RESUME CSF V2 CYBER SECURITY

Makalah Konsep NIST Cybersecurity Framework 2.0: Potensi Pembaruan Signifikan pada Kerangka Cybersecurity

DI SUSUN OLEH :

Nadya Indah Trisnawati (3122640034)

D4 LJ IT B

PROGRAM STUDI TEKNIK INFORMATIKA

DEPARTEMEN TEKNIK INFORMATIKA DAN KOMPUTER

POLITEKNIK ELEKTRONIKA NEGERI SURABAYA

1. Pendahuluan

Kerangka Keamanan Siber NIST (CSF atau Framework) memberikan panduan kepada organisasi untuk lebih memahami, mengelola, mengurangi, dan mengomunikasikan risiko keamanan siber. Ini adalah dasar dan sumber daya penting yang digunakan oleh semua sektor di seluruh dunia. Meskipun risiko keamanan siber berkembang, banyak responden NIST Cybersecurity RFI melaporkan bahwa CSF tetap efektif untuk menangani risiko keamanan siber dengan memfasilitasi tata kelola dan program manajemen risiko dan meningkatkan komunikasi di dalam dan lintas organisasi. CSF telah diadopsi secara sukarela dan dalam kebijakan dan mandat pemerintah di semua tingkatan di seluruh dunia, mencerminkan sifatnya yang tahan lama dan fleksibel untuk melampaui risiko, sektor, teknologi, dan batas negara.

CSF dimaksudkan untuk menjadi dokumen hidup yang disempurnakan dan diperbaiki dari waktu ke waktu. Otoritas hukum untuk CSF mengarahkan NIST untuk "memfasilitasi dan mendukung pengembangan" dari Kerangka kerja dan “berkoordinasi erat dan teratur” dengan organisasi terkait. 1 Dengan ekstensif keterlibatan masyarakat, NIST 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. Dengan pembaruan ini, NIST terbuka untuk membuat perubahan yang lebih substansial daripada di pembaruan sebelumnya. Versi “CSF 2.0” mencerminkan lanskap keamanan siber yang berkembang tetapi kebutuhan masyarakat akan mendorong luas dan isi perubahan. CSF 2.0 awal garis waktu diusulkan dalam gambar ini:

Pengembangan CSF 2.0 bersifat iteratif dan sangat didasarkan pada input sektor swasta dan publik. Kemajuan dalam upaya CSF 2.0, serta cara untuk terlibat, dapat ditemukan di NIST CSF 2.0 halaman web. Makalah ini didasarkan pada umpan balik yang diterima sejauh ini melalui:

1. 134 respons terhadap RFI Keamanan Siber NIST Februari 2022;
2. Lokakarya #1 “Journey to the NIST Cybersecurity Framework 2.0” Agustus 2022, dihadiri hampir 4.000 peserta dari 100 negara;
3. Umpan balik dari organisasi yang memanfaatkan CSF; Dan
4. Partisipasi NIST di konferensi, webinar, meja bundar, dan pertemuan di seluruh dunia.

2. **CSF 2.0 akan secara eksplisit mengenali penggunaan luas CSF untuk memperjelas potensinya aplikasi**
    a. Mengubah judul dan teks CSF untuk mencerminkan tujuan penggunaannya oleh semua organisasi

        Ruang lingkup CSF 2.0 akan mencakup semua organisasi lintas pemerintahan, industri, dan akademisi, namun tidak terbatas pada infrastruktur kritis. Referensi ke infrastruktur kritis di CSF dapat dipertahankan Perubahan ini tidak dimaksudkan untuk mengurangi CSF relevansi dengan organisasi infrastruktur kritis, termasuk pentingnya memastikan keamanan dan ketahanan infrastruktur kritis bangsa kita, tetapi untuk merangkul dan meningkatkannya penggunaan yang lebih luas.
    b. Lingkup CSF untuk memastikannya bermanfaat bagi organisasi terlepas dari sektor, jenis, atau ukuran

        Sejak publikasi CSF 1.1, Kongres secara eksplisit mengarahkan NIST untuk mempertimbangkan usaha kecil dan kebutuhan cybersecurity institusi pendidikan tinggi di CSF. NIST akan meningkatkan upayanya untuk memastikan Framework sangat membantu organisasi dalam menangani cybersecurity menantang dan mendorong semua pihak yang berkepentingan untuk berpartisipasi dalam proses tersebut.
    c. Meningkatkan kerjasama dan keterlibatan internasional

        NIST akan terus terlibat secara langsung dan melalui kemitraan antar lembaga untuk berbagi manfaat penggunaan CSF, serta untuk meminta masukan tentang potensi perubahan, sehingga CSF dapat terus diakui sebagai suatu sumber daya internasional.

3. **CSF 2.0 akan tetap menjadi kerangka kerja, menyediakan konteks dan koneksi ke yang sudah ada standar dan sumber daya**
    a. Mempertahankan tingkat detail CSF saat ini.

        Ada nilai yang diakui dengan jelas dalam mengatur hasil keamanan siber oleh Fungsi CSF, termasuk menyediakan konteks untuk bahasa yang lebih spesifik yang biasa digunakan di sebagian besar keamanan siber standar. Tidak ada kekurangan standar keamanan siber, praktik terbaik, daftar periksa, tujuan, dan sumber daya.
    b. Mengaitkan CSF dengan jelas ke kerangka kerja NIST lainnya.

