Inovan Publisher

Orbit: Jurnal Ilmu Multidisiplin Nusantara

| ISSN (Online) 3064-5883 |

DOI: https://doi.org/10.63217/orbit.v1i3

Strategi Manajemen Sekuriti Dalam Menghadapi Ancaman Siber di Era Digital

Jihan Luthfi Nabillah[1], Nofri Satriawan[2], Farhan Saputra[3]

[1]Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia, jihanluthfinabillah@gmail.com

[2]Universitas Negeri Padang, Padang, Indonesia, nofrisatriawan3@gmail.com

[3]Universitas Bhayangkara Jakarta Raya, Jakarta, Indonesia, farhansaputra121@gmail.com

Corresponding Author:jihanluthfinabillah@gmail.com [1]

Abstract: *The digital era has brought great progress in information technology, but also created challenges in the form of increasingly complex cyber threats. This study aims to analyze effective security Communication Science strategies in dealing with cyber threats in organizational environments. Through a qualitative case study approach, data were collected from several organizations that implement advanced technology-based security Communication Science, such as artificial intelligence (AI) and Zero Trust architecture. The results of the study show that effective strategies include a combination of advanced security technology, ongoing training for employees, and compliance with international security standards. These findings underscore the importance of a comprehensive approach to improving organizational resilience in the face of cyber threats. By implementing a comprehensive security Communication Science strategy, organizations can minimize risks and strengthen their information security in the digital era.*

Keyword: Security Management Strategy, Cyber Threats, Digital Era

Abstrak: Era digital telah membawa kemajuan besar dalam teknologi informasi, tetapi juga menciptakan tantangan berupa ancaman siber yang semakin kompleks. Penelitian ini bertujuan untuk menganalisis strategi Ilmu Komunikasi sekuriti yang efektif dalam menghadapi ancaman siber di lingkungan organisasi. Melalui pendekatan kualitatif studi kasus, data dikumpulkan dari beberapa organisasi yang menerapkan Ilmu Komunikasi sekuriti berbasis teknologi canggih, seperti kecerdasan buatan (AI) dan arsitektur Zero Trust. Hasil penelitian menunjukkan bahwa strategi yang efektif mencakup kombinasi antara teknologi keamanan yang canggih, pelatihan berkelanjutan bagi karyawan, dan kepatuhan terhadap standar keamanan internasional. Temuan ini menggarisbawahi pentingnya pendekatan yang menyeluruh untuk meningkatkan ketahanan organisasi dalam menghadapi ancaman siber. Dengan menerapkan strategi Ilmu Komunikasi sekuriti yang komprehensif, organisasi dapat meminimalkan risiko dan memperkuat keamanan informasi mereka di era digital.

Kata Kunci: Strategi Manajemen Sekuriti, Ancaman Siber, Era Digital

PENDAHULUAN

Di era digital saat ini, teknologi informasi telah menjadi fondasi utama bagi operasional organisasi di berbagai sektor, baik pemerintahan, bisnis, pendidikan, hingga kesehatan. Ketergantungan pada teknologi digital membawa berbagai kemudahan, seperti efisiensi operasional, aksesibilitas informasi yang lebih cepat, serta peningkatan produktivitas(Al Jum'ah, 2019). Namun, di balik kemajuan ini, terdapat tantangan signifikan berupa ancaman siber yang semakin kompleks dan sulit diantisipasi. Ancaman ini dapat berbentuk pencurian data, peretasan sistem, serangan malware, ransomware, hingga distributed denial-of-service (DDoS) yang mampu melumpuhkan sistem operasional dalam hitungan detik (Al Jum'ah, 2019).

