Journal of Information and Information Security (JIFORTY)
Vol. 5, No. 2, Desember 2024, *321-334*
e-ISSN : 2722-4058
Available Online at http://ejurnal.ubharajaya.ac.id/index.php/jiforty

Meningkatkan Keamanan Jaringan Dalam Pendekatan Terhadap Ancaman Siber Modern

Muhammad Ryan Widianto [1,*], Fibril Acyuta Salsabitah [1], Muhammad Daffa Arifin [1], Mohammad Irsyad Suryanata [1]

[1]Informatika;Universitas Bhayangkara Jakarta Raya;Jl. Raya Perjuangan No. 81 Marga Mulya, Bekasi Utara Jawa Barat, 17143,(021) 88955882
202210715220@mhs.ubharajaya.ac.id , 202210715186@mhs.ubharajaya.ac.id, 202210715225@mhs.ubharajaya.ac.id , 202210715196@mhs.ubharajaya.ac.id

* Korespondensi: e-mail: 202210715220@mhs.ubharajaya.ac.id

Diterima: 9 Jan 25; Review: 9 Jan 25; Disetujui: 15 Jan 25; Diterbitkan: 15 Jan 25

Abstract

The escalating complexity of digital threats has transformed the landscape of cybercrime, necessitating robust security frameworks to protect digital infrastructure. Indonesia faces an array of cybersecurity challenges, encompassing unauthorized system penetration, data compromise, digital infrastructure disruption, and malicious software deployment. The management of these risks encompasses systematic approaches to detection, evaluation, mitigation, and ongoing monitoring. Strategic defense initiatives include recruiting specialized digital security professionals to enhance national protection mechanisms and establishing dedicated cybersecurity operations facilities. As digital transformation accelerates, the protection of information assets and computing resources has become paramount. This research examines the multifaceted challenges of digital security, with particular emphasis on methodological approaches, empirical observations, and analytical discourse regarding Indonesia's cybersecurity landscape. The opening segment contextualizes the critical nature of digital defense mechanisms amid rising technological threats. The theoretical framework examines contemporary cybersecurity paradigms and relevant scholarly contributions. The investigation employs qualitative methodologies, utilizing targeted case analyses to thoroughly examine digital security challenges. The investigation reveals that while students demonstrate basic cybersecurity awareness, substantial improvements are needed in Indonesia's broader digital defense capabilities. The study identifies key protective measures against digital threats, including robust authentication protocols, critical information consumption practices, and enhanced security awareness programs. The analysis highlights the intricate nature of combating digital threats and emphasizes the need for strengthened institutional responses coupled with enhanced public understanding of digital safety protocols.
Keywords*:* Cybersecurity, Digital Transformation, Digital Threats, Security Awareness, Qualitative Methodology.

Abstrak

Meningkatnya kompleksitas ancaman digital telah mengubah lanskap kejahatan siber, yang mengharuskan adanya kerangka keamanan yang kuat untuk melindungi infrastruktur digital. Indonesia menghadapi berbagai tantangan keamanan siber, meliputi penetrasi sistem tanpa izin, kompromi data, gangguan infrastruktur digital, dan penyebaran perangkat lunak berbahaya. Pengelolaan risiko ini mencakup pendekatan sistematis untuk deteksi, evaluasi, mitigasi, dan

pemantauan berkelanjutan. Inisiatif pertahanan strategis termasuk merekrut profesional keamanan digital khusus untuk meningkatkan mekanisme perlindungan nasional dan membangun fasilitas operasi keamanan siber khusus. Seiring percepatan transformasi digital, perlindungan aset informasi dan sumber daya komputasi menjadi sangat penting. Penelitian ini mengkaji tantangan beragam keamanan digital, dengan penekanan khusus pada pendekatan metodologis, pengamatan empiris, dan diskursus analitis mengenai lanskap keamanan siber Indonesia. Bagian pembuka mengkontekstualisasikan sifat kritis mekanisme pertahanan digital di tengah ancaman teknologi yang meningkat. Kerangka teoretis mengkaji paradigma keamanan siber kontemporer dan kontribusi ilmiah yang relevan. Investigasi menggunakan metodologi kualitatif, memanfaatkan analisis kasus terarah untuk menguji secara menyeluruh tantangan keamanan digital. Investigasi mengungkapkan bahwa meskipun mahasiswa menunjukkan kesadaran dasar akan keamanan siber, peningkatan substansial diperlukan dalam kemampuan pertahanan digital Indonesia secara lebih luas. Studi ini mengidentifikasi langkah-langkah perlindungan utama terhadap ancaman digital, termasuk protokol otentikasi yang kuat, praktik konsumsi informasi kritis, dan program peningkatan kesadaran keamanan. Analisis menyoroti sifat rumit dalam memerangi ancaman digital dan menekankan kebutuhan akan respons institusional yang diperkuat serta ditingkatkannya pemahaman publik tentang protokol keamanan digital.
Kata kunci: Keamanan Siber, Transformasi Digital, Ancaman Digital, Kesadaran Keamanan, Metodologi Kualitatif.

