TUGAS

KEAMANAN JARINGAN

“Cyber Security Framework V2”

Nama : Mega Putri Rahmawati Darta

Kelas : D4 LJ IT B

NRP : 3122640038

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

TAHUN AJARAN 2022/2023

NIST (National Institute of Standards and Technlogy) awalnya menghasilkan Framework pada tahun 2014 dan memperbaruinya pada tahun 2018 dengan CSF 1.1. CSF diperbarui secara terbuka dengan masukan dari pemerintah, akademisi, dan industri, termasuk melalui lokakarya, tinjauan dan komentar publik, dan lainnya bentuk-bentuk keterlibatan.

Versi “CSF 2.0” mencerminkan keamanan siber yang berkembang tetapi kebutuhan masyarakat akan mendorong luas dan isi perubahan. Awal timeline CSF 2.0 sebagai berikut ini :

Perkembangan CSF 2.0 bersifat iterative dan sangat didasarkan pada sketor baik swasta dan public. Draft CSF 2.0 didasarkan dari feedback yang diterima dari :

1. 134 respon RFI CyberSecurity NIST Februari 2022
2. Lokakarya #1 “Journey to the NIST Cybersecurity Framework 2.0” Agustus 2022,
3. Umpan balik dari organisasi yang memanfaatkan CSF
4. Partisipasi NIST di konferensi, webinar, meja bundar, dan pertemuan di seluruh dunia

A. POTENSI PERUBAHAN SIGNIFIKAN IN CSF 2.0

1. CSF 2.0 akan secara eksplisit mengenali penggunaan luas CSF untuk memperjelas potensinya aplikasi
   - Ubah judul dan teks CSF untuk mencerminkan tujuan penggunaannya oleh semua organisasi
     - CSF 2.0 akan menggunakan nama yang lebih luas dan umum digunakan, "Cybersecurity Framework".
     - Ruang lingkup CSF 2.0 akan mencakup semua organisasi lintas pemerintahan, industri, dan akademisi, termasuk namun tidak terbatas pada infrastruktur kritis.
     - Kategori dan Subkategori Inti CSF yang khusus untuk infrastruktur kritis, seperti ID.BE-2 dan ID.RM-3, akan diperluas.
   - Lingkup CSF untuk memastikannya bermanfaat bagi organisasi terlepas dari sektor, jenis, atau ukuran
     - NIST akan meningkatkan upayanya untuk memastikan Framework sangat membantu organisasi – terlepas dari sektor, jenis, atau ukuran – dalam menangani cybersecurity menantang
     - Mendorong semua pihak yang berkepentingan untuk berpartisipasi dalam proses tersebut
   - Meningkatkan kerjasama dan keterlibatan internasional
     - NIST akan memprioritaskan pertukaran dengan pemerintah asing dan industri sebagai bagian dari pengembangan CSF 2.0.
     - NIST juga akan memprioritaskan bekerja sama dengan organisasi untuk berkembang terjemahan CSF 2.0 sehubungan dengan perkembangannya, membangun upaya sebelumnya untuk menerjemahkan CSF 1.1 dan sumber daya yang relevan.
2. CSF 2.0 akan tetap menjadi kerangka kerja, menyediakan konteks dan koneksi ke yang sudah ada standar dan sumber daya
   - Pertahankan tingkat detail CSF saat ini
     - NIST bertujuan untuk mempertahankan tingkat detail dan spesifisitas saat ini dalam CSF 2.0 untuk memastikannya tetap dapat diskalakan dan fleksibel untuk berbagai organisasi.
     - Framework akan terus menyediakan struktur pengorganisasian umum untuk banyak orang pendekatan keamanan siber, termasuk dengan memanfaatkan dan menghubungkan, tetapi tidak mengganti, standar dan pedoman yang diakui secara global.
   - Kaitkan CSF dengan jelas ke kerangka kerja NIST lainnya
     - CSF 1.1 diterbitkan sebelum publikasi Kerangka Privasi; Karena itu, CSF Bagian 3.6, Metodologi untuk Melindungi Privasi dan Kebebasan Sipil dapat diamandemen di CSF 2.0 untuk membahas bagaimana Kerangka Privasi dapat dimanfaatkan saat menerapkan CSF.

- Manfaatkan Cybersecurity dan Alat Referensi Privasi untuk CSF 2.0 Core online
    - Selain format PDF dan Excel, CSF 2.0 akan dipamerkan melalui yang baru diluncurkan Cybersecurity and Privacy Reference Tool (CPRT) NIST. CPRT menawarkan format yang dapat dibaca mesin dan antarmuka pengguna yang konsisten untuk mengakses data referensi dari cybersecurity NIST dan standar privasi, pedoman, dan kerangka kerja, serta pendekatan yang fleksibel untuk karakterisasi hubungan antara standar, pedoman, dan kerangka kerja serta berbagai aplikasi dan teknologi.
- Gunakan Referensi Informatif online yang dapat diperbarui
    - Di CSF 2.0, NIST akan beralih ke penggunaan referensi online yang dapat diperbarui yang ditampilkan melalui CPRT.
- Gunakan Referensi Informatif untuk memberikan lebih banyak panduan untuk menerapkan CSF
    - Akan memungkinkan pemetaan untuk CSF 2.0 di Fungsi dan Kategori level, selain level Subkategori, mendukung koneksi ke sumber daya tambahan.
- Tetap netral teknologi dan vendor, tetapi mencerminkan perubahan dalam keamanan siber praktik
    - CSF 2.0 akan tetap netral teknologi dan vendor
    - CSF 2.0 akan memperluas pertimbangan hasil dalam CSF Menanggapi dan Memulihkan Fungsi
    - CSF 2.0 dapat mencakup lebih banyak pertimbangan tentang hasil perencanaan respons dan pemulihan, meningkatkan keselarasan dengan Panduan Penanganan Insiden Keamanan Komputer yang populer, serta memanfaatkan Panduan untuk Pemulihan Peristiwa Keamanan Siber.
    - NIST akan mengeksplorasi pembaruan Identitas CSF Kategori Manajemen, Otentikasi, dan Kontrol Akses, termasuk potensi penataan ulang Subkategori, untuk mencerminkan komponen model identitas digital dan fase siklus hidup identitas digital lebih jelas