Kemunculan berbagai ancaman siber ini menjadi semakin relevan karena meningkatnya kompleksitas teknologi yang digunakan. Adopsi teknologi Internet of Things (IoT), kecerdasan buatan (AI), dan komputasi awan (cloud computing) pada berbagai industri, misalnya, memperbesar ruang ancaman siber karena semakin banyak perangkat yang terhubung ke jaringan (Muzakir Ully, 2023). Ketergantungan ini menciptakan lingkungan yang lebih rentan terhadap risiko keamanan, di mana penyerang siber dapat dengan mudah mengeksploitasi celah atau kerentanan yang ada pada jaringan atau sistem informasi. Oleh karena itu, penting bagi organisasi untuk memiliki pendekatan yang sistematis dan terstruktur dalam Ilmu Komunikasi sekuriti guna melindungi data dan operasional dari potensi ancaman tersebut (Ali et al., 2024).

Ilmu Komunikasi sekuriti, atau keamanan informasi, menjadi salah satu aspek krusial dalam mengantisipasi dan memitigasi risiko siber. Ilmu Komunikasi sekuriti tidak hanya mencakup tindakan teknis, seperti pemasangan firewall atau enkripsi data, tetapi juga menyangkut aspek kebijakan, prosedur, dan kesadaran sumber daya manusia (Kehista et al., 2023). Pengembangan strategi Ilmu Komunikasi sekuriti yang efektif memerlukan pemahaman mendalam tentang risiko siber yang dihadapi serta teknologi yang tersedia untuk melindungi aset informasi. Dalam hal ini, pendekatan Ilmu Komunikasi risiko menjadi esensial. Melalui pendekatan tersebut, organisasi dapat mengidentifikasi dan mengevaluasi berbagai risiko siber, serta menentukan tindakan preventif atau korektif yang perlu diambil untuk meminimalkan dampaknya (Ilhamalimy & Ali, 2021).

Studi ini bertujuan untuk menjawab kebutuhan yang mendesak akan strategi Ilmu Komunikasi sekuriti yang komprehensif di era digital. Sebuah strategi sekuriti yang baik harus melibatkan beberapa komponen kunci, termasuk teknologi canggih, kerangka kerja *Zero Trust Architecture* (ZTA), serta pelatihan dan kesadaran keamanan bagi seluruh anggota organisasi. Teknologi seperti kecerdasan buatan dan pembelajaran mesin, misalnya, telah terbukti mampu mendeteksi dan merespons ancaman dengan lebih cepat dan akurat. Teknologi ini memungkinkan organisasi untuk melakukan analisis ancaman secara real-time dan otomatis, sehingga dapat mengidentifikasi pola serangan yang tidak terdeteksi oleh sistem tradisional. Adopsi *Zero Trust Architecture* juga semakin penting dalam lingkungan yang terhubung dengan jaringan global, di mana prinsip utamanya adalah "tidak mempercayai siapa pun, selalu memverifikasi."

Pendekatan ini membatasi akses hanya pada pihak-pihak yang sah dengan autentikasi berlapis, sehingga mengurangi risiko kebocoran data atau akses yang tidak diizinkan (Felix & Aklani, 2025).

Selain implementasi teknologi, faktor manusia juga memainkan peran penting dalam Ilmu Komunikasi sekuriti. Banyak serangan siber yang berhasil karena adanya kelemahan dalam kesadaran dan perilaku karyawan terkait keamanan informasi (Ilhami, 2022). Oleh karena itu, pelatihan berkelanjutan mengenai keamanan siber sangat diperlukan untuk meningkatkan pemahaman karyawan tentang potensi ancaman dan cara menanggulangi risiko. Program pelatihan yang baik akan memberikan pengetahuan kepada karyawan mengenai tindakan preventif dasar, seperti mengenali email phishing, melindungi kata sandi, dan mengikuti protokol keamanan yang ditetapkan. Dengan demikian, budaya keamanan dapat terbentuk dalam organisasi, di mana setiap anggota memiliki kesadaran untuk berperan aktif dalam menjaga keamanan informasi (Citra Kurniawan, ST, 2016).

