EKONOMI, BISNIS MANAJEMEN DAN KEUANGAN (EBMK)
Vol. 1, No, 1, 2026

OPEN ACCESS ISSN : XXXX-XXXX

TINJAUAN LITERATUR STRATEGI ADAPTASI DAN TANTANGAN KEAMANAN SIBER

Dedi Saputra*[1], Devi Satriawan[2] and Fikri Ardiansyah[3]

[1, 2, 3] Universitas Satyagama, Jakarta, Indonesia.

Email: *dedisaputrastsh233@gmail.com, devisatriawan36@gmail.com, Fikri Ardiansyah123@gmail.com

ARTICLE INFO

Article History
Received: March 08th, 2026
Accepted: March 09th, 2026
Published: March 09th, 2026

Kata Kunci:
Keamanan Siber,
Strategi Adaptasi,
Tantangan Digital,
Zero Trust,
Ketahanan Organisasi.

ABSTRAK

Transformasi digital yang cepat telah mengamplifikasi permukaan serang siber, mengakibatkan perlunya organisasi untuk mengembangkan strategi adaptasi yang efektif. Artikel ini dimaksudkan untuk melihat literatur terkini untuk mengidentifikasi tantangan keamanan siber utama dan efektivitas berbagai strategi adaptasi. Melalui literatur akademis berbagai sumber, penulis mampu mengidentifikasi bahwa ransomware, phishing berbasis AI, dan kerentanan infrastruktur kritis adalah beberapa masalah yang paling menguatkan. Variasi strategi adaptasi yang paling efektif adalah penggunaan kombinasi dari teknologi konservasi berlapis, kerangka kerja Zero Trust, dan budaya kesadaran siber pada sumber daya manusia. Secara keseluruhan, artikel ini menyimpulkan bahwa adaptasi proaktif dan responsif jauh lebih efektif daripada taktik reaktif tradisional.

I. PENDAHULUAN

Di era konektivitas global modern, keamanan siber telah mengalami pergeseran paradigma. Satu-satunya hal yang umum dari perlindungan informasi ialah bagaimana digunakannya untuk menghasilkan jaminan dan kesehatan kerja karyawannya. Perlindungan informasi perusahaan sekarang tanpa dukungan dari di mana saja, mengancam perintah perjudian di tingkat nasional. Perlindungan informasi telah berkembang dari isu teknis yang perlu ditangani oleh departemen sangat Teknologi Informasi hanya menjadi satu dari pilar-pilar penting bagi kelangsungan hidup organisasi dan kedaulatan data nasional (Restika & Sonita, 2023).

Transformasi digital telah secara efektif memaksa semua entitas bisnis dan pemerintahan tersebut. untuk menggunakan peralatan yang mutakhir Namun, meskipun disiplin ini berpotensi membawa efisiensi operasional muncul, pemanfaatannya jelas menjadi potensi sumber kecelakaan yang kompleks (Pratama & Nugraha, 2026). Saat ini, penjahat siber bukan lagi operasi tangan; sebaliknya, mereka telah menjadi sindikat terorganisir dengan dukungan aplikasi yang otomatis. Penggunaan AI dalam pengembangan serangan phasing fiksi atau polimorfik benar-benar membuktikan bahwa ancaman telah berkembang (Khasanah, Azzahra & Aji, 2026).

Sehingga, pemahaman lanskap tantangan siber bukanlah pilihannya. Kurang pengetahuan menghalangi organisasi untuk menjadi relawan kuda yang jatuh ke dalam pertahanan dengan pola reaktif yang secara konsisten tertinggal dari para penyerang. Selanjutnya, kerugian internal terhadap sistem informasi dapat memprovokasi total penurunan peningkatan layanan umum dan infrastruktur dan peraturan (Marlina, 2025). Kerugian tidak hanya terbatas pada nilai akuntansi dari ransomware, tetapi juga termasuk reputasi dan hiyas dunia maya. tanpa pengenalan strategi adaptasi latar belakang ini akan terus terjadi permintaan yang membayangi keinginan bagi metode kehidupan manusia untuk menjalankan kehidupan manusia.

III. METODE PENELITIAN

Penelitian ini menggunakan metode sistematis literatur kajian (SLR). Langkah pertama adalah defiinisasi secara ketat gaya prosedur pencarian untuk menavigasikan data informasi dalam web. Data Informasi dikumpulkan melalui database sumber luaran akademik mencolok seperti Google Scholar, dan Sinta. Jam dan rentang waktu publikasi terbatas pada lima tahun terakhir, 2021–2026, untuk menjaga relevansi terhadap dinamika ancaman siber. Fokus kriteria inklusi pada makalah yang membahas ancaman baru, yaitu

Advanced Persistent Threats, eksploitasi AI, dan trick model adaptasi organisasi NIST, 2023, dan proses analisis melibatkan ekstraksi data dan sintesis untuk membandingkan kerangka kerja siber seluruh dunia yang berbeda. Peneliti tahu bahwa tantangan dari pola mereka muncul di sektor industri yang berbeda,. Maka dari itu, penulis tertarik dengan kecenderungan umum.

