JIIC: JURNAL INTELEK INSAN CENDIKIA
https://jicnusantara.com/index.php/jiic
Vol : 3 No: 8, Agustus 2026
E-ISSN : 3047-7824

Evaluasi Pemahaman dan Implementasi Strategi *Defense-in-Depth* pada Keamanan Jaringan di Era Ancaman Siber Modern

Evaluation of the Understanding and Implementation of Defense-in-Depth Strategies for Network Security in the Era of Modern Cyber Threats

Naufal Fadhiil Nasurullah
Universitas Sebelas April
Email: 1220660121174@student.unsap.ac.id

Article Info

Article history:
Received : 08-08-2026
Revised : 10-08-2026
Accepted : 12-08-2026
Pulished : 14-08-2026

Abstract

Cyber threats that are increasingly complex and structured, such as ransomware attacks and Advanced Persistent Threats (APT), require organizations to implement defense strategies that do not rely solely on technology, but also encompass human and policy aspects. Defense-in-Depth (DiD) is a layered approach that integrates various technical and administrative controls to create a resilient and adaptive security system. This study aims to evaluate the understanding and implementation of the DiD strategy in organizational environments using a quantitative survey approach. The research instrument was developed based on the NIST SP 800-53, ISO/IEC 27001:2022, COBIT 2019, and the KAMI Index frameworks. The data were analyzed using Structural Equation Modeling based on Partial Least Squares (PLS-SEM) with the SmartPLS application. The results show that security awareness and an understanding of threat phenomena have a significant influence on the effectiveness of DiD implementation. These findings highlight the importance of continuous training, incident simulations, and the updating of technical policies as part of a comprehensive network security strategy.

Keywords: Defense-in-Depth, Network Security, Cybersecurity Awareness

Abstrak

Ancaman siber yang semakin kompleks dan terstruktur, seperti serangan ransomware dan Advanced Persistent Threats (APT), menuntut organisasi untuk menerapkan strategi pertahanan yang tidak hanya mengandalkan teknologi semata, melainkan juga mencakup aspek manusia dan kebijakan. Defense-in-Depth (DiD) merupakan pendekatan berlapis yang mengintegrasikan berbagai kontrol teknis dan administratif untuk menciptakan sistem keamanan yang tangguh dan adaptif. Penelitian ini bertujuan untuk mengevaluasi pemahaman dan implementasi strategi DiD dalam lingkungan organisasi, menggunakan pendekatan kuantitatif dengan metode survei. Instrumen penelitian dikembangkan berdasarkan kerangka kerja NIST SP 800-53, ISO/IEC 27001:2022, COBIT 2019, dan Indeks KAMI. Data dianalisis menggunakan teknik Structural Equation Modeling berbasis Partial Least Squares (PLS-SEM) melalui aplikasi SmartPLS. Hasil penelitian menunjukkan bahwa kesadaran keamanan (awareness) dan pemahaman terhadap fenomena ancaman memiliki pengaruh signifikan terhadap efektivitas implementasi DiD. Temuan ini menggarisbawahi pentingnya pelatihan berkelanjutan, simulasi insiden, serta pembaruan kebijakan teknis sebagai bagian dari strategi keamanan jaringan yang komprehensif.

Kata kunci: Defense-in-Depth, Keamanan Jaringan, Kesadaran Keamanan

PENDAHULUAN

Dalam beberapa tahun terakhir, lanskap keamanan siber telah mengalami transformasi signifikan akibat meningkatnya intensitas, kompleksitas, dan kecanggihan serangan digital seperti

