Aktivitas Incident Respon**

# Tabel 4.1 Aktivitas Incident Respon

|  |  |  |
| --- | --- | --- |
| **LANGKAH** | **AKTIVITAS** | **AKTOR** |
| 1 | Tim Security Incident Respon menemukan insiden dan melaporkan kepada Tim Teknis | Tim Security Incident Respon |
| 2 | Tim Security Incident Respon melakukan analisis Awal dengan mencari informasi dan data – data yang terkait insiden | Tim Security Incident Respon |
| 3 | Berdasarkan hasil analisis kemudian menentukan seberapa besar potensial serangan tersebut. Jika false positive maka akan dibuatkan laporan akhir | Tim Security Incident Respon |
| 4 | Apabila insiden berpotensi serangan maka melakukan eskalasi lebih dalam dan melakukan pengkajian | Tim Security Incident Respon |
| 5 | Mengklasifikasikan kategori Insiden dari jenis serangan, jika bukan termasuk ke top 3 maka akan dimasukan ke log events | Tim Security Incident Respon |
| 6 | Kategori insiden termasuk Top 3 , maka tim analisis Security Incident Respon membuat laporan penanganan | Tim Security Incident Respon |
| 7 | Tim analisis Security Incident Respon membuat laporan akhir | Tim Security Incident Respon |

1. **Diagram Alir Incident Respon**

**Gambar 4.2 Diagram Alir Incident Respons**



Laporan

Insiden

Laporan Awal

Analisis Awal

Potensial

Serangan

Eskalasi Insiden

False Positif

Klasifikasi

Top 3 Insiden

Level High,

L

ow, Medium

Membuat

Laporan Akhir

Log Event

**Tim Teknis**

**Tim Security Incident Respon**

1. **Proses Penanganan Insiden DoS/DdoS**

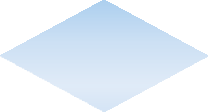
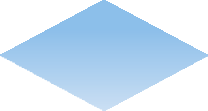
# Tabel 4.2 Proses Penanganan Insiden DoS/DDoS

|  |  |  |
| --- | --- | --- |
| **LANGKAH** | **AKTIVITAS** | **Aktor** |
| 1 | Tim Security Incident Respon menemukan insiden DoS dan melaporkan kepada Tim Teknis | Tim Security Incident Respon |
| 1.2 | Membuat laporan awal terkait insiden DoS | Tim Teknis |
| 1.3 | Melakukan prioritas untuk penanganan |  |
| 2 | Tim Security Incident Respon membuat tiket insiden pada portal serta melaporkan ke tim teknis | Tim Security Incident Respon |
| 3 | Melakukan pengumpulan data – data terkait Insiden DoS (Log) | Tim Security Incident Respon |
| 4 | Apa pengaruh dari dampak serangan insiden DoS terhadap jaringan di Kemhan, dan menutup service apache yang bermasalah | Tim Security Incident Respon |
| 5 | Melakukan identifikasi serta mitigasi kerentanan Service Apache yang dieksploitasi dari serangan DoS |  |
| 6 | Apakah serangan belum berhenti ? | Tim Security Incident Respon |
| 6.1 | Melakukan filtering berdasarkan karateristik serangan DoS |  |
| 6.2 | Melakukan mitigasi ulang terhadap kerentanan Service Apache |  |
| 7 | Apabila serangan berhenti | Tim Security Incident Respon |
| 7.1 | Service Apache yang sudah di Patch dioperasikan kembali | Tim Security Incident Respon |
| 8 | Konfirmasi ke user apakah masih terjadi serangan | Tim Teknis |
| 8.1 | Apabila belum maka proses mitigasi diulangi kembali | Tim Security Incident Respon |
| 9 | Melakukan pembahasan insiden DoS | Tim Teknis |
| 10 | Membuat laporan hasil Analisis Serangan DoS terhadap Service Apache dan penangulangan terhadap insiden tersebut. | Tim Teknis |

1. **Diagram Alir Penanganan Insiden DoS/DDoS**

**Gambar 4.3 Diagram Alir Penanganan Insiden DoS/DDoS**

Tim Security Incident Respon Tim Teknis



Insiden Berupa

DOS

Laporan Awal

Membuat Tiket

Pada Portal

Mengumpulkan

Data-data

Melakukan Perioritas Berdasarkan Dampak Insiden

Estimasi Teknis dan Eskalasi Insiden

Mitigasi Kelemahan Yang di Exploitasi

Serangan Sudah Berhenti?