IV. HASIL DAN PEMBAHASAN

Diskusi Saat ini, tantangan keamanan siber "persenjataan AI" oleh aktor ancaman (Restika & Sonita, 2023). Serangan tersebut disamarkan tanpa manusia memperlambat proses tersebut. Masalah terbesar adalah saat malware menggunakan AI untuk mempelajari situasi pada targetnya sendiri dan menghasilkan cara untuk menghindari deteksi berdasarkan deteksi berbasis perilakunya. Biasanya, ini tidak cukuk karena, jika pemrograman, maka melakukannya dengan cara berbasis tanda tangan shell-up berbasis tanda tangan, tetapi hal itu menolak beberapa detektor perangkat lunak. Social Engineering, seperti biasa, menjadi kata kuncinya. Faktor manusia adalah "pintu de'erre" yang paling tidak terhindarkan akan ditemui dari timpal semuanya (Pratama & Nugraha, 2026). Foto ini digrafis untuk melibatkan staf eksentrik untuk memastikan transaksinya. Proses masukle pie, sehubungan dengan kerumahan, telah membuat konsep-konsep sepele tergadaskan, meskipun perimeter jaringan dan jaringan luar "pelindung" telah lama menjadi buruk (Khasanah, Azzahra & Aji, 2026). Jawaban biasal yang sama adalah Zero Trust Architecture ZTA. Prinsip perilaku tersebut adalah tidak pernah percaya, selalu memverifikasi, beberapa menborztak semua seperti jikaengaruhi setian permintaan untuk mengandalkan koyaasan peminta dan mengungkapkan aksesnya "mask-out" bebeas (Khasanah, Azzahra & Aji, 2026). Biasal melibatkan sistem yang matang Identity and Access Management IAM.

Strategi adaptasi modern telah beralih ke Ketahanan Siber. Secara khusus, literatur meminta organisasi untuk berasumsi bahwa mereka akan berhasil ditembus. Akibatnya, investasi dapat dialihkan dari upaya untuk mencegah setiap penetrasi ke kemampuan deteksi dengan sangat cepat dan pemulihan melalui SOC yang diperkuat dengan SOAR untuk merespons ancaman dalam hitungan milidetik.

V. KESIMPULAN

Tantangan keamanan siber adalah fenomena yang terus berubah mengikuti perkembangan teknologi informasi. Sebagian besar sistem tidak bisa benar-benar kebal terhadap serangan. Namun, strategi adaptasi komprehensif telah terbukti mampu mengurangi dampak secara signifikan. Keamanan siber yang efektif membutuhkan gabungan teknologi tinggi, proses teruji, dan manusia terlatih. Sebagian besar organisasi besar memerlukan strategi Zero Trust dan memperkuat Ketahanan Siber untuk menghadapi ancaman siber modern. Dari analisis di atas, rekomendasi berikut dapat dikerjakan oleh organisasi. Pertama, investasikan lebih banyak anggaran pada Cyber Security Awareness untuk semua karyawan karena penelitian menunjukkan bahwa manusia adalah faktor risiko yang paling rentan. Kedua, perbaikan kolaborasi antara pemerintah dan perusahaan dalam bidang dianatar ancaman intelijen. Penelitian selanjutnya dapat dilakukan untuk mempelajari pengaruh keamanan dari AI generatif dan penyusunan protokol "post-quantum" untuk menangani potensi komputasi komputasi.

VI. AUTHOR'S CONTRIBUTION

Conceptualization: Dedi Saputra, Devi Satriawan and Fikri Ardiansyah
Methodology: Dedi Saputra, Devi Satriawan and Fikri Ardiansyah
Investigation: Dedi Saputra, Devi Satriawan and Fikri Ardiansyah
Discussion of results: Dedi Saputra, Devi Satriawan and Fikri Ardiansyah
Writing – Original Draft: Dedi Saputra, Devi Satriawan and Fikri Ardiansyah
Writing – Review and Editing: Dedi Saputra, Devi Satriawan and Fikri Ardiansyah
Approval of the final text: Dedi Saputra, Devi Satriawan and Fikri Ardiansyah

VIII. REFERENCES

Restika, R., & Sonita, E. (2023). Tantangan keamanan siber dalam manajemen likuiditas bank syariah: Menjaga stabilitas keuangan di era digital. *Krigan: Journal of Management and Sharia Business*, *1*(2), 25-36.

Pratama, N. A., & Nugraha, M. R. (2026). Strategi Pertahanan Keamanan Siber Berbiaya Rendah untuk UMKM: Tinjauan Literatur. *Jurnal Ilmu Komputer dan Informatika| E-ISSN: 3063-9026*, *2*(3), 67-72.

Khasanah, U., Azzahra, N. S., & Aji, G. (2026). Tantangan Keamanan Siber dalam Penerapan Sistem Akuntansi Digital: Tinjauan Literatur Sistematik. *RIGGS: Journal of Artificial Intelligence and Digital Business*, *4*(4), 8585-8596.

Marlina, S. (2025). Keamanan Siber pada Aplikasi Cloud Computing: Analisis Ancaman dan Strategi Mitigasi. *Jurnal Komputer Dan Teknologi Informasi*, *1*(1), 29-35.

Kristianti, N., & Kurniasi, R. (2024). Peraturan dan Regulasi Keamanan Siber di Era Digital. *Satya Dharma: Jurnal Ilmu Hukum*, *7*(1), 297-310.