        Kerangka Kerja Manajemen Risiko, Kerangka Kerja Privasi, Prakarsa Nasional untuk Tenaga Kerja Pendidikan Cybersecurity Framework for Cybersecurity, dan Secure Software Development Framework. masing-masing akan tetap kerangka kerja yang terpisah. Masing-masing berfokus pada topik tertentu yang layak untuk panduan khusus. Namun, seperti yang ditunjukkan oleh pemberi komentar, setiap kerangka kerja memiliki hubungan dengan CSF, jadi mereka akan dirujuk sebagai panduan baik dalam CSF 2.0 atau materi pendamping, seperti pemetaan.
    c. Memanfaatkan 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 Keamanan Siber dan Alat Referensi Privasi (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.

d. Menggunakan Referensi Informatif online yang dapat diperbarui.

   Di CSF 2.0, NIST akan beralih ke penggunaan referensi online yang dapat diperbarui yang ditampilkan melalui CPRT. Sejak publikasi CSF 1.1, beberapa sumber telah dipetakan ke CSF selanjutnya yang termasuk dalam CSF 1.1 Core.

e. Menggunakan Referensi Informatif untuk memberikan lebih banyak panduan untuk menerapkan CSF.

   NIST akan bekerja dengan masyarakat untuk mendorong dan mengaktifkan produksi pemetaan yang mendukung CSF 2.0. Ada minat masyarakat yang kuat terhadap pemetaan tambahan; responden untuk RFI meminta pemetaan ke hampir 50 standar keamanan siber, pedoman, dan lainnya kerangka kerja, banyak yang ditulis oleh organisasi lain.

f. Tetap netral teknologi dan vendor, tetapi mencerminkan perubahan dalam keamanan cybersecurity praktik.

   NIST berkolaborasi dengan komunitas untuk mengembangkan pemetaan khusus teknologi untuk dideskripsikan hubungan antara kemampuan keamanan yang dapat dicapai dengan mengkonfigurasi atau mengaktifkan fitur keamanan dalam tumpukan teknologi dan hasil yang diinginkan dijelaskan dalam CSF.

4. CSF 2.0 (dan sumber pendamping) akan menyertakan panduan yang diperbarui dan diperluas tentang implementasi Framework

a. Menambahkan contoh penerapan untuk Subkategori CSF

   Membantu mengklarifikasi arti dan maksud dari setiap Subkategori dan memberikan ide implementasi tingkat tinggi dalam Inti CSF bagi mereka yang belum terlalu familiar dengan standar keamanan siber terperinci yang diidentifikasi dalam Referensi Informatif. Contohnya juga dapat membantu mengatasi sifat teknologi dan teknik keamanan siber yang terus berkembang menyoroti kemungkinan perbedaan dalam implementasi untuk platform seperti IT, IoT, OT, dan cloud computing.

b. Mengembangkan template Profil CSF

   NIST telah menghasilkan contoh untuk beberapa Profil khusus sektor dan ancaman yang mungkin ada dimanfaatkan oleh suatu organisasi untuk membangun Profil organisasinya. Profil sampel ini membuatnya lebih mudah bagi organisasi untuk menerapkan CSF dengan memprioritaskan dan menyelaraskan hasil CSF dengan risiko dan standar khusus sektor dan ancaman.

c. Meningkatkan situs web CSF untuk menyoroti sumber daya implementasi

   Banyak sumber daya yang dikembangkan oleh NIST dan eksternal organisasi, termasuk sampel CSF, pemetaan, panduan, alat, studi kasus, publikasi terkait (seperti Panduan Memulai Cepat CSF). Pembaruan ke Framework juga memberikan kesempatan untuk meningkatkan kesadaran akan sumber daya yang ada sebagai mengidentifikasi yang baru.

5. **CSF 2.0 akan menekankan pentingnya tata kelola keamanan cyber security**
   a. Menambahkan Fungsi Pemerintahan baru
      Mencerminkan input substansial untuk NIST, CSF 2.0 akan menyertakan Fungsi "Pemerintah" baru untuk menekankan hasil tata kelola manajemen risiko keamanan siber. Sedangkan kelima Fungsi CSF telah diadopsi secara luas dalam kebijakan nasional dan internasional, termasuk standar ISO.
   b. Meningkatkan pembahasan hubungan dengan manajemen risiko
      Merevisi CSF menawarkan kesempatan untuk mengklarifikasi hubungan antara tata kelola dan manajemen risiko keamanan siber di seluruh narasi CSF dan Core. 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.

6. **CSF 2.0 akan menekankan pentingnya risiko rantai pasokan keamanan cyber manajemen (C-SCRM)**
   a. Memperluas cakupan rantai pasokan.
      Mengelola keamanan cyber dalam rantai pasokan adalah salah satu tambahan utama dalam pembaruan terakhir ke CSF. Sejak itu, lebih banyak perhatian telah diberikan untuk mengembangkan panduan untuk meningkat kepercayaan dan jaminan dalam produk dan layanan teknologi, termasuk panduan yang dikembangkan berdasarkan pada Perintah Eksekutif, “Improving the Nation’s Cybersecurity” (EO 14028).

7. **CSF 2.0 akan memajukan pemahaman tentang pengukuran keamanan siber dan penilaian**
   a. Memperjelas 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.
   b. Memberikan 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. Dengan demikian, pengukuran dan penilaian hasil bervariasi tergantung pada konteksnya.
   c. Memperbarui Panduan Pengukuran Kinerja NIST 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.
   d. Memberikan panduan tambahan tentang Tingkatan Implementasi Framework
      CSF 2.0 akan mengklarifikasi ruang lingkup dan penerapan Tingkatan untuk mengatasi ketahanan risiko proses manajemen, program, dan komunikasi eksternal.