JURNAL TECHNOLOGIE

E-ISSN : XXXX | P-ISSN : XXXX
Volume 1, Number 1, 2026, pp. 1-7

OPTIMALISASI KEAMANAN JARINGAN INFRASTRUKTUR TI DALAM MENDUKUNG TRANSFORMASI DIGITAL LAYANAN PUBLIK DI DPM-PTSP BANYUASIN

Berlia Nisyah[1], Ahmad Jibrael Algandi[2], ,Muhammad Rivan[3] ,Muhammad Adim Dwi[4]

Universitas Islam Negeri Raden Fatah Palembang
berlianisyah7@gmail.com[1] jibrael106@gmail.com[2] sultanrivan0@gmail.com[3] adim885@gmail.com[4]

ARTICLE INFO

Article History
Received : January 2026
Revised : January 2026
Accepted : January 2026

Keywords
Network Security
IT Infracstructure
Digital Transformation
Public Servive

ABSTRACT

Digital transformation is a strategic step in improving the quality of public services, including at the Banyuasin Regency Investment and One-Stop Integrated Services Service (DPMPTSP). This research aims to identify the condition of the information technology (IT) infrastructure, evaluate the security challenges and risks faced, and analyze the implementation of security systems on the DPMPTSP IT infrastructure in supporting digital services. The research method used was qualitative with data collection techniques through interviews and direct observation at the DPMPTSP Banyuasin Office. Using qualitative descriptive methods and literature studies, this research identifies the main threats as well as technical and policy solutions that can be implemented. The research results show that the existing IT infrastructure has enabled licensing services to run online, faster and more transparently. However, there are still challenges such as internet network disruptions, hardware limitations, and a lack of IT experts. DPMPTSP has implemented security measures such as routine data backup, use of antivirus, double authentication, and refers to national and international security standards. Optimizing IT infrastructure security has proven to be a key factor in supporting sustainable digital transformation, maintaining data integrity, and increasing public trust in digital public services in the Banyuasin Regency DPMPTSP.

Pendahuluan

Di era digital yang semakin maju, teknologi informasi (TI) telah menjadi dasar bagi berbagai operasi di sektor publik maupun swasta. Hampir semua aspek kehidupan manusia, mulai dari aktivitas pribadi, bisnis, hingga pemerintahan, bergantung pada teknologi digital. Namun, seiring dengan kemajuan teknologi, ancaman terhadap keamanan data dan informasi

juga meningkat. Kejahatan siber kini menjadi ancaman besar yang dapat membahayakan kepentingan individu, perusahaan, bahkan negara . Kejahatan siber adalah jenis kejahatan virtual yang memanfaatkan media komputer yang terhubung ke internet dan mengeksploitasi komputer lain yang juga terhubung ke internet. Apabila sistem operasi memiliki celah keamanan, peretas (hacker), perusak (cracker), dan pelaku siber tidak berpengalaman (script kiddies) dapat memanfaatkan celah tersebut untuk menyusup ke dalam komputer .

Serangan siber seperti ransomware, phishing, dan distributed denial of service (DDoS)semakin marak dan memiliki dampak signifikan di dunia yang kian terhubung. Salah satu kelemahan dalam penelitian keamanan siber saat ini adalah kurangnya pemahaman menyeluruh tentang sejauh mana teknologi keamanan yang diterapkan dapat melindungi infrastruktur TI. keamanan jaringan infrastruktur TI di DPM-PTSP Banyuasin perlu dioptimalkan untuk memastikan bahwa semua layanan digital dapat berjalan dengan aman, efisien, dan terpercaya.

Optimalisasi ini mencakup berbagai aspek, mulai dari penguatan infrastruktur jaringan itu sendiri, penerapan kebijakan keamanan yang komprehensif, hingga peningkatan kesadaran dan kapasitas sumber daya manusia (SDM) terkait keamanan siber.Oleh karena itu, penelitian ini tidak hanya bertujuan untuk mengidentifikasi kerangka kerja keamanan terkini tetapi juga untuk mengisi kesenjangan pengetahuan dalam sejauh mana implementasinya dapat mengatasi ancaman yang semakin kompleks.

Dengan memperhatikan aspek-aspek ini, DPM-PTSP Banyuasin dapat memastikan bahwa implementasi transformasi digital dapat berjalan dengan lancar tanpa mengorbankan keamanan dan privasi data masyarakat. Dalam konteks ini, optimalisasi keamanan jaringan infrastruktur TI bukan hanya sekadar tindakan preventif, tetapi juga menjadi bagian dari strategi untuk menciptakan layanan publik yang lebih efisien dan aman bagi masyarakat.