ransomware, phishing, Distributed Denial of Service (DDoS), dan Advanced Persistent Threats (APT). Fenomena ini menimbulkan tantangan serius bagi organisasi di berbagai sektor, terutama yang bergantung pada sistem jaringan dan infrastruktur informasi digital (Ali et al., 2021). Serangan tidak lagi bersifat acak, melainkan terstruktur dan seringkali menyasar celah keamanan manusia dan sistem yang paling rentan. Menghadapi kondisi tersebut, pendekatan keamanan konvensional yang hanya bergantung pada satu atau dua lapisan proteksi terbukti tidak lagi memadai. Oleh karena itu, pendekatan Defense-in-Depth (DiD) menjadi solusi strategis yang semakin banyak diadopsi oleh organisasi. DiD merupakan konsep yang menekankan perlindungan berlapis, menggabungkan berbagai kontrol teknis, administratif, serta edukasi pengguna untuk menciptakan sistem pertahanan berkelanjutan dan terintegrasi (Bishop, 2005).

Strategi ini tidak hanya melibatkan penggunaan firewall dan antivirus, namun juga mencakup kesadaran pengguna, manajemen insiden, dan penerapan kebijakan keamanan yang konsisten (Anderson, 2020). Penerapan strategi DiD perlu dievaluasi secara berkala untuk mengetahui sejauh mana pemahaman personel dan efektivitas implementasi di lapangan. Faktor-faktor seperti kesadaran karyawan terhadap kebijakan keamanan, kemampuan mendeteksi insiden, hingga penerapan kontrol teknis seperti otentikasi multifaktor dan manajemen patching menjadi elemen penting dalam mengukur kesiapan organisasi menghadapi ancaman (White et al., 2017; NIST, 2020). Dalam konteks Indonesia, instrumen seperti Indeks KAMI dari BSSN serta standar internasional seperti ISO/IEC 27001 dan NIST SP 800-53 menjadi acuan dalam membangun dan mengevaluasi sistem keamanan informasi (ISO/IEC, 2022; BSSN, 2022). Penelitian lain oleh Yusuf et al. (2021) menunjukkan bahwa integrasi kebijakan keamanan dengan pelatihan kesadaran dapat meningkatkan kepatuhan pengguna terhadap prosedur keamanan.

METODE PENELITIAN

Berdasarkan tujuan penelitian untuk mengevaluasi pemahaman dan implementasi Defense-in-Depth (DiD) serta menguji pengaruh faktor-faktor yang terkait, penelitian ini menggunakan pendekatan kuantitatif melalui survei agar kondisi dapat diukur secara objektif. Instrumen disusun mengacu pada NIST SP 800-53, ISO/IEC 27001:2022, COBIT 2019, dan Indeks KAMI, kemudian data dianalisis dengan SmartPLS menggunakan PLS-SEM untuk menilai validitas–reliabilitas serta menguji hubungan antar variabel penelitian (Hair et al., 2017; Creswell, 2018).

Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan pendekatan kuantitatif deskriptif dengan metode survei untuk mengevaluasi pemahaman dan implementasi strategi Defense-in-Depth pada organisasi. Pendekatan ini dipilih karena mampu mengukur secara objektif hubungan antar variabel laten seperti awareness, fenomena ancaman, dan praktik keamanan yang diterapkan (Ali et al., 2021).

Populasi dan Sampel

Populasi dalam penelitian ini adalah pegawai dari sektor pemerintahan dan pendidikan yang memiliki tanggung jawab terhadap keamanan sistem informasi dan jaringan. Teknik purposive sampling digunakan untuk memilih responden yang relevan dengan topik penelitian, yaitu mereka yang terlibat langsung dalam pengelolaan infrastruktur TI. Jumlah responden yang dikumpulkan adalah sebanyak 100 orang, dengan proporsi seimbang antara jabatan teknis dan non-teknis.

Instrumen Penelitian

Instrumen utama dalam penelitian ini adalah kuesioner berbasis Likert skala 5 poin, yang disusun berdasarkan referensi dari kerangka kerja keamanan informasi seperti NIST SP 800-53, ISO/IEC 27001:2022, COBIT 2019, dan Indeks KAMI (ISACA, 2019; BSSN, 2022). Kuesioner dibagi ke dalam tiga dimensi utama:

1. Awareness (AWR): mengukur tingkat pemahaman dan kesadaran responden terhadap kebijakan dan prosedur keamanan.
2. Fenomena (FEN): mengevaluasi pengetahuan responden tentang tren dan jenis ancaman siber terkini.
3. Security (SEC): menilai implementasi kontrol teknis dan administratif dalam lingkungan kerja responden.

