KEAMANAN JARINGAN

Cyber Security Framework

Disusun Oleh :
Muhammad Dzaky Mahfuzh
3122640050
D4 LJ B
Teknik Informatika

Politeknik Elektronika Negeri Surabaya
Kampus ITS Keputih Sukolilo Surabaya 60111
Telp. 031-5947280, 031-5946114, Fax:031-5946114

Cyber Security Framework

CSF atau **Cyber Security Framework** merupakan sebuah framework yang berfokus pada meningkatkan Cyber Security dari sebuah framework yang mana dapat berkembang dan ditingkatkan seiring waktu berjalan, untuk selalu beradaptasi dengan tren teknologi yang terus berkembang dan ancaman cyber terbaru.

Berawal dari amerika serikat yang mulai menganggap bahwa ancaman eksploitasi pada infrastuktur negara merupakan hal yang kritis dan dapat mempengaruhi kestabilan keamanan, ekonomi dan kesehatan. dan dapat disandingkan dengan resiko keuangan pada suatu negara, hal ini dianggap akan mempengaruhi sektor pendapatan dari perusahaan karna dapat membahayakan kemampuan organisasi dalam berinovasi, mempertahankan, dan mendapatkan pelanggan. Oleh karna itu pada 12 februari 2013, presiden amerika serikat mengeluarkan dekrit Executive Order 13636 yang isinya adalah untuk meningkatkan cyber security pada infrastruktur yang dianggap kritis. Dengan adanya kebijakan untuk meningkatkan keamanan dan ketahanan infrastruktur yang dianggap kritis, menjaga lingkuangan cyber yang mendorong efisiensi, inovasi, dan kemakmuran ekonomi dengan tetap mengedepankan keselamatan, keamanan, kerahasiaan bisnis, privasi, dan kebebasan rakyat sipil.

setelah hasil kolaborasi banyak pihak dalam membuat cyber security framework hasilnya adalah framework cyber security versi stabil 1.1 yang memprioritaskan recover, identify, protect, detect, dan respon atau disebut sebagai framework core.

- Identifikasi - Mengembangkan pemahaman organisasi untuk mengelola risiko cybersecurity untuk sistem, aset, data, dan kemampuan.

  Kegiatan dalam fungsi Identifikasi merupakan dasar untuk penggunaan yang efektif dari Framework. Memahami konteks bisnis, sumber daya yang mendukung fungsi kritis, dan risiko cybersecurity terkait memungkinkan organisasi untuk fokus dan memprioritaskan upaya, konsisten dengan strategi manajemen risiko dan kebutuhan bisnis. Contoh kategori hasil dalam Fungsi ini meliputi: Manajemen Aset, Lingkungan bisnis, Pemerintahan, dan Strategi Manajemen Risiko.

- Melindungi - Mengembangkan dan melaksanakan pengamanan yang memadai untuk memastikan pengirimanlayanan infrastruktur yang kritis.

  Fungsi Protect mendukung kemampuan untuk membatasi atau mengandung dampak dari potensi kejadian cybersecurity. Contoh Categories hasil dalam Fungsi ini meliputi:Kontrol akses; Kesadaran dan Pelatihan, Keamanan data, Proses dan Prosedur Perlindungan informasi, Pemeliharaan; dan pelindung Teknologi.

- Respond - Mengembangkan dan melaksanakan kegiatan sesuai untuk mengambil tindakan pada kejadian cybersecurity yang terdeteksi.

  Fungsi Respond mendukung kemampuan untuk mengkarantina dampak dari potensial kejadian cybersecurity. Contoh dari keluaran Categories dalam Fungsi ini meliputi: Perencanaan Respon; Komunikasi, Analisa, mitigasi, dan Perbaikan.

- Recover - Mengembangkan dan melaksanakan kegiatan mempertahankan rencana untuk ketahanan dan untuk memulihkan setiap kemampuan atau jasa yang terganggu karena kejadian cybersecurity.

Fungsi Recover mendukung pemulihan tepat waktu untuk operasi yang normal untuk mengurangi dampak dari kejadian cybersecurity. Contoh Categories keluaran dalam fungsi ini meliputi: Recovery Planning, Perbaikan, dan Komunikasi.

Cyber Security Framework Version 2.0

Pada saat ini telah dikembangkan versi lanjutan dari cyber security framework dari versi 1.1 menuju ke versi 2.0 yang mana saat ini masuk ke dalam tahap pengerjaan dan melihat dari timeline yang telah dibagikan terlihat bahwa cyber security framework versi 2.0 akan rilis pada 2024. Pembaruan yang ada pada cyber security framework versi 2.0 merupakan hasil kolaborasi dari banyak pihak, dimana National Institute of Standards and Technology mencari dan menerima berbagai jenis informasi untuk memperhitungkan dan meningkatkan sumber cyber security dan supply chain risk management. National Institute of Standards and Technology (NIST) menerima lebih dari 130 tanggapan RFI, termasuk banyak komentar yang disampaikan bersama oleh berbagai organisasi atau asosiasi yang mewakili banyak organisasi.