Metode Penelitian

Metode penelitian yang akan digunakan dalam penelitian ini adalah penelitian kualiatif dengan pendekatan studi pustaka. Langkah awal melibatkan pemilihan sumber literatur yang relevan dengan keamanan siber, infrastruktur TI, dan teknologi terkait. Jurnal ilmiah, buku referensi, laporan penelitian, dan artikel terkini akan menjadi fokus utama untuk mendapatkan wawasan mendalam. Setelah pemilihan sumber, penelitian akan melibatkan review dan analisis terperinci terhadap literatur yang terpilih.

Fokus utama analisis adalah pada kerangka kerja keamanan yang umum diterapkan, tren terkini dalam ancaman siber, serta teknologi dan strategi keamanan yang dapat efektif dalam melindungi infrastruktur TI. Rancangan penelitian yang digunakan dalam penelitian ini bersifat deskriptif dengan pendekatan kualitatif. Penelitian ini bertujuan untuk memahami secara mendalam konsep, tantangan, dan solusi terkait keamanan siber, khususnya di Indonesia.

Hasil dari studi pustaka ini akan digunakan untuk merangkum temuan literatur dan mengembangkan kesimpulan tentang kondisi keamanan infrastruktur TI DPM-PTSP saat ini. Lebih lanjut, penelitian ini akan menyusun rekomendasi praktis berdasarkan literatur yang telah dianalisis, memberikan panduan bagi organisasi dalam meningkatkan strategi keamanan mereka menghadapi ancaman siber yang terus berkembang. Dengan pendekatan studi pustaka ini, diharapkan penelitian dapat memberikan kontribusi yang berharga terhadap pemahaman dan penanganan efektif terhadap ancaman keamanan siber dalam konteks infrastruktur TI.

Hasil

1. Ancaman Cybersecurity

Ancaman cybersecurity atau ancaman siber merupakan segala bentuk gangguan, serangan, atau upaya yang dilakukan secara digital untuk merusak, mencuri, atau mengakses data dan sistem secara ilegal. Di lingkungan pemerintahan, ancaman ini semakin meningkat seiring dengan masifnya digitalisasi layanan publik. Istilah Cybersecurity sebenarnya telah ada, ketika ARPA – NET masih secara aktif di kembangkan oleh Pemerintah Amerika Serikat. Tahun 1970-an ketika peneliti Bob Thomas menciptakan program komputer yang disebut Creeper yang dapat bergerak melintasi jaringan ARPANET, meninggalkan jejak virus di dalam elemen kontrol grafis yang digunakan sebagai bantuan navigasi di antarmuka pengguna dan di halaman web. Ray Tomlinson, penemu email, menulis program Reaper, yang mengejar dan menghapus Creeper. Reaper adalah contoh pertama perangkat lunak antivirus dan program yang mereplikasi diri sendiri, menjadikannya worm komputer pertama (Davies, 2021).

Ancaman fisik terhadap infrastruktur TI merupakan suatu ancaman yang memerlukan tindakan pencegahan dan perlindungan yang cermat. Potensi kerusakan atau kehilangan terhadap komponen fisik dapat memiliki dampak signifikan terhadap integritas, ketersediaan, dan operasional keseluruhan infrastruktur TI. Pencegahan Pencurian Perangkat Keras

Pencurian perangkat keras dapat menyebabkan kerugian finansial dan kehilangan data yang penting. Untuk mencegah pencurian, langkah-langkah berikut dapat diimplementasikan:

1) Melakukan pencatatan inventaris yang akurat dan pemantauan terhadap perangkat keras un tuk mendeteksi setiap perubahan atau kehilangan.
2) Membangun pusat data dengan pertimbangan desain tahan bencana untuk melindungi perangkat keras dari gempa, banjir, atau kejadian alam lainnya.
3) Mengembangkan prosedur evakuasi dan pemulihan darurat untuk mengatasi ancaman fisik yang dapat menyebabkan kerusakan.
4) Pemantauan Aktivitas Suspicious: Melakukan pemantauan terus-menerus terhadap aktivitas di sekitar fasilitas dan mengidentifikasi tanda-tanda kegiatan mencurigakan.
5) Memberikan pelatihan kepada karyawan untuk mengenali potensi ancaman dan melaporkannya dengan segera.

2. Strategi dalam menghadapi ancaman keamanan siber

Tantangan dan Strategi Keamanan Cyber di Indonesia Keamanan informasi menjadi perhatian utama bagi bisnis di seluruh dunia karena operasi yang berada dalam pasar global, ketergantungan yang tinggi pada teknologi informasi, serta kehadiran online dan digital yang menyeluruh. Manajemen keamanan informasi menjadi tantangan penting bagi perusahaan-perusahaan ini, yang berusaha untuk mencegah terjadinya ancaman keamanan dan privasi terhadap sistem informasi dan infrastruktur jaringan. Perkembangan teknologi yang pesat telah membawa tantangan baru dalam bidang keamanan siber. Semakin banyaknya perangkat yang terhubung ke internet meningkatkan kerentanan terhadap serangan, baik oleh individu, kelompok terorganisir, maupun negara. Kekurangan tenaga ahli keamanan siber menjadi masalah serius, sementara teknik serangan yang semakin canggih mempersulit upaya perlindungan.

