Keamanan Jaringan

Cyber Security Framework

Dosen Pembimbing :

Ferry Astika Saputra ST, M.Sc

Disusun oleh :

Iqbal Darmawan (3122640041)

KELAS LJ D4 IT B

JURUSAN D4 TEKNIK INFORMATIKA

DEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

2023

Cybersecurity Framework

Cybersecurity Framework (CSF) versi 2.0 adalah sebuah kerangka kerja yang dikembangkan oleh National Institute of Standards and Technology (NIST) di Amerika Serikat untuk membantu organisasi dalam mengembangkan, menerapkan, dan memperbaiki program keamanan siber mereka. Kerangka kerja ini didasarkan pada prinsip-prinsip manajemen risiko dan memberikan panduan tentang cara mengidentifikasi, melindungi, mendeteksi, merespons, dan memulihkan dari serangan keamanan siber.

CSF v2 terdiri dari tiga komponen utama, yaitu:

1. Core: merupakan inti dari kerangka kerja CSF v2 dan terdiri dari lima fungsi keamanan siber utama, yaitu Identify, Protect, Detect, Respond, dan Recover.
2. Profiles: digunakan untuk memetakan tujuan bisnis dan risiko keamanan siber pada kerangka kerja CSF v2.
3. Implementation Tiers: digunakan untuk membantu organisasi dalam mengevaluasi tingkat kematangan program keamanan siber mereka.

A. Core

   Komponen Core adalah inti dari kerangka kerja ini dan terdiri dari lima fungsi keamanan siber utama, yaitu:

   Identify: meliputi aktivitas untuk mengidentifikasi aset, risiko, dan kerentanan keamanan siber yang terkait dengan tujuan bisnis organisasi.
   Protect: meliputi aktivitas untuk melindungi aset dan sistem dari serangan keamanan siber dengan mengimplementasikan teknologi dan prosedur yang tepat.
   Detect: meliputi aktivitas untuk mendeteksi ancaman dan serangan keamanan siber dengan menggunakan teknologi dan prosedur yang tepat.
   Respond: meliputi aktivitas untuk merespons serangan keamanan siber dengan cepat dan tepat agar kerugian bisa diminimalisir.
   Recover: meliputi aktivitas untuk memulihkan aset dan sistem setelah terjadi serangan keamanan siber.

B. Profiles

   Komponen Profiles digunakan untuk memetakan tujuan bisnis dan risiko keamanan siber pada kerangka kerja CSF v2. Profiles ini membantu organisasi dalam menentukan fokus dan prioritas program keamanan siber mereka sesuai dengan kebutuhan bisnis dan risiko keamanan siber yang dihadapi.

C. Implementation Tiers
   Komponen Implementation Tiers digunakan untuk membantu organisasi dalam mengevaluasi tingkat kematangan program keamanan siber mereka. Implementation Tiers ini terdiri dari empat tingkatan, yaitu Partial, Risk-Informed, Repeatable, dan Adaptive. Setiap tingkatan ini menunjukkan tingkat kematangan program keamanan siber organisasi dan memberikan panduan tentang cara meningkatkan program keamanan siber tersebut.

Dalam implementasinya, CSF v2 dapat membantu organisasi dalam beberapa hal, antara lain:

1. Mengidentifikasi risiko keamanan siber yang terkait dengan tujuan bisnis organisasi.
2. Mengembangkan program keamanan siber yang terintegrasi dengan strategi bisnis organisasi.
3. Meningkatkan kesadaran dan keterampilan personel dalam menghadapi ancaman keamanan siber.

contoh implementasi CSF v2 pada suatu organisasi:

Tahap Pemetaan

Organisasi melakukan pemetaan terhadap aset-aset IT yang dimilikinya, seperti sistem, aplikasi, data, dan infrastruktur. Selain itu, organisasi juga melakukan identifikasi terhadap ancaman-ancaman yang mungkin terjadi pada aset-aset tersebut.

Tahap Perlindungan

Organisasi membuat kebijakan keamanan untuk melindungi aset-aset IT yang dimilikinya. Contohnya adalah membuat kebijakan untuk penggunaan kata sandi yang kuat, membatasi akses ke aset-aset penting hanya untuk pegawai yang membutuhkan, dan menggunakan sistem proteksi dari serangan malware.

Tahap Deteksi

Organisasi menggunakan sistem pendeteksi yang otomatis atau manual untuk memantau aset-aset ITnya dan mendeteksi adanya serangan atau ancaman keamanan lainnya. Contohnya, menggunakan software antivirus atau IDS (Intrusion Detection System) untuk mendeteksi adanya malware atau serangan hacking.

Tahap Respons

Organisasi membuat rencana respons terhadap ancaman-ancaman keamanan yang mungkin terjadi. Contohnya, membuat rencana darurat dalam hal terjadi serangan DDoS atau serangan malware yang parah.

Tahap Pemulihan

Organisasi membuat rencana pemulihan untuk mengatasi kerusakan pada sistem dan aset-aset IT yang terdampak oleh serangan atau bencana. Contohnya, melakukan backup data secara berkala dan membuat rencana pemulihan sistem yang telah terinfeksi oleh malware atau terkena serangan hacking.

Tahap Evaluasi

Organisasi melakukan evaluasi terhadap semua proses yang telah dilakukan untuk memastikan bahwa kebijakan keamanan dan rencana yang telah dibuat efektif dan terus ditingkatkan sesuai dengan perkembangan teknologi dan ancaman-ancaman keamanan yang baru.