1. Pendahuluan

Perlindungan dunia maya merupakan rangkaian tindakan komprehensif yang mencakup berbagai komponen digital, termasuk infrastruktur fisik, program aplikasi, dan sistem interkoneksi, untuk mengamankannya dari berbagai bentuk gangguan dan ancaman. Sebagai disiplin terapan, fokus utamanya adalah mengamankan seluruh ekosistem digital, mulai dari perangkat komputasi hingga basis data sensitif, dari beragam risiko keamanan.

Tata kelola keamanan mengacu pada pertahanan berkelanjutan; tata kelola kelangsungan usaha, hingga kesiapan operasional saat terjadi bencana. Bersama-sama, kedua komponen ini membentuk manajemen keamanan (Adawiyyah et al., 2023).

Di tengah akselerasi transformasi digital, aspek keamanan maya menjadi semakin vital. Integrasi teknologi informasi telah meresap ke berbagai sektor kehidupan, mulai dari aktivitas komersial hingga urusan kenegaraan dan ranah personal. Konsekuensinya, diperlukan pendekatan multilateral yang mengintegrasikan berbagai aspek strategis dan regulasi untuk mencapai tingkat perlindungan yang optimal.

Diperlukan analisis mendalam tentang ancaman yang dihadapi dalam lingkungan digital dan solusi yang dapat diterapkan untuk meningkatkan keamanan cyber (Soesanto et al., 2023).

Transformasi digital yang pesat mengakibatkan peningkatan signifikan dalam volume dan kerumitan informasi yang beredar dalam ruang maya. Dalam konteks ini, pengamanan informasi menjadi prioritas yang tidak dapat

dikesampingkan. Berbagai bentuk ancaman digital, seperti pembobolan sistem, pengambilan data tanpa izin, dan program pemerasan digital, menjadi risiko nyata yang dapat berdampak luas.

Masalah utama yang dihadapi adalah kurangnya sistem keamanan yang memadai pada jaringan yang ada, terutama untuk melindungi router Mikrotik dari serangan Brute Force dan Fraud (Syaifuddin et al., 2024)

Perkembangan inovasi digital mensyaratkan implementasi sistem pengamanan yang andal untuk melindungi berbagai tingkatan data, baik individual, korporat, maupun nasional. Tantangan kontemporer terletak pada pengembangan mekanisme pertahanan yang adaptif terhadap ancaman yang terus berevolusi.

Keamanan digital menjadi suatu aspek yang penting untuk diperhatikan karena tujuannya adalah melindungi informasi dari potensi risiko, termasuk penyebaran berita palsu, kejahatan digital, dan ancaman lainnya (Pengabdian et al., 2024).

2. Metode Penelitian

Metode penelitian adalah suatu cara yang digunakan untuk memperoleh informasi dan data, yang kemudian digabungkan dengan informasi dan data lain untuk diproses, dianalisis, dan dipelajari lebih lanjut. Penelitian ini menggunakan metode kualitatif dengan pendekatan studi kasus. Pendekatan ini bersifat deskriptif, tetapi lebih berfokus pada analisis mendalam untuk menggali informasi secara rinci.

Keamanan siber merupakan komponen penting dalam menjaga keamanan dan integritas informasi di era digital yang berubah dengan cepat (Soesanto et al., 2023) (Putra et al., 2024).

