**STANDAR 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** |
| … | … | … |
|  |  |  |

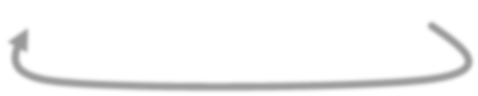
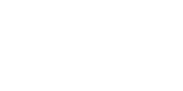
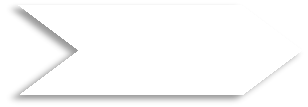
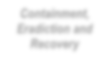
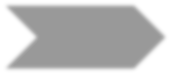
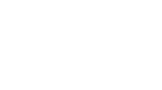
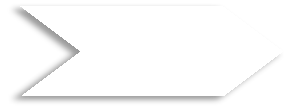
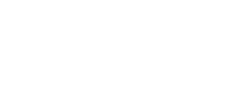
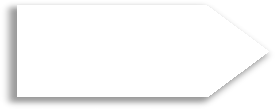
1. **TUJUAN**
   1. Untuk memastikan bahwa:
      1. Pengendalian/respon insiden keamanan Aplikasi Berbasis Webdapat diatasi secepat mungkin.
      2. Adanya *knowledge management* dan *continuous improvement* dari setiap insiden yang terjadi.
   2. Memberikan petunjuk dalam melakukan pengendalian insiden keamanan Aplikasi Berbasis Web.
2. **RUANG LINGKUP**
   1. Tahapan Pengendalian Insiden Keamanan
   2. Pencegahan Insiden
   3. Penerapan Tahapan Pengendalian Insiden Keamanan berdasarkan jenis insiden
3. **ISTILAH DAN DEFINISI**

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | *Suspicious files/Malicious Code* | : | Perangkat perusak, perangkat lunak berbahaya atau perangkat lunak jahat adalah perangkat lunak yang diciptakan untuk menyusup atau merusak sistem komputer, server atau jejaring komputer tanpa izin dari pemilik. |
| 2. | Instansi | : | Kementerian/Lembaga, Instansi pusat atau daerah. |
| 3. | *Password* | : | Kata sandi yang digunakan bersamaan dengan *username* (*sign on/sign in/log-on/log-in*) oleh pemilik yang sah sebelum melakukan koneksi/akses ke sistem komputer. |
| 4. | *Patch* | : | Rutin program atau sekumpulan kecil instruksi yang biasanya dibuat sebagai solusi sementara untuk mengatasi atau memperbaiki permasalahan (*bugs*) pada program komputer dan sering dibuat dalam bentuk *’object code’* yang disisipkan ke dalam program yang  akan dieksekusi. |

1. **REFERENSI**
   1. NIST Special Publication 800-61 Rev2: Computer Security Incident Handling Guide
2. **STANDAR**
   1. **Tahapan Pengendalian Insiden**

Standar Tahapan Pengendalian Insiden meliputi:

