(https://infrasec.proxsisgroup.com)

Mengenal NIST CSF: Pengertian, Sejarah, Regulasi, Adobsi di Indonesia dan Rekomendasi Asesment Gratisnya

Kita perlu tahu salah satu kerangka kerja keamanan siber paling andal di dunia, yaitu NIST *Cybersecurity Framework* (CSF). Di era digital seperti sekarang ini, kita sering mendengar istilah keamanan siber, tetapi apa sebenarnya yang mendasarinya? Apakah ada panduan yang bisa membantu perusahaan atau bahkan kita sendiri untuk melindungi diri dari ancaman siber? Jawabannya ada, dan salah satunya adalah NIST CSF yang akan kita bahas tuntas di sini.

Bagi Anda yang berkecimpung di dunia teknologi, khususnya keamanan informasi, nama NIST CSF mungkin sudah tidak asing lagi. Namun, bagi yang baru mengenalnya, jangan khawatir! Artikel ini dirancang khusus dengan bahasa yang mudah dipahami, tanpa menghilangkan esensi

Admin Biztech

pentingnya. Kita akan mengupas tuntas mulai dari pengertian, sejarah, hingga bagaimana kerangka kerja ini diadopsi di Indonesia. Siap untuk menjelajahi lebih dalam? Mari kita mulai!

Mengenal NIST CSF: Apa Itu Sebenarnya?

NIST *Cybersecurity Framework* (CSF) adalah sebuah panduan yang dibuat oleh *National Institute of Standards and Technology* (NIST) di Amerika Serikat. Tujuannya sangat jelas, yaitu membantu organisasi dari berbagai ukuran dan sektor untuk mengelola serta mengurangi risiko keamanan siber secara efektif. Kerangka kerja ini bersifat sukarela dan tidak mengikat, namun banyak diadopsi karena pendekatannya yang komprehensif dan fleksibel.

NIST CSF tidak hanya berfokus pada teknologi, tetapi juga pada bagaimana manajemen risiko, proses, dan orang-orang di dalam organisasi berinteraksi. Pendekatan ini membuat kerangka kerja ini sangat relevan untuk siapa saja, mulai dari perusahaan kecil hingga korporasi besar, dan bahkan bagi lembaga pemerintahan.

Baca juga : NIST Cybersecurity Framework: Implementasi & Manfaat untuk Bisnis (https://infrasec.proxsisgroup.com/nist-cybersecurity-framework-implementasi-manfaat-untuk-bisnis/)

Sejarah Singkat di Balik Lahirnya NIST CSF

NIST CSF lahir dari kebutuhan mendesak untuk meningkatkan keamanan siber di Amerika Serikat. Pada tahun 2013, Presiden Barack Obama mengeluarkan Executive Order 13636. Perintah ini mengamanatkan NIST

untuk mengembangkan sebuah kerangka kerja keamanan siber yang dapat digunakan oleh infrastruktur kritis di AS.

Respon dari NIST sangat cepat. Mereka bekerja sama dengan berbagai pihak, termasuk industri, akademisi, dan lembaga pemerintahan, untuk menciptakan sebuah kerangka kerja yang solid. Hasilnya adalah NIST CSF versi 1.0 yang dirilis pada tahun 2014. Kerangka kerja ini kemudian terus diperbarui untuk menyesuaikan dengan perkembangan ancaman siber yang semakin kompleks. Versi terbaru, NIST CSF 2.0, dirilis untuk menambahkan fungsi baru dan memperluas cakupannya.

Regulasi yang Mendorong Penggunaannya, Khususnya di Indonesia

Meskipun NIST CSF adalah kerangka kerja sukarela, banyak regulasi di berbagai negara yang mengadopsi atau merujuk pada prinsip-prinsipnya. Di Indonesia, dorongan untuk penerapan keamanan siber semakin kuat, terutama di lingkungan Badan Usaha Milik Negara (BUMN).

Salah satu regulasi penting adalah Keputusan Menteri BUMN Nomor SK-275/MBU/11/2024. Keputusan ini secara spesifik mengamanatkan penerapan 15 kontrol keamanan siber di lingkungan BUMN. Kontrol-kontrol ini mencakup berbagai aspek, mulai dari identifikasi aset, perlindungan data, hingga respons terhadap insiden. Prinsip-prinsip yang ada dalam regulasi ini sangat selaras dengan fungsi-fungsi utama di NIST CSF.

Admin Biztech

Selain itu, Peraturan BSSN No. 8 Tahun 2020 tentang Sistem Pengamanan dalam Penyelenggaraan Sistem Elektronik juga menjadi landasan hukum yang kuat. Regulasi ini menekankan pentingnya manajemen risiko dan penerapan kontrol keamanan, yang semuanya dapat diintegrasikan dengan baik melalui NIST CSF.