Dalam pelaksanaan penelitian ini, pengumpulan data dilakukan melalui beberapa teknik yaitu penyebaran angket atau kuesioner kepada narasumber, observasi, serta pencarian informasi dari media sosial. Untuk membantu peneliti menyelesaikan penelitian dengan lebih terorganisir, berikut adalah tahapan metodologi penelitian yang akan dilakukan:

Sumber: Hasil Penelitian (2024)

Gambar 1. Flowchart Tahapan Penelitian

Pada Gambar 1 menunjukan Alur dalam flowchart dalam sebuah jenis diagram yang mewakili algoritme, alur kerja atau proses, yang menampilkan Langkah Langkah dalam bentuk symbol-simbol grafis.

1. Studi Literatur

   Tahap ini melibatkan pengkajian mendalam terhadap berbagai sumber literatur yang relevan, seperti jurnal ilmiah, buku referensi, dan dokumentasi teknis tentang keamanan jaringan. Studi literatur ini penting untuk membangun pemahaman teoretis yang kuat dan mengidentifikasi praktik terbaik dalam implementasi keamanan jaringan.

2. Pengumpulan Data

   Sesuai dengan pendekatan kualitatif yang dipilih, pengumpulan data dilakukan melalui tiga metode utama yang saling melengkapi untuk mendapatkan

informasi yang mendalam dan komprehensif. Pertama, penyebaran angket atau kuesioner kepada narasumber yang melibatkan pihak-pihak terkait dalam penelitian. Metode ini bertujuan untuk mengumpulkan informasi langsung dari responden mengenai pandangan, pengalaman, dan pendapat mereka terkait topik yang sedang diteliti.

Kedua, dilakukan observasi langsung terhadap objek penelitian. Observasi ini bertujuan untuk memahami secara langsung kondisi nyata di lapangan, baik dari segi fisik maupun perilaku yang terkait dengan penelitian.

Ketiga, pencarian informasi dari media sosial digunakan untuk melengkapi data yang diperoleh dari angket dan observasi. Media sosial menjadi sumber data tambahan yang relevan, terutama untuk memahami perspektif publik, tren, dan informasi yang bersifat dinamis terkait dengan topik penelitian.

Dengan menggabungkan ketiga metode ini, penelitian diharapkan mampu memberikan hasil yang lebih kaya dan menyeluruh, mencakup perspektif langsung dari narasumber, pengamatan lapangan, serta data sekunder dari media sosial yang relevan.

3. Perancangan Topologi

   Berdasarkan hasil pengumpulan data dan analisis kebutuhan, dilakukan perancangan sistem melalui beberapa tahap penting. Tahap pertama adalah analisis kebutuhan sistem keamanan jaringan, yang bertujuan untuk mengidentifikasi potensi ancaman, menentukan kebutuhan perlindungan, dan memastikan sistem memenuhi standar keamanan yang diperlukan. Selanjutnya, dilakukan perancangan arsitektur dan topologi jaringan, mencakup pengaturan perangkat keras dan perangkat lunak, pemilihan protokol komunikasi, serta segmentasi jaringan untuk meningkatkan efisiensi dan keamanan.

4. Pengujian Keamanan Jaringan

   Tahap pengujian keamanan jaringan dilakukan untuk memvalidasi efektivitas sistem yang telah dirancang, memastikan setiap elemen memenuhi standar keamanan yang diharapkan. Proses ini dimulai dengan evaluasi mekanisme keamanan yang diimplementasikan, mencakup pengujian fungsi firewall, enkripsi data, autentikasi pengguna, serta sistem deteksi dan pencegahan intrusi (IDS/IPS) untuk memastikan semua komponen berfungsi sesuai spesifikasi. Selanjutnya, dilakukan pengujian ketahanan sistem terhadap berbagai ancaman, seperti serangan DDoS, malware, phishing, dan eksploitasi kerentanan, guna mengidentifikasi potensi kelemahan yang mungkin ada.

   Tantangan utama yang akan dihadapi dalam era digital ini adalah menerapkan pertahanan dan keamanan data siber. Kejahatan(Azzahrah et al., 2024)

3. Hasil dan Pembahasan

Keamanan jaringan mencakup kebijakan, metode, dan teknologi yang bertujuan melindungi jaringan komputer beserta data di dalamnya. Fokus utamanya adalah menjaga integritas, privasi, dan ketersediaan informasi sambil mencegah akses ilegal serta ancaman dari dalam maupun luar jaringan.