Di samping itu, kepatuhan terhadap standar keamanan internasional juga menjadi fondasi yang penting dalam menyusun strategi sekuriti yang andal. Standar-standar seperti ISO 27001 dan NIST *Cybersecurity Framework* menyediakan panduan yang sistematis dalam menyusun kebijakan, prosedur, dan kontrol keamanan yang sesuai dengan kebutuhan organisasi. Kepatuhan terhadap standar ini tidak hanya meningkatkan keamanan informasi, tetapi juga meningkatkan reputasi organisasi di mata publik dan pemangku kepentingan (Al Jum'ah, 2019).

Melalui penelitian ini, akan dieksplorasi bagaimana penerapan strategi Ilmu Komunikasi sekuriti yang efektif dapat membantu organisasi untuk menghadapi ancaman siber yang terus berkembang. Artikel ini akan memaparkan berbagai pendekatan dan teknologi yang relevan dalam membangun sistem keamanan yang tangguh. Diharapkan bahwa temuan-temuan dalam penelitian ini dapat memberikan panduan praktis bagi organisasi dalam memperkuat sistem sekuriti mereka, meningkatkan ketahanan terhadap ancaman siber, dan mengembangkan budaya keamanan yang solid di era digital ini.

Berdasarkan latar belakang di atas, maka mendapatkan rumusan masalah dalam penelitian ini adalah sebagai berikut :

1. Bagaimana strategi Ilmu Komunikasi sekuriti yang efektif dalam menghadapi ancaman siber yang semakin kompleks di era digital?
2. Bagaimana peran teknologi keamanan seperti kecerdasan buatan (AI) dan *Zero Trust Architecture* dalam memperkuat sistem keamanan organisasi?
3. Bagaimana pengaruh pelatihan keamanan siber bagi karyawan terhadap efektivitas Ilmu Komunikasi sekuriti di dalam organisasi?
4. Sejauh mana kepatuhan terhadap standar keamanan internasional meningkatkan ketahanan organisasi terhadap ancaman siber?

METODE

Penelitian deskriptif kualitatif merupakan metode penelitian yang bertujuan untuk menggambarkan dan memahami fenomena secara mendalam berdasarkan data dan informasi yang dikumpulkan secara kualitatif. Dalam konteks penelitian ini, metode deskriptif kualitatif dipilih untuk memperoleh pemahaman yang lebih komprehensif mengenai bagaimana Ilmu Komunikasi sekuriti mengimplementasikan teknologi lanjutan

untuk melindungi data dari berbagai ancaman siber di era digital. Penelitian ini tidak berfokus pada pengukuran angka atau statistik, melainkan lebih kepada deskripsi detail mengenai proses, strategi, dan metode yang diterapkan untuk memperkuat keamanan data di tengah ancaman siber yang semakin kompleks.

Dasar dari penelitian ini adalah hasil-hasil penelitian sebelumnya yang telah diterbitkan, baik dalam publikasi domestik maupun internasional. Dengan memanfaatkan berbagai referensi, peneliti dapat memahami lebih lanjut mengenai perkembangan terkini di bidang keamanan data. Alat referensi seperti Mendeley dimanfaatkan untuk mengelola daftar pustaka yang relevan, termasuk penelitian-penelitian dari platform seperti Google Scholar dan sumber daring lainnya. Hal ini membantu peneliti untuk mengumpulkan dan mengorganisasikan informasi penting yang mendukung topik yang dibahas.

Sebagai pendekatan deskriptif kualitatif, penelitian ini bertujuan untuk memperoleh hasil yang berwujud dalam bentuk narasi, deskripsi, atau gambar yang mendukung pemahaman mengenai topik. Data yang dikumpulkan bukan dalam bentuk angka, melainkan deskripsi rinci tentang upaya Ilmu Komunikasi sekuriti dalam memitigasi ancaman melalui implementasi teknologi canggih. Misalnya, penerapan kecerdasan buatan, machine learning, atau *Zero Trust Architecture* menjadi fokus perhatian untuk memahami peran teknologi dalam mengamankan data. Penelitian ini diharapkan menghasilkan wawasan baru yang dapat memberikan solusi inovatif serta menjadi acuan bagi pengembangan kebijakan keamanan data yang lebih kuat, khususnya dalam merespons tantangan yang dinamis di era digital.

