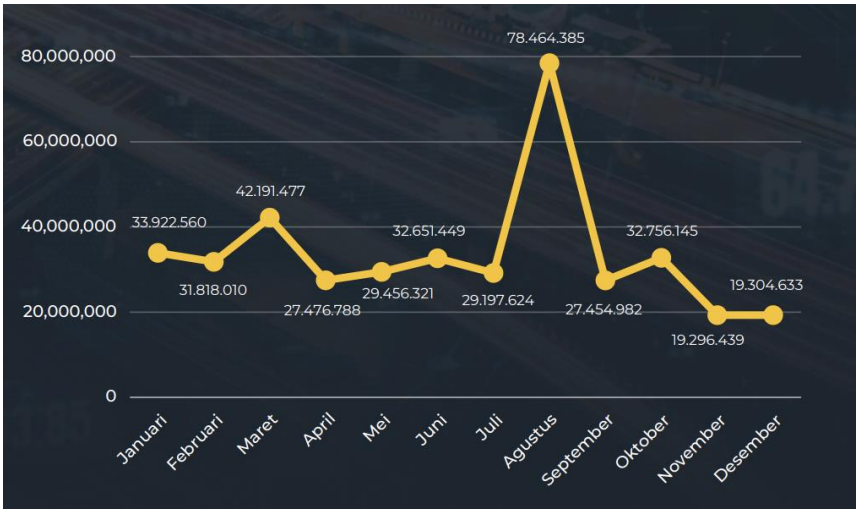
BAB I PENDAHULUAN

I.1 Latar Belakang

Seiring dengan kemajuan teknologi yang semakin meluas, keamanan siber telah menjadi aspek yang sangat penting bagi kelangsungan organisasi di seluruh dunia, khususnya Indonesia. Peningkatan ketergantungan pada teknologi informasi dan komunikasi membuka peluang bagi ancaman siber yang semakin kompleks. Menurut data dari Badan Siber dan Sandi Negara (BSSN) yang dikutip dari berita kompas.com tahun 2023, Indonesia menghadapi sekitar lebih dari 403 juta serangan siber, dengan mayoritas berupa *generic trojan* RAT (Badan Siber dan Sandi Negara Republik Indonesia, 2023).



Gambar I.1 Trafik Anomali Serangan Siber Di Indonesia (Badan Siber dan Sandi Negara Republik Indonesia, 2023)

Ancaman ini tersebut menargetkan sektor publik dan swasta. Menurut berita yang dikutip dari reuters.com, pada Juni 2024, serangan *ransomware* yang menargetkan Pusat Data Nasional Indonesia mengakibatkan adanya gangguan terhadap layanan pemerintah, termasuk imigrasi dan operasi bandara utama. Insiden ini menyoroti kerentanan keamanan siber nasional dan pentingnya penerapan strategi yang efektif.

Meskipun telah dilakukan upaya dalam meningkatkan keamanan siber, peringkat Indonesia dalam *Global Cybersecurity Index* (GCI) menunjukkan bahwa

keamanan siber Indonesia masih memerlukan perbaikan. Berdasarkan data GCI tahun 2024, Indonesia menempati peringkat ke-24 dari 194 dan masuk ke dalam kategori *Tier* 1-*Role-modelling* dengan skor 95 sampai 100 (Sector, 2024). Meskipun peringkat tersebut menunjukkan peningkatan dibandingkan tahun-tahun sebelumnya, posisi Indonesia di *Global Cybersecurity Index* (GCI) juga mengindikasikan masih adanya tantangan yang perlu diatasi untuk mencapai tingkat keamanan siber yang lebih optimal. Salah satu tantangan utama adalah ketidakseimbangan antara regulasi yang sudah diterapkan dengan pelaksanaannya di lapangan, terutama di sektor-sektor yang belum memiliki prioritas tinggi terhadap keamanan siber.

Selain itu, meskipun Indonesia telah masuk ke dalam kategori *Tier 1-Role-modelling*, masih terdapat kesenjangan dalam implementasi *framework* keamanan siber secara konsisten di seluruh sektor industri, baik sektor publik maupun swasta. Faktor lain yang menjadi perhatian adalah kebutuhan untuk meningkatkan kolaborasi internasional dan investasi dalam teknologi keamanan, mengingat ancaman siber tidak hanya bersifat lokal tetapi juga global.

Sehubungan dengan kondisi tersebut, penilaian dan manajemen terhadap kesiapan siber yang terintegrasi merupakan hal yang sangat krusial bagi kebutuhan organisasi saat ini. Penilaian tersebut akan memungkinkan identifikasi ancaman secara proaktif dan akurat sehingga dapat melakukan implementasi langkah mitigasi yang sesuai dan efektif. Dengan demikian, organisasi dapat membangun keamanan siber yang kuat dan responsif untuk menghadapi ancaman keamanan siber yang akan terus berkembang.

I.2 Perumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan di atas, rumusan masalah dari penelitian ini adalah:

1. Apa parameter yang digunakan untuk melakukan penilaian tingkat kematangan keamanan siber (*maturity assessment*) berdasarkan *framework* keamanan siber yang tersedia secara global?
2. Bagaimana tingkat relevansi dan tingkat kepentingan untuk setiap parameter yang telah diidentifikasi?

I.3 Tujuan Penelitian

Berdasarkan rumusan masalah di atas, penelitian ini bertujuan untuk:

1. Melakukan identifikasi terhadap parameter-parameter yang penting dengan menentukan parameter-parameter kunci yang akan digunakan dalam evaluasi berdasarkan *framework-framework* yang tersedia secara global.
2. Mengevaluasi parameter dalam *framework* dengan menggunakan metode pengambilan keputusan *multicriteria decision makin*g *Best-Worst Method* (BWM) untuk menentukan nilai dan kepentingan parameter yang ada.

I.4 Batasan Penelitian

Batasan penelitian ini yaitu:

1. Penelitian ini hanya berfokus pada *framework* keamanan siber global yang digunakan untuk mengukur tingkat kematangan organisasi.
2. Penelitian ini membatasi pada parameter yang dianggap paling relevan dan memberikan kontribusi signifikan terhadap kebutuhan dan tujuan keamanan siber organisasi.
3. Penelitian ini berfokus pada validasi aspek dan parameter yang digunakan dalam *framework*, tanpa melanjutkan ke tahap implementasi langsung atau studi kasus.
4. Penelitian ini juga tidak mempertimbangkan perbedaan tingkat kematangan keamanan siber berdasarkan ukuran atau wilayah geografis organisasi, melainkan melihatnya secara keseluruhan.

I.5 Manfaat Penelitian

Manfaat dari penelitian ini yaitu:

1. Bagi organisasi, penelitian ini sebagai dasar dalam melakukan penilaian dalam keamanan siber sehingga dapat mendukung pengambilan keputusan strategis terkait dengan tata kelola dan manajemen risiko siber, sehingga perusahaan dapat mencapai tujuan dan strateginya dengan lebih efektif.
2. Bagi peneliti, penelitian ini bertujuan untuk mendapatkan pemahaman yang mendalam tentang keamanan siber, serta pengaruhnya terhadap keberhasilan sebuah perusahaan, khususnya pada organisasi dan dapat digunakan sebagai referensi dalam penelitian berikutnya.