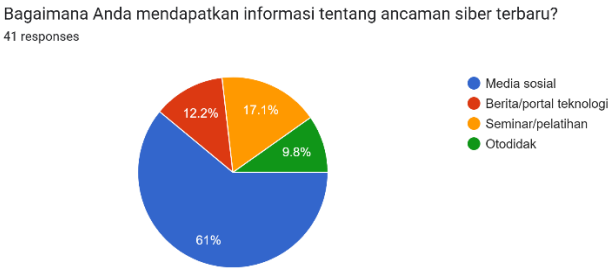
Pratama Persadha, mengatakan bahwa serangan siber dan ancaman peretasan ini terjadi berkali-kali dalam satu bulan, hal ini yang menyebabkan keamanan siber di Indonesia dalam tahap Red Alert atau tahap berbahaya (Vimy et al., 2022).

Langkah-langkah seperti kontrol akses, perlindungan dari program berbahaya, penggunaan firewall, enkripsi, dan pemantauan secara berkala menjadi bagian dari strategi keamanan ini. Dengan menerapkan keamanan jaringan yang efektif, organisasi dapat menghindari gangguan operasional, pencurian informasi, atau serangan siber yang dapat mengakibatkan kerugian besar.

Sumber: Penelitian (2024)

Gambar 2. Diagram Konsep Keamanan Jaringan

Pada Gambar 2 menunjukan data dari diagram, sebanyak 17,1% responden memiliki pemahaman yang sangat baik tentang konsep keamanan jaringan, sementara mayoritas responden, yaitu 53,7%, mengaku memahami topik ini dengan baik, diikuti oleh 29,3% responden yang memiliki tingkat pemahaman cukup namun masih memerlukan peningkatan; menariknya, tidak ada responden yang sama sekali tidak memahami konsep ini, menunjukkan bahwa secara umum tingkat pengetahuan tentang keamanan jaringan di kalangan responden sudah cukup baik, meskipun masih ada ruang untuk meningkatkan wawasan pada sebagian kelompok agar pemahaman mereka lebih mendalam.



Sumber: Hasil Penelitian (2024)

Gambar 3. Diagram Informasi Ancaman Siber Terbaru

Pada Gambar 3 menunjukan diagram tersebut, sebanyak 61% responden memperoleh informasi tentang ancaman siber terbaru melalui media sosial, menjadikannya sumber utama informasi; sementara itu, 17,1% responden mendapatkan informasi dari berita atau portal teknologi, diikuti oleh 12,2% yang memanfaatkan seminar atau pelatihan, serta 9,8% lainnya yang belajar secara mandiri (otodidak), yang secara keseluruhan menunjukkan bahwa media sosial menjadi platform yang dominan untuk memperoleh informasi terkait ancaman siber, meskipun beberapa responden juga memanfaatkan sumber-sumber lain untuk memperluas wawasan mereka.

Penggunaan teknologi keamanan seperti SNORT IDS, Port Knocking, dan Artificial Intelligence (AI) telah diterapkan untuk deteksi ancaman siber. SNORT IDS efektif dalam mendeteksi malware dan ransomware, sementara AI meningkatkan deteksi ransomware.(Khairunnisa et al., 2024)

Sumber: Hasil Penelitian (2024)

Gambar 4. Grafik Serangan Ancaman Keamanan Siber

Pada Gambar 4. menunjukan diagram batang, sebagian besar responden mengenal istilah Phishing (97,6%) dan Malware (95,1%), menunjukkan bahwa kedua istilah tersebut lebih umum diketahui, diikuti oleh Ransomware (87,8%) dan DDoS (75,6%) yang juga memiliki tingkat pengenalan cukup tinggi; sedangkan

istilah Man-in-the-Middle (MitM) dikenal oleh 39% responden, dan Zero-Day Exploit memiliki tingkat pengenalan terendah, yaitu hanya 19,5%, yang secara keseluruhan mencerminkan bahwa istilah-istilah yang lebih sering dibahas di media atau kasus publik cenderung lebih mudah dikenali, sementara istilah teknis seperti MitM dan Zero-Day Exploit membutuhkan lebih banyak edukasi untuk dipahami oleh responden.

