LAPORAN

KEMANAN JARINGAN

Teacher : Dr. Ferry Astika Saputra ST, M.Sc

CYBER SECURITY FRAMEWORK

DISUSUN OLEH :

SYIHAB MUHAMMAD UBAIDILLAH

3122640043

PROGRAM STUDI TEKNIK INFORMATIKA

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

D4 TI LANJUT JENJANG

Pendahuluan

Dalam era digital yang terus berkembang, ancaman keamanan siber semakin meningkat. Serangan siber dapat mengakibatkan kerugian finansial, pencurian data sensitif, atau bahkan gangguan pada infrastruktur kritis suatu negara. Untuk melawan ancaman ini, diperlukan pendekatan yang komprehensif dan terstruktur dalam mengelola keamanan siber. Dalam konteks ini, Kerangka Kerja Keamanan Cyber (Cybersecurity Framework) yang dikembangkan oleh National Institute of Standards and Technology (NIST) Amerika Serikat menjadi alat yang sangat berharga.

Versi kedua dari Cybersecurity Framework (CSF) yang dikembangkan oleh National Institute of Standards and Technology (NIST) adalah langkah penting dalam meningkatkan keamanan siber.

Tujuan

Tujuan dari esai ini adalah untuk membahas peran yang dimainkan oleh Kerangka Kerja Keamanan Cyber NIST dalam meningkatkan keamanan siber secara umum. Kami akan menganalisis komponen utama kerangka kerja, proses implementasi, dan manfaat yang diperoleh melalui penggunaannya.

1. **Konteks dan Tujuan:**

CSF versi 2 bertujuan untuk memperkuat pemahaman dan implementasi kerangka kerja sebelumnya dengan memperkenalkan perbaikan berdasarkan umpan balik dari pengguna CSF versi sebelumnya. CSF versi 2 dirancang untuk menjadi lebih responsif terhadap lingkungan keamanan siber yang terus berkembang.

2. **Pendekatan Integritas Tinggi:**

CSF versi 2 mengadopsi pendekatan integritas tinggi, dengan fokus pada pemahaman yang lebih baik tentang organisasi dan tujuan bisnis. Ini membantu organisasi untuk mengenali aset yang perlu dilindungi, risiko yang relevan, serta memastikan implementasi kontrol keamanan yang sesuai.

3. **Prinsip Dasar:**

CSF versi 2 menggabungkan prinsip dasar yang mencakup Risiko Didukung, Kerangka yang Dinamis, Fokus pada Kemampuan, dan Pengejaran Kolaboratif. Prinsip-prinsip ini membantu organisasi untuk membangun dan memperbaiki kemampuan keamanan mereka secara berkelanjutan.

4. **Komponen Utama:**

CSF versi 2 terdiri dari tiga komponen utama, yaitu: Framework Core, Implementation Tiers, dan Profiles.

- Framework Core: Memetakan komponen keamanan siber ke dalam lima kategori, yaitu Identify, Protect, Detect, Respond, dan Recover. Ini membantu organisasi dalam mengembangkan strategi yang holistik dalam mengelola risiko keamanan.
- Implementation Tiers: Memberikan penilaian tentang kedewasaan dan tingkat kematangan organisasi dalam mengimplementasikan praktik keamanan siber. Terdapat empat tingkatan implementasi: Partial, Risk Informed, Repeatable, dan Adaptive.
- Profiles: Digunakan untuk menyesuaikan CSF dengan kebutuhan organisasi tertentu. Profil memetakan kebutuhan keamanan dan kontrol keamanan yang relevan ke dalam kerangka kerja.

5. **Manfaat CSF versi 2:**

- Meningkatkan pemahaman tentang aset, risiko, dan kontrol keamanan yang relevan.

- Memfasilitasi komunikasi yang lebih baik antara pemangku kepentingan dalam organisasi.
- Memungkinkan pemantauan dan pengukuran kemampuan keamanan secara sistematis.
- Membantu dalam identifikasi dan prioritisasi upaya perbaikan keamanan.
- Mendukung peningkatan kemampuan organisasi dalam menghadapi ancaman siber.

Dalam keseluruhan, CSF versi 2 merupakan pembaruan penting dari kerangka kerja sebelumnya yang memberikan arah yang lebih kuat dalam mengelola keamanan siber. Dengan pendekatan integritas tinggi, prinsip dasar yang kuat, dan komponen yang terstruktur, CSF versi 2 memungkinkan organisasi untuk menghadapi tantangan keamanan siber dengan lebih baik dan meningkatkan kemampuan mereka dalam melindungi aset penting dari serangan dan ancaman.

Pengembangan

1. Pendahuluan tentang NIST Cybersecurity Framework
    a. Latar belakang dan tujuan pengembangan.
    b. Komponen utama kerangka kerja: Pemahaman, Pengelolaan Risiko, dan Respon.
2. Komponen Kerangka Kerja NIST
    a. Kategori: Identifikasi, Perlindungan, Deteksi, Respons, dan Pemulihan.
    b. Subkategori dan kelompok kontrol yang relevan.

3. Proses Implementasi Kerangka Kerja NIST
    a. Langkah-langkah evaluasi awal
    b. Penilaian risiko dan kebutuhan
    c. Penyusunan rencana perlindungan dan penerapan kontrol
    d. Pengawasan, deteksi, dan respons terhadap serangan
    e. Proses pemulihan dan pembelajaran

4. Manfaat dan Keuntungan Kerangka Kerja NIST
    a. Meningkatkan kemampuan identifikasi dan perlindungan
    b. Meningkatkan resiliensi terhadap serangan dan ancaman
    c. Meningkatkan kerjasama dan komunikasi dalam industry

5. Studi Kasus: Keberhasilan Implementasi Kerangka Kerja NIST
    a. Contoh perusahaan yang berhasil menerapkan kerangka kerja
    b. Pengurangan risiko dan dampak serangan setelah implementasi

Kesimpulan

Kerangka Kerja Keamanan Cyber NIST adalah alat yang efektif dalam meningkatkan keamanan siber. Dalam esai ini, kami telah menggambarkan komponen utama, proses implementasi, dan manfaat yang diperoleh melalui penggunaan kerangka kerja ini. Dengan adopsi dan penerapan yang tepat, organisasi dan perusahaan dapat meningkatkan kemampuan mereka dalam mengelola risiko, mendeteksi serangan, dan memulihkan diri setelah terjadinya insiden keamanan.