HASIL DAN PEMBAHASAN

Analisis Risiko Siber dalam Organisasi

Analisis risiko siber merupakan proses sistematis untuk mengidentifikasi, mengevaluasi, dan mengelola risiko yang berkaitan dengan ancaman siber. Hasil penelitian menunjukkan bahwa organisasi yang memiliki sistem Ilmu Komunikasi risiko yang baik mampu mengantisipasi dan merespons ancaman siber dengan lebih efektif. Ini berarti bahwa mereka telah mengidentifikasi potensi risiko dan menerapkan langkah-langkah mitigasi untuk meminimalkan dampak jika terjadi serangan.

Organisasi yang melakukan analisis risiko secara berkala cenderung memiliki ketahanan yang lebih tinggi terhadap serangan siber. Mereka dapat secara proaktif mendeteksi celah dalam keamanan dan menerapkan perbaikan sebelum celah tersebut dieksploitasi oleh penyerang. Analisis risiko yang komprehensif mencakup evaluasi terhadap aset, kerentanan, ancaman, dan dampak potensial, sehingga organisasi dapat mengalokasikan sumber daya dengan lebih efektif untuk memperkuat pertahanan mereka.

Peran Teknologi Terkini dalam Mitigasi Ancaman

Penggunaan teknologi canggih seperti kecerdasan buatan (AI) dan pembelajaran mesin (ML) menjadi krusial dalam meningkatkan kemampuan organisasi untuk mendeteksi dan merespons ancaman siber. Penelitian menemukan bahwa implementasi teknologi ini memungkinkan deteksi ancaman secara real-time, sehingga organisasi dapat merespons lebih cepat terhadap insiden keamanan.

Zero Trust Architecture (ZTA) juga menjadi perhatian dalam mitigasi ancaman siber. ZTA menuntut verifikasi identitas setiap pengguna, perangkat, dan aplikasi yang mencoba mengakses sistem, terlepas dari apakah mereka berada di dalam atau di luar jaringan organisasi. Pendekatan ini berhasil mengurangi akses yang tidak diotorisasi dan meningkatkan perlindungan data. Dengan menerapkan prinsip Zero Trust, organisasi dapat lebih baik mengelola risiko dan mengurangi kemungkinan kebocoran data.

Efektivitas Pelatihan Keamanan Siber

Pelatihan keamanan siber bagi karyawan merupakan langkah penting dalam membangun budaya keamanan di tempat kerja. Penelitian menunjukkan bahwa organisasi yang mengintegrasikan program pelatihan rutin memiliki tingkat keberhasilan yang lebih tinggi dalam mencegah serangan yang diakibatkan oleh kesalahan manusia.

Kesalahan manusia, seperti mengklik tautan yang berbahaya atau menggunakan kata sandi yang lemah, merupakan salah satu penyebab utama terjadinya pelanggaran keamanan. Dengan memberikan pelatihan yang efektif, karyawan dapat belajar untuk mengenali tanda-tanda serangan siber dan mengambil tindakan yang tepat untuk melindungi data dan sistem organisasi.

Program pelatihan juga harus diperbarui secara berkala untuk mencakup teknik dan ancaman baru yang muncul, memastikan bahwa karyawan selalu terinformasi dan siap menghadapi tantangan keamanan yang terus berkembang.

Implementasi Kebijakan dan Kepatuhan Terhadap Standar

Kepatuhan terhadap kerangka kerja dan standar internasional, seperti ISO 27001, memainkan peran penting dalam menciptakan sistem Ilmu Komunikasi keamanan yang kuat. Organisasi yang mengikuti standar ini memiliki prosedur dan kebijakan yang lebih baik dalam mengelola risiko keamanan siber.