Kerentanan pada sistem dan aplikasi juga sering dimanfaatkan oleh penyerang. Ancaman keamanan siber terus berkembang dan memerlukan respons yang cepat dan adaptif. Namun, tantangan dalam memperkuat keamanan siber meliputi kurangnya ketersediaan pakar teknologi, munculnya penyedia layanan telekomunikasi baru, dan kurangnya peraturan internasional yang mengatur perilaku negara. Oleh karena itu, perlindungan terhadap keamanan siber menjadi semakin penting dalam menghadapi ancaman dan risiko yang terus berkembang di dunia maya.banyak beberapa aspek strategi seperti

- penerapan teknologi keamanan yang canggih seperti firewall, antivirus, dan sistem deteksi intrusi sangat diperlukan untuk mencegah serangan dari luar.

- pelatihan dan peningkatan kesadaran sumber daya manusia menjadi kunci agar para pegawai memahami risiko dan cara menghadapinya
- kebijakan keamanan yang jelas dan tegas harus dirumuskan dan diterapkan agar seluruh pihak yang terlibat menjalankan prosedur keamanan dengan disiplin.

Ancaman Operasional

Ancaman operasional merupakan tantangan serius yang timbul dari faktor internal di dalam suatu organisasi, dapat berupa kesalahan manusia, kelalaian, atau ketidakpatuhan terhadap prosedur keamanan. Kesalahan manusia seperti konfigurasi sistem yang salah atau penghapusan data tidak sengaja dapat merugikan keberlanjutan operasional. Untuk mengatasi hal ini, pelatihan karyawan secara rutin dan otomatisasi proses dapat menjadi langkah pencegahan yang efektif . Kelalaian, yang mencakup kurangnya perhatian dalam tugas-tugas operasional, juga dapat menjadi sumber ancaman. Kebijakan keamanan yang jelas dan monitoring aktivitas pengguna membantu mengurangi risiko dari kelalaian ini.Ancaman juga dapat muncul dari ketidakpatuhan terhadap prosedur keamanan yang telah ditetapkan. Edukasi karyawan tentang pentingnya mematuhi prosedur keamanan, bersamaan dengan sanksi atau konsekuensi untuk pelanggaran, menjadi kunci dalam mengurangi ancaman ini. Pengelolaan akses karyawan yang baik, melalui prinsip kepisahan kewenangan dan pemantauan akses, dapat membantu mengurangi potensi risiko.

3. Optimalisasi Infrastruktur TI dalam Mendukung Keamanan Siber

Optimalisasi infrastruktur teknologi informasi (TI) merupakan langkah krusial dalam memperkuat keamanan siber, terutama dalam menghadapi ancaman yang semakin kompleks dan canggih. Menurut penelitian oleh (Simu & Zaman, 2023), pendekatan pertahanan berlapis yang mencakup segmentasi jaringan, deteksi anomali, dan pemeriksaan integritas sistem dapat secara signifikan meningkatkan ketahanan infrastruktur TI terhadap serangan malware seperti Industroyer dan Triton.

Selain itu, modernisasi sistem TI melalui migrasi ke cloud dan penerapan teknologi kecerdasan buatan (AI) telah terbukti meningkatkan efisiensi operasional dan keamanan. Studi oleh (Onih et al., 2024) menunjukkan bahwa integrasi AI dalam infrastruktur TI dapat mempercepat deteksi ancaman dan respons terhadap insiden siber, sehingga memperkuat pertahanan organisasi terhadap serangan yang berkembang pesat.

4. Peningkatan Kapasitas Sumber Daya Manusia (SDM) dalam Keamanan TI

Sumber daya manusia (SDM) memainkan peran penting dalam menjaga keamanan TI. Meskipun teknologi canggih telah diterapkan, tanpa dukungan SDM yang kompeten dan sadar akan risiko keamanan, perlindungan terhadap infrastruktur TI tetap rentan. Penelitian oleh (Yeng et al., 2022) menekankan bahwa faktor manusia, termasuk kesadaran keamanan dan perilaku karyawan, merupakan elemen kritis dalam mencegah pelanggaran data dan serangan siber.