3.1 Pemahaman Persepsi Ancaman Siber

Persepsi ancaman siber merujuk pada cara individu atau kelompok memahami, menilai, dan merespons berbagai risiko atau bahaya yang berasal dari aktivitas di dunia maya. Ancaman ini mencakup serangan seperti phishing, malware, ransomware, serangan DDoS (Distributed Denial of Service), Man-in-the-Middle (MitM), dan Zero-Day Exploit, yang masing-masing memiliki dampak serta tingkat risiko yang berbeda-beda.

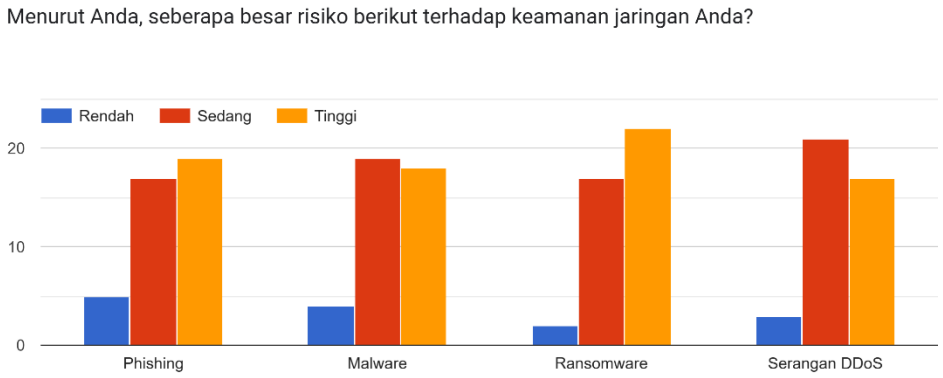
Sumber: Hasil Penelitian (2024)

Gambar 5. Diagram Pemahaman Ancaman Siber

Pada Gambar 5 menunjukan responden, yaitu 58,5%, menyatakan "Setuju" bahwa ancaman siber semakin kompleks dan sulit diatasi, sementara 19,5% lainnya "Sangat Setuju" dengan pernyataan tersebut. Dengan demikian, sebanyak 78% responden mengakui peningkatan kompleksitas ancaman siber. Sebaliknya, 22% responden bersikap "Netral," menunjukkan bahwa mereka mungkin tidak memiliki pengalaman langsung dengan ancaman siber atau belum memahami sepenuhnya dampaknya. Tidak ada responden yang memilih "Tidak Setuju" maupun "Sangat Tidak Setuju," menandakan kesadaran yang cukup tinggi terhadap isu ini di antara peserta survei.

Hasil ini mencerminkan kekhawatiran masyarakat terhadap perkembangan ancaman siber, yang mungkin disebabkan oleh peningkatan serangan seperti ransomware, phishing, dan malware, serta kemajuan teknologi yang membuat ancaman ini semakin sulit diatasi.

Untuk mengatasi tantangan ini, diperlukan langkah-langkah konkret, seperti kampanye edukasi tentang keamanan siber, adopsi teknologi perlindungan seperti firewall dan antivirus, serta pelatihan untuk meningkatkan kesadaran keamanan di kalangan masyarakat. Selain itu, kolaborasi antara sektor publik dan swasta sangat penting dalam menghadapi ancaman siber secara kolektif dan efektif.



Sumber: Hasil Penelitian (2024)

Gambar 6. Grafik Risiko Terhadap Keamanan Jaringan

Pada Gambar 6 menunjukan grafik kuesioner yang ditampilkan, terdapat survei tentang persepsi risiko keamanan jaringan terhadap empat jenis ancaman utama: phishing, malware, ransomware, dan serangan DDoS. Tingkat risiko dibagi menjadi tiga kategori: rendah (biru), sedang (merah), dan tinggi (oranye).