Setiap dimensi terdiri atas 6–7 indikator yang telah divalidasi melalui uji coba awal (pilot test) kepada 10 responden.

Teknik Analisis Data

Data yang terkumpul dianalisis menggunakan perangkat lunak SmartPLS 4.0, dengan pendekatan Partial Least Squares Structural Equation Modeling (PLS-SEM). Tahapan analisis meliputi:

1. Evaluasi Outer Model: untuk menguji validitas konstruk (convergent & discriminant validity) dan reliabilitas (Cronbach's Alpha, Composite Reliability).
2. Evaluasi Inner Model: untuk menguji hubungan antar variabel laten melalui nilai koefisien determinasi (R^2), nilai path coefficient, dan nilai signifikansi (p-value).

Pendekatan ini digunakan karena PLS-SEM mampu menangani model dengan kompleksitas tinggi, sampel kecil, dan tidak mensyaratkan data berdistribusi normal (Anderson, 2020; Hair et al., 2017).

HASIL DAN PEMBAHASAN

Setelah proses pengumpulan data kuesioner dan pengolahan menggunakan SmartPLS dengan pendekatan PLS-SEM selesai dilakukan, tahap selanjutnya adalah menyajikan temuan penelitian secara sistematis. Bagian hasil dan pembahasan ini memaparkan karakteristik responden serta hasil evaluasi model pengukuran (validitas dan reliabilitas) dan model struktural (hubungan/pengaruh antar variabel), kemudian diinterpretasikan untuk menjelaskan kondisi pemahaman dan implementasi Defense-in-Depth (DiD) serta implikasinya pada lingkungan organisasi.

Deskripsi Responden

Responden dalam penelitian ini terdiri dari 100 orang yang berasal dari sektor pemerintahan dan pendidikan. Mayoritas responden berusia 25–45 tahun (60%), dengan latar belakang pendidikan pascasarjana (55%) dan sarjana (20%), serta sebanyak 70% bekerja di bidang teknologi informasi (35% staf teknis dan 15% manajemen IT, ditambah staf non-IT dan peran lainnya). Hal ini menunjukkan bahwa responden memiliki latar belakang yang relevan untuk memberikan gambaran

terhadap kondisi penerapan strategi Defense-in-Depth.

Kategori Karakteristik	Sub-Kategori	Persentase (%)
Lama Bekerja	< 1 Tahun	35%
Lama Bekerja	1 - 5 Tahun	40%
Lama Bekerja	6 - 10 Tahun	20%
Lama Bekerja	> 10 Tahun	5%
Jenis Kelamin	Pria	65%
Jenis Kelamin	Wanita	35%
Usia	Di bawah 25 tahun	25%
Usia	25 - 35 tahun	20%
Usia	36 - 45 tahun	35%
Usia	Di atas 45 tahun	20%
Pendidikan Terakhir	SMA / SMK	20%
Pendidikan Terakhir	Diploma	5%
Pendidikan Terakhir	Sarjana (S1)	20%
Pendidikan Terakhir	Pascasarjana (S2/S3)	55%
Jabatan / Peran	Staff IT / Teknis	35%
Jabatan / Peran	Manajemen IT	15%
Jabatan / Peran	Staff Non-IT	25%
Jabatan / Peran	Lainnya	25%

Analisis Deskriptif Tiap Dimensi

Awareness: Sebanyak 80% responden mengaku pernah mengikuti pelatihan keamanan informasi, namun hanya 55% yang mengetahui prosedur pelaporan insiden di institusinya. Hal ini menunjukkan bahwa meskipun pelatihan tersedia, masih terdapat kesenjangan dalam pemahaman prosedural.