**Gambar 3.6 Tahapan Pengendalian Insiden**



***Preparation***

***Detection and Analysis***

***Containment, Eradiction and Recovery***

***Post Incident***

* + 1. Persiapan *(Preparation)*
       - Membangun dan melatih tim respon insiden, mempersiapkan aplikasi analisis yang akan digunakan dan sumber daya yang diperlukan.
       - Tim insiden menyiapkan untuk menganalisis insiden, tim respon insiden menentukan insiden yang paling mungkin terjadi di dalam organisasi. Analisis risiko sangat penting untuk menentukan insiden-insiden yang mungkin terjadi pada suatu aset informasi di instansi. Dengan pimpinan tim insiden respon melakukan identifikasi risiko-risiko yang terjadi, apa yang harus dilakukan dan bagaimana mencari solusi dari permasalahan tersebut.
       - Pembatasan jumlah insiden yang akan terjadi dengan memilih dan menerapkan satu set kontrol berdasarkan hasil penilaian risiko
    2. Deteksi & Analisis (*Detection and Analysis*)
       - Ada beberapa sumber untuk pendeteksian insiden, seperti pemantaun traffic IDS, laporan dari internal. Dari laporan pendeteksian insiden maka tim respon insiden melakukan analisis insiden, dan laporan analisis tersebut disajikan bukan berdasarkan spekulasi dan asumsi, tetapi berdasarkan hasil analisis yang sudah dilakukan dengan menggunakan aplikasi – aplikasi analisis khusus disesuaikan berdasarkan laporan insiden tersebut.
       - Pendeteksian pelanggaran keamanan diperlukan sebagai bahan analisis Tim Insiden, untuk mengetahui kapan insiden tersebut terjadi. Disesuaikan dengan tingkatan setiap insiden tersebut dapat mengurangi dampak dari insiden sehingga proses pemulihan dapat terselesaikan dengan cepat. Selama fase ini , aktivitas siklus kembali ke deteksi dan analisis - misalnya, untuk melihat apakah tambahan host yang terinfeksi oleh malware sementara pemberantasan insiden malware
    3. Penahanan, Pemberantasan & Pemulihan (*Containment, Eradiction and Recovery*)

Setelah proses analisis, maka proses selanjutnya bagaimana menentukan strategi untuk proses *Containment, Eradiction dan Recovery*. Kompatibilitas dalam perancangan strategi sangat penting untuk mempertimbangkan hal – hal:

* + - * Kemungkinan potensi kerusakan pada sumber daya
      * Efektifitas dan durasi dalam strategi pemberian solusi dari setiap penanganan insiden Sebelum memulai proses penanganan, pihak pimpinan tim insiden respon sudah megetahui dan menyetujui laporan hasil analisis insiden tersebut, karena laporan hasil analisis insiden tersebut akan menjadi pendukung utama dalam memulai proses penanganan insiden tersebut.
    1. Aktivitas Paska Insiden (*Post Incident Activity*)
       - Tim Insiden menerbitkan sebuah laporan yang merinci penyebab dan biaya insiden tersebut dan langkah-langkah organisasi untuk melakukan pencegahan insiden di masa depan
       - Setelah melakukan proses containment, eradiction dan recovery, maka tahap selanjutnya melakukan pertemuan antara pimpinan dan steakholder untuk menyusun langkah – langkah kedepan-nya apabila terjadi insiden tersebut terjadi lagi di masa depan.
  1. **Pencegahan Insiden**
     1. Blokir *suspicious files*
* Konfigurasi email server dan client untuk memblokir *attachment* dengan ekstensi file yang berkaitan dengan *malicious code* (misalnya .pif, .vbs, bisa juga .rar atau .zip agar lebih ketat) dan kombinasi ekstensi file yang mencurigakan (misalnya .txt.vbs., .Htm.exe.). Namun cara ini mungkin juga memblokir aktifitas yang sah. Beberapa instansi mengubah ekstensi file terlebih dahulu sebelum dikirim kemudian penerima harus men-*save* dan me- *rename* file terlebih dahulu sebelum dijalankan.
* Mengurangi sharing file pada OS karena banyak worm yang menyebar melalui sharing file pada host yang menjalankan OS. Sebuah infeksi tunggal dapat dengan cepat menyebar ke ratusan atau ribuan host melalui unsecured share.
  + 1. Menetapkan prosedur kepada semua user dari sistem, aplikasi, domain, sampai workstation untuk mengubah password mereka secara periodik. Hal ini merupakan cara mencegah akses yang tidak terotorisasi.
    2. Meningkatkan Pengetahuan Keamanan Informasi (*Security Awareness*)
* Unit IT Security harus mengadakan pelatihan security awareness yang dilakukan satu kali dalam setahun yang diikuti oleh seluruh pegawai. Hal ini dimaksudkan agar setiap karyawan menyadari aturan perilaku dan tanggungjawab mereka dalam melindungi misi Instansi.
* Untuk meningkatkan *security awareness* tidak hanya melalui pelatihan saja satu kali setahun saja, tetapi dapat dilakukan dalam sesi-sesi kecil perdivisi atau grup dengan materi yang menyeluruh mengenai keamanan informasi. Misalnya masalah attachment pada email, pergantian password, serta sharing file. Selain itu juga dapat dilakukan workshop, melalui situs Web, dan stiker.
  1. **Deteksi Insiden**
     1. Manajemen *Patch*