belum

Filter Berdasarkan Karakteristik Serangan

belum

Relokasi Target

Mengembalikan Sistem Seperti Semula

Konfirmasi Sistem

Telah Normal

Sudah

Pembahasan

Insiden

Membuat Laporan Akhir, Update Portal

1. **Aktivitas Penanganan Insiden Malware**

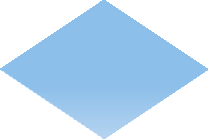
# Tabel 4.3 Aktivitas Penanganan Insiden Malware

|  |  |  |
| --- | --- | --- |
| **LANGKAH** | **AKTIVITAS** | **PERSONIL** |
| 1 | Tim Security Incident Respon menemukan insiden Malware dan melaporkan kepada Tim Teknis | Tim Security Incident Respon |
| 1.2 | Membuat laporan awal terkait insiden Malware | Tim Teknis |
| 1.3 | Melakukan prioritas untuk penanganan | Tim Teknis |
| 2 | Tim Security Incident Respon membuat tiket insiden pada portal serta melaporkan ke tim teknis | Tim Security Incident Respon |
| 3 | Melakukan identifikasi serta mitigasi sistem yang terinfeksi |  |
| 4 | Apabila malware tersebut sangat berbahaya maka dilakukan pemutusan jaringan terhadap sistem yang terinfeksi | Tim Security Incident Respon |
| 5 | Melakukan Mitigasi terhadap kerentanan yang dieksploitasi oleh malware | Tim Security Incident Respon |
| 6 | Tim Security Incident Respon memberikan arahan kepada tim teknis untuk membersihkan, mengkarantina atau mendelete file yang terinfeksi | Tim Security Incident Respon |
| 7 | Konfirmasi ke Tim Teknis apakah masih terjadi serangan | Tim Teknis |
| 7.1 | Apabila belum maka proses mitigasi diulangi kembali | Tim Security Incident Respon |
| 8 | Melakukan pembahasan insiden Malware | Tim Teknis |
| 9 | Membuat laporan hasil Analisis Serangan Malware terhadap Sistem dan penangulangan terhadap insiden tersebut. | Tim Teknis |

1. **Diagram Alir Penanganan Insiden Malware**

**Gambar 4.4 Diagram Alir Penanganan Insiden Malware**

Tim Security Incident Respon Tim Teknis



Insiden Berupa Malware

Laporan Awal

Membuat Tiket

Pada Portal

Estimasi Teknis dan Eskalasi Insiden

Melakukan Perioritas Berdasarkan Dampak Insiden

Identifikasi Sistem yang Terinfeksi

Memutuskan Sistem Pada Jaringan

belum

Mitigasi Kerentanan yang Tereksploitasi

Quarantined/ Delete File yang

terinfeksi

Konfirmasi Sistem

Telah Normal

Sudah

Pembahasan

Insiden

Membuat Laporan Akhir, Update Portal

1. **Aktivitas Penanganan Insiden Web Defacement**

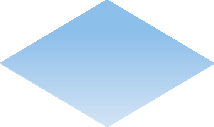
# Tabel 4.4 Aktivitas Penanganan Insiden Web Defacement

|  |  |  |
| --- | --- | --- |
| **LANGKAH** | **AKTIVITAS** | **PERSONIL** |
| 1 | Tim Security Incident Respon menemukan insiden Web defacement dan melaporkan kepada Tim Teknis | Tim Security Incident Respon |
| 1.2 | Membuat laporan awal terkait insiden Web Defacement | Tim Teknis |
| 1.3 | Melakukan prioritas untuk penanganan | Tim Teknis |
| 2 | Tim Security Incident Respon membuat tiket insiden pada portal serta melaporkan ke tim teknis | Tim Security Incident Respon |
| 3 | Apa pengaruh atau dampak dari serangan defacement tersebut. | Tim Security Incident Respon |
| 4 | Memberikan arahan pengantian halaman web yang terdefacement diganti dengan halaman informasi “sedang dalam perbaikan” | Tim Security Incident Respon |
| 5 | Melakukan pengumpulan data – data terkait temuan – temuan aplikasi hacking seperti backdoor dan file halaman informasi defacement | Tim Security Incident Respon |
| 6 | Melakukan indentifikasi serta mitigasi kerentanan pada web yang ter-deface | Tim Security Incident Respon |
| 6 | Hapus file backdoor dan file halaman informasi deface | Tim Security Incident Respon |
| 7 | Mengembalikan halaman web seperti semula, berdasarkan data web yang pernah di backup |  |
| 8 | Konfirmasi ke Tim Teknis apakah masih terjadi serangan | Tim Teknis |
| 8.1 | Apa bila belum maka proses mitigasi diulangi kembali | Tim Security Incident Respon |
| 8 | Melakukan pembahasan insiden Web defacement | Tim Teknis |
| 9 | Membuat laporan hasil Analisis Web defacement terhadap Sistem dan penangulangan terhadap insiden tersebut. | Tim Teknis |