Fenomena Ancaman: Hanya 38% responden yang memahami tren ancaman siber terbaru seperti ransomware, phishing, atau DDoS. Lebih rendah lagi, hanya 30% yang pernah mengikuti simulasi insiden. Ini menunjukkan kurangnya eksposur terhadap real-case training dan pembaruan informasi keamanan.

Security Implementation: Dari sisi teknis, 64% organisasi telah menerapkan multi-factor authentication (MFA) dan 60% melakukan backup data secara berkala. Namun, hanya 46% yang melakukan patching secara terjadwal. Temuan ini menunjukkan bahwa aspek teknis belum sepenuhnya terintegrasi dalam kebijakan keamanan yang konsisten.

Hasil Analisis SmartPLS

Uji validitas konvergen menunjukkan bahwa semua item memiliki outer loading > 0.71, yang menandakan kontribusi indikator terhadap konstruk utama cukup kuat. Nilai Cronbach's Alpha dan Composite Reliability dari semua variabel berada di atas nilai ambang batas 0.70, yang menunjukkan tingkat reliabilitas tinggi pada instrumen pengukuran.

Pembahasan Komprehensif

Temuan penelitian ini memperkuat hasil studi sebelumnya yang menegaskan bahwa kesadaran pengguna (security awareness) merupakan faktor kunci dan benteng pertahanan utama dalam keberhasilan strategi pertahanan siber berlapis (Ali et al., 2021; Bailey et al., 2020). Pelatihan yang berkelanjutan dan kebijakan internal yang jelas terbukti mampu meningkatkan kesiapan individu dalam mengenali ancaman serta merespons insiden keamanan dengan tepat. Ketika personil memiliki pemahaman yang matang mengenai vektor serangan seperti spear-phishing dan social engineering, risiko masuknya vektor serangan awal dapat ditekan secara signifikan.

Namun demikian, rendahnya pemahaman terhadap fenomena ancaman siber modern (hanya 38% yang memahami tren ancaman terkini dan 30% yang pernah mengikuti simulasi) menunjukkan adanya keretakan fatal antara kebijakan formal organisasi dan kesiapan taktis pengguna di lapangan (Arifin & Nugroho, 2022; Hartono et al., 2022). Kurangnya simulasi insiden dan pembaruan edukasi keamanan secara berkala menyebabkan organisasi kurang siap secara psikologis dan teknis menghadapi dinamika serangan modern yang sangat adaptif. Kondisi ini diperparah oleh ditemukannya kelemahan pada eksekusi kontrol teknis dasar, di mana pembaruan sistem dan patch management terjadwal baru diterapkan oleh 46% organisasi. Celah patching ini memberi ruang bagi eksploitasi kerentanan yang telah diketahui (known vulnerabilities) oleh pihak luar.

Secara komprehensif, hasil analisis model struktural (Inner Model) dengan SmartPLS mengungkapkan bahwa variabel Awareness (AWR) dan Fenomena Ancaman (FEN) secara simultan berpengaruh signifikan dan mampu menjelaskan sebesar 67,2% variasi keberhasilan implementasi Defense-in-Depth (SEC). Hal ini membuktikan secara empiris bahwa efektivitas pertahanan berlapis tidak bisa dipandang hanya sebagai proyek pengadaan alat teknis (seperti firewall dan antivirus), melainkan sebuah ekosistem sinergis yang mengintegrasikan aspek teknis, manusia, dan kebijakan operasional secara berimbang (Mahendra et al., 2024; Yusuf et al., 2021). Tanpa adanya intervensi berupa simulasi insiden berkala, penguatan prosedur pelaporan, serta otomatisasi manajemen patch, implementasi Defense-in-Depth di organisasi akan tetap rentan mengalami kegagalan pada titik terlemahnya.