Secara rutin unit IT Security melakukan *vulnerability assessment* secara periodik. Hal ini dilakukan untuk mengurangi potensi terjadinya insiden keamanan. Dari hasil penilaian kerentanan yang telah diinformasikan kepada Penanggungjawab masing - masing perangkat seharusnya dilakukan eskalasi terhadap kerentanan yang ada. *Manajemen patch* sangat penting untuk mengurangi kerentanan yang ada pada aplikasi. Unit IT Security juga bertanggungjawab untuk melakukan manajemen *patch*, misalnya dengan memperoleh, menguji, dan mendistribusikan *patch* untuk para administrator yang sesuai dan pengguna diseluruh Instansi. Terkadang manajemen *patch* sering dibutuhkan saat mencoba untuk melakukan pemulihan dari insiden dengan skala besar.

* + 1. Penggunaan SIEM (*Security Incident Event Management*) lebih ditingkatkan.

Terkadang sulit untuk mengidentifikasi suatu event sebagai insiden yang potensial. Semua yang mengeluarkan log harus dimonitor dengan baik. Mulai dari log aplikasi, perangkat (firewall, IDPS, appliance), sistem operasi, maupun database. SIEM bekerja untuk meningkatkan keamanan informasi pada infrastruktur jaringan instansi dengan efisien dan dapat mendeteksi kejadian yang mencurigakan. SIEM bertugas untuk memberikan deteksi awal dan peringatan terhadap event keamanan.

* 1. **Deteksi & Analisis Berdasarkan Jenis Insiden**
     1. Insiden Secara Umum

# Tabel 3.3 Deteksi & Analisis Insiden Secara Umum

|  |  |
| --- | --- |
| **Tahap** | **Kontrol** |
| Deteksi dan Analisis | * Mengetahui insiden yang telah terjadi * Menganalisis sesuatu yang akan datang berdasarkan indikasi yang ada * Mencari informasi yang saling berhubungan * Melakukan pengkajian * Mendokumentasikan semua proses investigasi dan hasil pengumpulan bukti yang ada. * Mengklasifikasi insiden menggunakan beberapa kategori yang ada |

* + 1. Insiden *Distributed Denial of Service (DDoS)*

# Tabel 3.4 Deteksi & Analisis DDoS

|  |  |
| --- | --- |
| **Tahap** | **Kontrol** |
| Deteksi dan analisis | * Memprioritaskan penanganan insiden berdasarkan pengaruh bisnis. * Mengidentifikasi sistem/resource mana yang terkena dan memprediksikan sistem/resource mana yang akan terkena selanjutnya. * Melakukan estimasi terhadap pengaruh secara teknis saat ini dan yang akan berpotensi terkena dari insiden tersebut. * Melaporkan insiden kepada internal staf insiden respon yang ditunjuk dan juga kepada organisasi yang diluar. |
| Penahanan, Penghapusan, dan | - Memperoleh, mempertahankan, mengamankan, dan mendokumentasi bukti yang ada. |

|  |  |
| --- | --- |
| Pemulihan | * Menahan insiden memberhentikan serangan DoS apabila serangan belum berhenti. * Mengidentifikasi dan mengurangi semua kerentanan yang digunakan. * Apabila belum tertahankan, jalankan filter berdasarkan sifat dari serangan jika memungkinkan. * Apabila belum tertahankan lakukan relokasi target. * Mengembalikan sistem yang terkena seperti sistem yang dapat dioperasikan sediakala. * Mengkonfirmasi sistem yang terkena dapat berfungsi secara normal. * Apabila diperlukan, jalankan monitoring tamba- han untuk melihat kemungkinan terjadinya aktifitas yang sama yang akan terjadi dimasa depan |
| Kegiatan Pasca Insiden | * Membuat laporan lanjutan * Mengadakan meeting yang membahas insiden tersebut |