Struktur dan Fungsi Utama NIST CSF 2.0

NIST CSF 2.0 dirancang dengan pendekatan yang sangat terstruktur dan mudah dipahami. Kerangka kerja ini memiliki enam fungsi utama yang saling berkaitan, yaitu:

- ***Govern*** **(Mengelola)**
  Fungsi ini adalah fondasi dari seluruh kerangka kerja. Di sini, organisasi menetapkan strategi, kebijakan, dan proses untuk mengelola risiko keamanan siber. Tujuannya adalah memastikan bahwa risiko siber selaras dengan tujuan bisnis organisasi.
- ***Identify*** **(Mengidentifikasi)**
  Pada tahap ini, organisasi mengidentifikasi aset-asetnya yang paling penting, baik itu data, sistem, maupun infrastruktur. Tujuannya adalah untuk memahami risiko keamanan siber yang dihadapi. Tanpa mengetahui apa yang perlu dilindungi, akan sulit untuk melindunginya.
- ***Protect*** **(Melindungi)**
  Setelah aset-aset penting teridentifikasi, fungsi ini berfokus pada penerapan pengamanan untuk melindungi aset-aset tersebut. Ini bisa berupa kontrol akses, enkripsi data, atau pelatihan kesadaran keamanan siber bagi karyawan.
- ***Detect*** **(Mendeteksi)**
  Dunia siber penuh dengan ancaman, dan tidak semua bisa dicegah.

Fungsi deteksi bertugas untuk memonitor dan mendeteksi aktivitas yang mencurigakan atau insiden keamanan siber secepat mungkin. Semakin cepat terdeteksi, semakin cepat pula bisa diatasi.

- ***Respond* (Merespon)**
  Setelah insiden terdeteksi, fungsi respons akan mengambil alih. Ini adalah tahap di mana organisasi melakukan tindakan terkoordinasi untuk mengatasi dan mengurangi dampak dari insiden tersebut. Ini mencakup komunikasi, analisis insiden, dan mitigasi.
- ***Recover* (Memulihkan)**
  Fungsi terakhir ini berfokus pada pemulihan aset dan operasi yang terkena dampak insiden. Tujuannya adalah mengembalikan keadaan operasional seperti semula, atau bahkan lebih baik, pasca serangan siber.

Baca juga : Menerapkan Model NIST untuk Cyber Incident Response (Respons Insiden Siber): Pedoman Praktis (https://itgid.org/insight/artikel-it/menerapkan-model-nist-untuk-cyber-incident-response-respons-insiden-siber-pedoman-praktis/)

Adopsi NIST CSF di Indonesia

Melihat manfaat dan relevansinya, tidak heran jika banyak perusahaan dan lembaga di Indonesia mulai mengadopsi NIST CSF. Kerangka kerja ini dianggap efektif karena memberikan pendekatan yang terstruktur dalam membangun postur keamanan siber yang kuat. Beberapa contoh lembaga yang disebutkan telah mengadopsi NIST CSF adalah:

- Bank Indonesia
- Otoritas Jasa Keuangan (OJK)
- Pertamina
- PLN Admin Biztech
- Telkom Indonesia

- BPJS Kesehatan
- Badan Siber dan Sandi Negara (BSSN)

Adopsi ini menunjukkan kesadaran yang semakin tinggi di Indonesia akan pentingnya keamanan siber. Dengan adanya kerangka kerja seperti NIST CSF, organisasi dapat bergerak maju dengan lebih percaya diri, mengetahui bahwa mereka memiliki peta jalan yang jelas untuk melindungi aset digital mereka.

Baca juga : Ancaman Cybersecurity 2025 di Keuangan Indonesia: Solusi Canggih yang Harus Diketahui (https://infrasec.proxsisgroup.com/ancaman-cybersecurity-2025-di-keuangan-indonesia-solusi-canggih-yang-harus-diketahui/)

Rekomendasi Asesmen Keamanan Siber Gratis

Mengimplementasikan NIST CSF mungkin terdengar rumit, tetapi ada banyak sumber daya yang bisa membantu Anda memulai. Untuk Anda yang ingin mengetahui seberapa kuat postur keamanan siber perusahaan Anda saat ini, melakukan asesmen adalah langkah yang tepat. Asesmen ini akan membantu Anda mengidentifikasi celah keamanan dan area yang perlu diperbaiki.

Saat ini, banyak platform dan penyedia layanan yang menawarkan asesmen keamanan siber berbasis NIST CSF secara gratis. Anda bisa mencari di internet dengan kata kunci “free NIST CSF assessment tool” atau “tes keamanan siber gratis”. Alat-alat ini biasanya akan memberikan laporan sederhana tentang status keamanan siber Anda, yang bisa menjadi titik awal yang baik untuk perbaikan lebih lanjut.

Admin Biztech

Ingat, keamanan siber adalah sebuah perjalanan, bukan tujuan. Dengan menggunakan panduan seperti NIST CSF, Anda tidak hanya melindungi diri dari ancaman, tetapi juga membangun fondasi yang kuat untuk pertumbuhan bisnis yang berkelanjutan di era digital.