KESIMPULAN

Penelitian ini bertujuan untuk mengevaluasi pemahaman dan implementasi strategi Defense-in-Depth dalam konteks keamanan jaringan di era ancaman siber yang semakin kompleks. Berdasarkan hasil analisis kuantitatif terhadap 100 responden dari sektor pemerintahan dan pendidikan, dapat disimpulkan bahwa implementasi kontrol teknis seperti multi-factor

authentication (MFA) dan backup data sudah berjalan cukup baik. Namun demikian, penerapan patching terjadwal dan manajemen risiko masih belum optimal, sehingga berpotensi menciptakan celah keamanan yang kritis.

Hasil analisis model struktural dengan SmartPLS menunjukkan bahwa variabel awareness dan fenomena ancaman secara simultan mampu menjelaskan 67.2% variasi dari keberhasilan implementasi strategi Defense-in-Depth, di mana masing-masing memiliki pengaruh yang signifikan secara statistik. Hal ini menegaskan bahwa faktor manusia dan pemahaman kontekstual ancaman memegang peranan pivotal dalam keberhasilan strategi pertahanan jaringan berlapis.

SARAN

Berdasarkan hasil penelitian, saran yang dapat diberikan adalah organisasi perlu memperkuat implementasi Defense-in-Depth secara lebih konsisten dengan menutup kesenjangan antara pelatihan dan pemahaman prosedural, khususnya pada aspek pelaporan insiden dan pembaruan pengetahuan ancaman. Program security awareness sebaiknya dilakukan secara berkelanjutan disertai simulasi insiden berkala agar pengguna lebih siap menghadapi dinamika serangan modern, serta memastikan kontrol teknis seperti patch management dijalankan secara terjadwal dan terintegrasi dengan kebijakan keamanan. Selain itu, penelitian berikutnya disarankan untuk memperluas cakupan responden dan menyempurnakan indikator pada konstruk Fenomena dan Security agar validitas model semakin kuat dan tingkat generalisasi hasil penelitian menjadi lebih luas.

DAFTAR PUSTAKA

Ali, S., et al. (2021). Cyber security threats and defense mechanisms in digital infrastructure. *Journal of Information Security*, 12(2), 75–90.

Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Wiley.

Arifin, L. R., & Nugroho, F. A. (2022). Simulasi insiden siber untuk meningkatkan kesiapan respon keamanan informasi. *Jurnal Sistem Informasi*, 18(1), 44–52.

Badan Siber dan Sandi Negara. (2022). *Indeks KAMI 2022: Indeks keamanan informasi*. https://bssn.go.id

Bailey, D., Clark, J., & Miller, S. (2020). *Layered security: Why defense in depth is critical* (SANS Institute White Paper).

Bishop, M. (2005). *Introduction to computer security*. Addison-Wesley.

Creswell, J. W., & Creswell, J. D. (2018). *Research design: Qualitative, quantitative, and mixed methods approaches* (5th ed.). SAGE Publications.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling (PLS-SEM)* (2nd ed.). SAGE Publications.

Hartono, D., Wibowo, B., & Prasetyo, A. (2022). Effectiveness of cybersecurity simulations in organizational settings. *Jurnal Keamanan Siber Indonesia*, 4(3), 95–105.

ISACA. (2019). *COBIT 2019 framework: Governance and management objectives*. ISACA.

ISO/IEC. (2022). *Information security management systems – Requirements* (ISO/IEC Standard No. 27001:2022). International Organization for Standardization.

Mahendra, A., Ramadhan, P., & Setiawan, I. (2024). Audit keamanan informasi berbasis ISO/IEC 27001 di instansi pemerintah. *Jurnal Rekayasa dan Sistem Informasi*, 11(1), 15–24.

National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations* (NIST Special Publication 800-53, Rev. 5). U.S. Department of Commerce.

White, G., Fisch, E., & Pooch, U. (2017). *Computer system and network security*. CRC Press.

Yusuf, M., Darmawan, S., & Hidayat, R. (2021). Security awareness and behavior of employees in public institutions. *Cyberpsychology Journal*, 5(4), 122–130.