Standar internasional membantu organisasi dalam menyusun kebijakan yang relevan, menyediakan panduan tentang pengelolaan risiko, perlindungan data, dan penanganan insiden. Implementasi kebijakan yang sesuai tidak hanya membantu organisasi dalam mematuhi regulasi yang berlaku tetapi juga meningkatkan kepercayaan dari pelanggan dan mitra bisnis.

KESIMPULAN

Penelitian ini menyimpulkan bahwa teknologi terkini, termasuk kecerdasan buatan (AI) dan pembelajaran mesin (ML), telah terbukti sangat efektif dalam mendeteksi dan merespons ancaman siber secara real-time. Implementasi Zero Trust Architecture (ZTA) semakin memperkuat pertahanan organisasi dengan membatasi akses hanya kepada pengguna dan perangkat yang terverifikasi. Oleh karena itu, investasi dalam teknologi canggih harus menjadi prioritas bagi organisasi untuk menghadapi tantangan keamanan yang kompleks.

Dalam era digital yang semakin canggih dan kompleks, Ilmu Komunikasi keamanan siber yang efektif tidak hanya menjadi pilihan, tetapi merupakan kebutuhan mendesak bagi organisasi. Dengan mengintegrasikan analisis risiko, menerapkan teknologi canggih, melatih karyawan, mematuhi standar internasional, dan berinvestasi dalam infrastruktur keamanan, organisasi dapat mengatasi ancaman siber dengan lebih baik. Organisasi yang berhasil membangun budaya keamanan yang solid dan responsif akan lebih mampu melindungi aset mereka, mempertahankan reputasi, dan memastikan kelangsungan operasional di tengah tantangan keamanan yang terus berubah.

REFERENSI

Al Jum'ah, M. N. (2019). Analisa Keamanan Dan Hukum Untuk Pelindungan Data Privasi. *Cyber Security Dan Forensik Digital*, *1*(2), 39–44. https://doi.org/10.14421/csecurity.2018.1.2.1370

Ali, M. F., Fahrullah, R., & Perkasa, D. H. (2024). *Strategi Penerapan Kecerdasan Buatan (AI) Dalam Mengelola Manajemen Sumber Daya Manusia Internasional (IHRM)*. *6*(2), 1121–1129.

Citra Kurniawan, ST, M. (2016). *IMPLEMENTASI ARTIFICIAL INTELLIGENCE DALAM*

PENYELESAIAN MASALAH DENGAN METODE UNIFICATION DAN BACK TRACKING VISUAL PROLOG (Studi Kasus: pemilihan mahasiswa terbaik).

Felix, I., & Aklani, S. A. (2025). *Analysis of the use of ChatGPT in Question and Answer Systems as an Educational Tool*. *6*(3), 1356–1363.

Ilhamalimy, R. R., & Ali, H. (2021). Model Perceived Risk and Trust: E-Wom and Purchase Intention (the Role of Trust Mediating in Online Shopping in Shopee Indonesia). *Dinasti International Journal of Digital Business Management*, *2*(2), 204–221. https://doi.org/10.31933/dijdbm.v2i2.651

Ilhami, D. A. S. (2022). Data Privasi dan Keamanan Siber pada Smart-City: Tinjauan Literatur. *Jurnal Sains, Nalar, Dan Aplikasi Teknologi Informasi*, *2*(1), 51–60. https://doi.org/10.20885/snati.v2i1.19

Kehista, A. P., Fauzi, A., Tamara, A., Putri, I., Fauziah, N. A., Klarissa, S., & Damayanti, V. B. (2023). Analisis Keamanan Data Pribadi pada Pengguna E-Commerce: Ancaman, Risiko, Strategi Kemanan (Literature Review). *Jurnal Ilmu Manajemen Terapan*, *4*(5), 625–632.

Muzakir Ully. (2023). PENERAPAN KECERDASAN BUATAN DALAM SISTEM INFORMASI: TINJAUAN LITERATUR TENTANG APLIKASI, ETIKA, DAN DAMPAK SOSIAL. *Jurnal Review Pendidikan Dan Pengajaran*, *6*(4), 1163–1169.