* + 1. Insiden *Unauthorized Access*

**Tabel 3.5 Deteksi & Analisis Insiden *Unauthorized Access***

|  |  |
| --- | --- |
| **Tahap** | **Kontrol** |
| Deteksi dan analisis | * Memprioritaskan penanganan insiden berdasarkan pengaruh bisnis. * Mengidentifikasi sistem/resource mana yang terkena dan memprediksikan sistem/resource mana yang akan terkena selanjutnya. * Melakukan estimasi terhadap pengaruh secara tehnis saat ini dan yang akan berpotensi terkena dari insiden tersebut. * Melaporkan insiden kepada internal staf insiden yang ditunjuk dan juga kepada organisasi yang diluar. |

|  |  |
| --- | --- |
| Penahanan, Penghapusan, dan Pemulihan | * Melakukan penahanan pada awal kejadian * Memperoleh, mempertahankan, mengamankan, dan mendokumentasi bukti yang ada. * Mengkonfirmasi penahanan kejadian * Melakukan analisis lebih lanjut terhadap insiden tersebut dan menentukan apakah penahanan sudah cukup (termasuk memeriksa sistem lain untuk tKita-tKita intrusi) * Melaksanakan tindakan penahanan tambahan jika perlu * Mengidentifikasi dan mitigasi semua kerentanan yang telah dieksploitasi. * Menghapus semua komponen insiden dari system * Mengembalikan sistem yang terkena ke keadaan operasional semula * Menkonfirmasikan bahwa sistem yang terkena te- lah berfungsi normal * Apabila diperlukan, jalankan monitoring tamba- han untuk melihat kemungkinan terjadinya aktiti- tas yang sama yang akan terjadi dimasa depan |
| Kegiatan Pasca Insiden | * Membuat laporan lanjutan * Mengadakan meeting yang membahas insiden tersebut |

* + 1. Insiden Virus/Worm/Trojan

# Tabel 3.6 Deteksi & Analisis Insiden Virus/Worm/Trojan

|  |  |
| --- | --- |
| **Tahap** | **Kontrol** |
| Deteksi dan analisis | * Memprioritaskan penanganan insiden berdasarkan pengaruh terhadap bisnis instansi. * Mengidentifikasi sistem/resource mana yang terkena dan memprediksikan sistem/*resource* mana yang akan terkena selanjutnya. * Melakukan estimasi terhadap pengaruh secara teknis saat ini dan yang akan berpotensi terkena dari insiden |

|  |  |
| --- | --- |
|  | tersebut.  - Melaporkan insiden kepada internal staf insiden respon yang ditunjuk dan juga kepada organisasi yang diluar. |
| Penahanan, Penghapusan, dan Pemulihan | * Mengidentifikasi sistem yang terinfeksi * Disconnect semua sistem yang terinfeksi dari jaringan * Mitigasi kerentanan yang dimanfaatkan oleh malicious code * Apabila diperlukan, halangi mekanisme transmisi untuk malicious code * Disinfeksi, mengkarantina, menghapus, dan mengganti file yang terinfeksi * Mengurangi kerentanan dieksploitasi untuk host lain dalam organisasi * Mengkonfirmasikan bahwa sistem yang terkena telah berfungsi normal * Apabila diperlukan, jalankan monitoring tambahan untuk melihat kemungkinan terjadinya aktiti- tas yang sama yang akan terjadi dimasa depan. |
| Kegiatan Pasca Insiden | * Membuat laporan lanjutan * Mengadakan meeting yang membahas insiden tersebut |