3. CSF 2.0 (dan sumber pendamping) akan menyertakan panduan yang diperbarui dan diperluas tentang implementasi Framework
    - Tambahkan contoh penerapan untuk Subkategori CSF
        - CSF 2.0 akan menyertakan contoh implementasi nosional dari proses yang ringkas dan berorientasi pada Tindakan dan kegiatan untuk membantu mencapai hasil Subkategori CSF, selain panduan disediakan dalam Referensi Informatif CSF.
    - Kembangkan template Profil CSF
        - NIST akan menghasilkan template dasar opsional untuk Profil CSF menyarankan format dan area untuk dipertimbangkan dalam Profil.
    - Tingkatkan situs web CSF untuk menyoroti sumber daya implementasi
        - NIST akan mengubah situs web CSF untuk menyegarkan konten dan meningkatkan kegunaan.

    - NIST akan menghapus sumber daya yang sudah usang dan menambahkan sumber daya terkini.
4. CSF 2.0 akan menekankan pentingnya tata kelola keamanan siber
    - Tambahkan Fungsi Pemerintahan baru
        - CSF 2.0 akan menyertakan Fungsi "Pemerintah" baru untuk menekankan hasil tata kelola manajemen risiko keamanan siber.
        - Tata kelola keamanan siber dapat mencakup penentuan prioritas dan toleransi risiko organisasi, pelanggan, dan masyarakat yang lebih luas; penilaian dari risiko dan dampak keamanan siber; penetapan kebijakan dan prosedur keamanan siber; Dan pemahaman tentang peran dan tanggung jawab keamanan siber.
        - Fungsi Pemerintahan baru di CSF 2.0 akan menginformasikan dan mendukung Fungsi lainnya.
        - CSF 2.0 juga akan memperluas pertimbangan topik terkait tata kelola di Fungsi baru.
    - Meningkatkan pembahasan hubungan dengan manajemen risiko
        - CSF 2.0 akan menjelaskan bagaimana sebuah proses manajemen risiko yang mendasari sangat penting untuk mengidentifikasi, menganalisis, memprioritaskan, menanggapi, dan memantau risiko, bagaimana hasil CSF mendukung keputusan respons risiko (menerima, mitigasi, transfer, hindari), dan berbagai contoh proses manajemen risiko (misalnya, Risiko Management Framework, ISO 31000) yang dapat digunakan untuk mendukung implementasi CSF.
5. CSF 2.0 akan menekankan pentingnya cybersecurity supply chain risk management (C-SCRM)
    - Memperluas cakupan rantai pasokan
        - CSF 2.0 harus memperjelas pentingnya organisasi mengidentifikasi, menilai, dan mengelola risiko pihak pertama dan ketiga. Namun, risiko pihak ketiga mungkin melibatkan penilaian dan pengawasan yang berbeda yang sering ditangani secara terpisah tim/organisasi.
6. CSF 2.0 akan memajukan pemahaman tentang pengukuran keamanan siber dan penilaian
    - Perjelas bagaimana memanfaatkan CSF dapat mendukung pengukuran dan penilaian dari program keamanan siber
        - CSF 2.0 akan memperjelas bahwa dengan memanfaatkan CSF, organisasi memiliki taksonomi yang sama dan leksikon untuk mengkomunikasikan hasil pengukuran dan upaya penilaian mereka, terlepas dari proses manajemen risiko yang mendasarinya.
        - Tujuan utama pengukuran dan penilaian keamanan siber adalah untuk menentukan seberapa baik mereka mengelola risiko keamanan siber, dan jika serta bagaimana mereka terus meningkat.
    - Berikan contoh pengukuran dan penilaian menggunakan CSF

    - Risiko, prioritas, dan sistem setiap organisasi adalah unik, sehingga metode dan tindakan digunakan untuk mencapai hasil yang dijelaskan oleh Kerangka Inti bervariasi.
    - CSF 2.0 akan menyertakan contoh bagaimana organisasi telah menggunakan CSF untuk menilai dan mengomunikasikan kemampuan keamanan siber mereka
- Perbarui Panduan Pengukuran Kinerja NIST untuk Keamanan Informasi
    - NIST memperbarui dokumen panduan pengukuran andalannya, Pengukuran Kinerja Panduan untuk Keamanan Informasi. SP 800-55r2 memberikan panduan kepada organisasi tentang penggunaan langkah-langkah untuk meningkatkan pengambilan keputusan, kinerja, dan akuntabilitas keamanan siber program atau sistem informasi.
- Berikan panduan tambahan tentang Tingkatan Implementasi Framework
    - Tingkatan CSF menyediakan mekanisme bagi organisasi untuk melihat dan memahami pendekatan mereka risiko keamanan siber serta proses dan program yang ada untuk mengelola risiko tersebut.