Untuk meningkatkan kapasitas SDM dalam keamanan TI, organisasi perlu mengimplementasikan program pelatihan yang komprehensif dan berkelanjutan. Studi oleh (Pokhrel, 2024) menunjukkan bahwa pelatihan yang berfokus pada pengembangan keterampilan teknis dan pemahaman tentang kebijakan keamanan informasi dapat meningkatkan kesiapan karyawan dalam menghadapi ancaman siber.

Kesimpulan

Transformasi digital dalam layanan publik di DPM-PTSP Kabupaten Banyuasin telah menunjukkan peningkatan signifikan dalam hal efisiensi, transparansi, dan kualitas pelayanan kepada masyarakat. Namun, optimalisasi keamanan jaringan infrastruktur TI menjadi aspek krusial yang tidak dapat diabaikan. Penelitian ini menunjukkan bahwa meskipun infrastruktur TI yang dimiliki sudah mendukung operasional layanan digital, masih terdapat tantangan berupa gangguan jaringan, keterbatasan perangkat keras, dan kurangnya tenaga ahli TI.Ancaman siber yang terus berkembang, baik dari sisi ancaman fisik, operasional, maupun digital, menuntut penerapan strategi keamanan yang komprehensif, termasuk penguatan sistem pertahanan TI, pengembangan kebijakan keamanan, serta pelatihan sumber daya manusia secara berkala. Optimalisasi melalui penerapan teknologi keamanan mutakhir, penerapan konsep Zero Trust Architecture (ZTA), serta peningkatan kesadaran keamanan pada seluruh elemen organisasi menjadi kunci keberhasilan perlindungan infrastruktur TI.Dengan upaya yang berkesinambungan dalam memperkuat keamanan jaringan dan meningkatkan kapasitas SDM, DPM-PTSP Banyuasin diharapkan mampu mempertahankan integritas, ketersediaan, dan kerahasiaan data, serta membangun kepercayaan publik terhadap layanan digital yang aman dan andal.

Daftar Pustaka

Ade Irawan, 2. H. (2024). Tantangan dan Strategi Manajemen Keamanan Siber di. *Zetroem*.

Anjuju, D. M. (2025). ANALISIS KEAMANAN INFRASTRUKTUR TEKNOLOGI INFORMASI DALAM MENGHADAPI ANCAMAN CYBERSECURITY. *Journal of Data Analytics, Information, and Computer Science*

Hoshmand, M. O. (2023). Analisis Keamanan Infrastruktur Teknologi Informasi dalam Menghadapi Ancaman Cybersecurity. *Applied Information Technology and Computer Science*.

Jhony Pranata, E. M. (2022). OPTIMASI KEAMANAN INFORMASI MENGGUNAKAN MANAJEMEN INDEKS KEAMANAN INFORMASI (KAMI) STUDI KASUS: IBISA PURWOREJO. CyberSecurity dan Forensik Digital.

Rahakbauw, I. K. (2024). Analisis Potensi Ancaman Siber pada Bidang Ekonomi di indonesia. Jurnal Kajian Stratejik Ketahanan Nasional

Rian Dwi Hapsari1*, K. G. (2023). ANCAMAN CYBERCRIME DI INDONESIA. jurnal konstituen

Onih, V. A., Sevidzem, Y. S., & Adeniji, S. (2024). The Role of AI In Enhancing Threat Detection and Response in Cybersecurity Infrastructures. International Journal of Scientific and Management Research, 07(04), 64–96. https://doi.org/10.37502/ijsmr.2024.7404

Pokhrel, S. (2024). No TitleΕΛΕΝΗ. Αγαη, 15(1), 37–48.

Simu, S. J., & Zaman, F. I. (2023). Advanced Cybersecurity Strategies for Protecting Critical Infrastructure : Strengthening the Backbone of National Security. 11(12), 999–1016. https://doi.org/10.18535/ijsrm/v11i12.ec07

Onih, V. A., Sevidzem, Y. S., & Adeniji, S. (2024). The Role of AI In Enhancing Threat Detection and Response in Cybersecurity Infrastructures. International Journal of Scientific and Management Research, 07(04), 64–96. https://doi.org/10.37502/ijsmr.2024.7404

Pokhrel, S. (2024). No TitleΕΛΕΝΗ. Αγαη, 15(1), 37–48.

Simu, S. J., & Zaman, F. I. (2023). Advanced Cybersecurity Strategies for Protecting Critical Infrastructure : Strengthening the Backbone of National Security. 11(12), 999–1016. https://doi.org/10.18535/ijsrm/v11i12.ec07

Yeng, P. K., Fauzi, M. A., & Yang, B. (2022). A Comprehensive Assessment of Human Factors in Cyber Security Compliance toward Enhancing the Security Practice of Healthcare Staff in Paperless Hospitals. *Information (Switzerland)*, *13*(7). https://doi.org/10.3390/info13070335