1. **Diagram Alir Penanganan Insiden Web Defacement**

**Gambar 4.5 Diagram Alir Penanganan Insiden Web Defacement**

Tim Security Incident Respon Tim Teknis



Insiden Berupa Web Defacement

Laporan Awal

Membuat Tiket

Pada Portal

Estimasi Teknis dan Eskalasi Insiden

Melakukan Perioritas Berdasarkan Dampak Insiden

Initial

Containment

Pengumpulan Data

Mitigasi Kerentanan yang Tereksploitasi

belum

Hapus File Backdoor/ Halaman Informasi

Defacement

Mengembalikan

Sistem Ke Semula

Konfirmasi Sistem

Telah Normal

Sudah

Pembahasan

Insiden

Membuat Laporan Akhir, Update Portal

1. **Aktivitas Penanganan Insiden Phising**

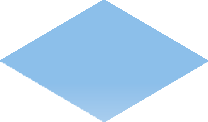
# Tabel 4.5 Aktivitas Penanganan Insiden Phising

|  |  |  |
| --- | --- | --- |
| **LANGKAH** | **AKTIVITAS** | **PERSONIL** |
| 1 | Tim Security Incident Respon menemukan insiden Phishing dan melaporkan kepada Tim Teknis | Tim Security Incident Respon |
| 1.2 | Membuat laporan awal terkait insiden Web Defacement | Tim Teknis |
| 1.3 | Melakukan prioritas untuk penanganan | Tim Teknis |
| 2 | Tim Security Incident Respon membuat tiket insiden pada portal serta melaporkan ke tim teknis | Tim Security Incident Respon |
| 3 | Apa pengaruh atau dampak dari Phishing tersebut apakah pencurian account (data user dan password) | Tim Security Incident Respon |
| 4 | Memberikan arahan mendisable halaman web Phishing | Tim Security Incident Respon |
| 5 | Melakukan pengumpulan data – data terkait temuan – temuan aplikasi hacking seperti backdoor dan file Phishing | Tim Security Incident Respon |
| 6 | Melakukan indentifikasi serta mitigasi kerentanan pada web yang tersisipi halaman Phishing | Tim Security Incident Respon |
| 6 | Hapus file backdoor dan file/Folder Phishing | Tim Security Incident Respon |
| 7 | Memberikan informasi halaman Aplikasi Berbasis Webyagn legitimate | Tim Security Incident Respon |
| 8 | Konfirmasi ke Tim Teknis apakah masih terjadi serangan | Tim Teknis |
| 8.1 | Apabila belum maka proses mitigasi diulangi kembali | Tim Security Incident Respon |
| 8 | Melakukan pembahasan insiden Phishing site | Tim Teknis |
| 9 | Membuat laporan hasil Analisis Phishing dan penangulangan terhadap insiden tersebut. | Tim Teknis |

1. **Diagram Alir Penanganan Insiden Phising**

**Gambar 4.6 Diagram Alir Penanganan Insiden Phising**

Tim Secuirty Incident Respon Tim Teknis



Insiden

Berupa Phising

Laporan Awal

Membuat Tiket

Pada Portal

Estimasi Teknis dan Eskalasi Insiden

Melakukan Perioritas Berdasarkan Dampak Insiden

Initial

Containment

Pengumpulan Data

Mitigasi Kerentanan yang Tereksploitasi

belum

Hapus Folder Phising

Memberikan Informasi halaman yang Legitimate

Konfirmasi Sistem

Telah Normal

Sudah

Pembahasan

Insiden

Membuat Laporan Akhir, Update Portal