Baca juga : 15 Tren Cyber Security Tahun 2025 (https://infrasec.proxsisgroup.com/15-tren-cyber-security-tahun-2025/)

Kesimpulan

Pada akhirnya, NIST *Cybersecurity Framework* (CSF) bukanlah sekadar dokumen teknis yang rumit. Lebih dari itu, ia adalah peta jalan yang strategis untuk membangun ketahanan siber yang kuat di setiap organisasi. Dengan mengikuti enam fungsi utamanya—Govern, Identify, Protect, Detect, Respond, dan Recover—perusahaan tidak hanya akan mematuhi regulasi, tetapi juga menciptakan ekosistem digital yang lebih aman bagi pelanggan, karyawan, dan seluruh pemangku kepentingan. Adopsi NIST CSF di berbagai lembaga kunci di Indonesia adalah bukti nyata bahwa pendekatan proaktif terhadap keamanan siber kini menjadi prioritas utama.

Mari kita jadikan keamanan siber sebagai bagian tak terpisahkan dari budaya kerja kita, bukan hanya sebagai formalitas. Dengan memahami dan menerapkan kerangka kerja seperti NIST CSF, kita tidak hanya melindungi data, tetapi juga menjaga kepercayaan dan keberlanjutan bisnis di masa depan. Langkah kecil hari ini, seperti melakukan asesmen sederhana, bisa menjadi fondasi yang kokoh untuk melindungi aset digital kita dari ancaman siber yang terus berevolusi.

Admin Biztech

(https://api.whatsapp.com/send/?phone=6282199971540&text=Halo%21+Saya+tertarik+untuk+mengetahui+

FAQ (Pertanyaan yang Sering Diajukan)

1. **Apa perbedaan utama antara NIST CSF dan ISO 27001?**
   NIST CSF berfokus pada manajemen risiko keamanan siber dengan pendekatan yang fleksibel dan berbasis fungsi. Sementara itu, ISO 27001 adalah standar internasional yang berfokus pada sistem manajemen keamanan informasi (ISMS) dan sering kali digunakan untuk tujuan sertifikasi. Keduanya dapat saling melengkapi, di mana NIST CSF dapat menjadi panduan operasional dalam mengimplementasikan kontrol yang disyaratkan oleh ISO 27001.
2. **Apakah NIST CSF hanya cocok untuk perusahaan besar atau BUMN?**
   Tidak. Salah satu keunggulan NIST CSF adalah fleksibilitasnya. Kerangka kerja ini dirancang untuk dapat diterapkan oleh organisasi dari berbagai ukuran, termasuk Usaha Mikro, Kecil, dan Menengah (UMKM). Pendekatan berbasis fungsi memungkinkan organisasi untuk menyesuaikan implementasi dengan kebutuhan dan sumber daya yang dimiliki.
3. **Apakah implementasi NIST CSF di Indonesia bersifat wajib?**
   Secara umum, NIST CSF bersifat sukarela. Namun, seperti yang disebutkan dalam artikel, regulasi tertentu seperti Keputusan

Menteri BUMN SK-275/MBU/11/2024 mewajibkan perusahaan BUMN untuk menerapkan kontrol keamanan siber yang sejalan dengan prinsip-prinsip dalam kerangka kerja ini. Jadi, untuk sektor tertentu, implementasinya menjadi bagian dari kepatuhan regulasi.

4. **Bagaimana cara memulai implementasi NIST CSF di perusahaan saya?**
   Langkah pertama adalah melakukan asesmen atau penilaian postur keamanan siber saat ini. Ini akan membantu Anda mengidentifikasi celah dan area yang perlu diperbaiki. Setelah itu, Anda bisa mulai dengan fungsi “Identify” untuk memetakan aset penting, kemudian dilanjutkan dengan fungsi “Protect” untuk menerapkan kontrol dasar. Menggunakan tools asesmen gratis atau berkonsultasi dengan ahli keamanan siber juga bisa menjadi langkah awal yang baik.
5. **Mengapa BSSN juga mengadopsi NIST CSF? Bukankah mereka memiliki regulasi sendiri?**
   BSSN (Badan Siber dan Sandi Negara) adalah lembaga pemerintah yang bertanggung jawab atas keamanan siber nasional. Adopsi NIST CSF oleh BSSN menunjukkan pengakuan terhadap efektivitas kerangka kerja ini sebagai best practice global. BSSN menggunakan prinsip-prinsip NIST CSF untuk memperkuat kebijakan dan standarnya sendiri, sehingga tercipta sinergi antara standar nasional dan internasional dalam menjaga ruang siber Indonesia.

Leave a Reply

Your email address will not be published. Required fields are marked *

Admin Biztech

Comment *

Name *

Email *

Website

Save my name, email, and website in this browser for the next time I comment.

Post Comment

Admin Biztech

Admin Biztech

Admin Biztech

Admin Biztech

Admin Biztech

Admin Biztech

Admin Biztech