* 1. **Mitigasi Ancaman**

# Tabel 3.7 Tindakan Mitigasi berdasarkan Jenis Ancaman

|  |  |  |
| --- | --- | --- |
| **Nama Ancaman** | **Gambaran Ancaman** | **Mitigasi** |
| DDoS | Jenis serangan terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber (resource) yang dimiliki oleh komputer tersebut sampai komputer tersebut tidak dapat menjalankan fungsinya dengan benar sehingga secara tidak langsung mencegah pengguna lain untuk memperoleh akses layanan dari komputer yang diserang.  Dalam sebuah serangan Denial of Service, si penyerang akan mencoba untuk mencegah akses seorang pengguna terhadap sistem atau jaringan dengan menggunakan beberapa cara, yakni sebagai berikut:   1. Membanjiri lalu lintas jaringan dengan banyak data sehingga lalu lintas jaringan yang datang dari pengguna yang terdaftar menjadi tidak dapat masuk ke dalam sistem jaringan. Teknik ini disebut sebagai traffic flooding. 2. Membanjiri jaringan dengan banyak request terhadap sebuah layanan jaringan yang disedakan oleh sebuah host sehingga request yang datang dari pengguna terdaftar tidak dapat dilayani oleh layanan tersebut. Teknik ini disebut sebagai request flooding. | * Indentifikasi aktifitas service apakah loadnya besar * Capturing aktifitas DDOS * Identifikasi Port serangan yang dilakakun DDOS * Melakukan pacthing terhadap bug – bug aplikasi yang memungkin bisa terserang DDOS * Melakukan monitoring IDS * Melakukan Blocking terhadap IP yang melakukan DDOS * Melakukan filtering dengan firewall dan dikombinasikan dengan perangkat monitoring IDS |

|  |  |  |
| --- | --- | --- |
|  | c. Mengganggu komunikasi antara sebuah host dan kliennya yang terdaftar dengan menggunakan banyak cara, termasuk dengan mengubah informasi konfigurasi sistem atau bahkan perusakan fisik terhadap komponen dan server |  |
| Malware | Adalah perangkat lunak yang di ciptakan untuk atau merusak sistem komputer atau jaringan komputer tanpa izin dari pemilik | * Identifikasi adanya port dan koneksi yang aktif * Identifikasi process yang mencurigakan * Identifikasi start up * Identifikasi service yang sedang berjalan * Identifikasi file dan folder yang mencurigakan * Melakukan monitoring IDS terhadapa anomaly malware * Menerapkan security policy terkait aturan sharing file dan browsing * Melakukan scanning menggunakan antivirus |
| Aplikasi Berbasis Web defacement | Adalah bentuk serangan untuk merubah tampilan Aplikasi Berbasis Web, hacker memanfaatkan vulnerability dari penggunaan cms open source yang tidak dimanajemen dengan baik ataupun karena password yang lemah. | * Backup log aktifitas dari webserver * Scanning dengan aplikasi Rootkit scanner * Backup source tools hacking * Selalu update CMS * Audit struktur pemrograman * Lakukan patching pada sistem operasi dan aplikasi |

|  |  |  |
| --- | --- | --- |
|  |  | * Dedicated hosting * Manajemen password * Manajemen user * Memasang FIM (File Integrity Monitoring) |
| Phishing | Adalah tindakan memperoleh informasi pribadi seperti User ID, Password dan data-data sensitif lainnya dengan menyamar sebagai orang atau organisasi yang berwenang melalui sebuah email. | * Pengecekan pola dari aktifitas phishing tersebut apakah melalui email atau link Aplikasi Berbasis Web * Pengecekan email header apakah IP tersebut legitimate * Pengecekan file folder yang mencurigakan di sisi server Aplikasi Berbasis Web * Backup log aktifitas Phishing * Menghapus file folder yang mencurigakan apabila phishing tersebut disisipkan di Aplikasi Berbasis Web * Menginformasikan IP dan Domain yang legitimate * Menginformasikan untuk analisis email header |