Hasil survei menunjukkan bahwa phishing dan ransomware dianggap memiliki risiko tinggi oleh sebagian besar responden, dengan nilai tertinggi sekitar 20 untuk keduanya. Sementara itu, malware dan serangan DDoS dinilai memiliki risiko sedang yang lebih dominan. Untuk setiap jenis ancaman, hanya sedikit responden yang menganggapnya berisiko rendah, dengan nilai di bawah 5.

Kejahatan siber dapat mengganggu dan menjadi ancaman bagi keamanan nasional suatu negara dikarenakan saat ini banyak negara yang sudah mengkoneksikan data-data dan kontrolnya terhadap beberapa sektor melalui internet atau daring (online) (Rosy, 2020).

3.2 Pencegahan Dalam Menangani Keamanan Jaringan

Pencegahan dalam menangani keamanan jaringan meliputi serangkaian langkah komprehensif yang saling terintegrasi, dimana implementasi firewall yang tepat harus dikonfigurasi untuk memfilter lalu lintas jaringan yang mencurigakan dan membatasi akses yang tidak sah, dikombinasikan dengan penggunaan sistem

deteksi intrusi (IDS) dan sistem pencegahan intrusi (IPS) untuk memantau aktivitas jaringan secara real-time serta mengidentifikasi dan memblokir ancaman potensial, ditambah dengan penerapan enkripsi data yang kuat menggunakan protokol seperti SSL/TLS untuk melindungi informasi sensitif selama transmisi.

Sumber: Hasil Penelitian (2024)

Gambar 7. Diagram Pencegahan Menangani Keamanan Jaringan

Pada Gambar 7 menunjukan hasil kuesioner dengan total 41 responden mengenai kepemilikan tim khusus untuk menangani keamanan jaringan dalam organisasi, data menunjukkan distribusi yang cukup beragam dimana 39% responden (16 organisasi) menyatakan memiliki tim khusus keamanan jaringan yang menunjukkan kesadaran akan pentingnya aspek ini, sementara proporsi terbesar yaitu 34.1% responden (14 organisasi) menyatakan tidak memiliki tim khusus yang dapat mengindikasikan keterbatasan sumber daya atau prioritas yang berbeda dalam pengelolaan keamanan jaringan mereka, dan sisanya sebesar 26.8% responden (11 organisasi) menjawab "Mungkin" yang dapat mengindikasikan bahwa mereka sedang dalam proses pembentukan tim atau memiliki petugas yang menangani keamanan jaringan namun belum dalam bentuk tim yang terstruktur khusus.

Sumber: Hasil Penelitian (2024)

Gambar 8. Diagram Pencegahan Melindungi Keamanan Jaringan

Pada Gambar 8 menunjukan hasil survei dengan 41 responden tentang langkah-langkah perlindungan jaringan yang diterapkan di organisasi, data menunjukkan bahwa enkripsi data merupakan metode yang paling banyak

digunakan dengan persentase 41.5% (17 organisasi), diikuti oleh penggunaan firewall sebesar 39% (16 organisasi), kemudian pelatihan keamanan bagi karyawan sebesar 14.6% (6 organisasi), serta penggunaan VPN dan sistem IDS/IPS dengan persentase yang lebih kecil.

Seiring dengan meningkatnya ketergantungan pada teknologi, ancaman keamanan siber juga semakin kompleks dan beragam.(Hafsah et al., 2024)

Sumber: Hasil Penelitian (2024)

Gambar 9. Grafik Pencegahan Terhadap Organisasi Keamanan Jaringan

Pada Gambar 9 menunjukan hasil survei mengenai frekuensi aktivitas keamanan di organisasi, data menunjukkan dua aspek utama: pembaruan perangkat lunak keamanan dan pelaksanaan audit keamanan, dimana untuk pembaruan perangkat lunak keamanan, sekitar 15 responden melakukannya secara rutin (selalu), 20 responden melakukannya kadang-kadang, dan 5 responden jarang melakukannya, sementara untuk audit keamanan, sekitar 9 responden melakukannya secara rutin (selalu), 25 responden melakukannya kadang-kadang, dan 7 responden jarang melakukannya, yang mengindikasikan bahwa mayoritas organisasi sudah memiliki kesadaran akan pentingnya pembaruan dan audit keamanan meskipun frekuensi pelaksanaannya masih bervariasi dan cenderung tidak konsisten.

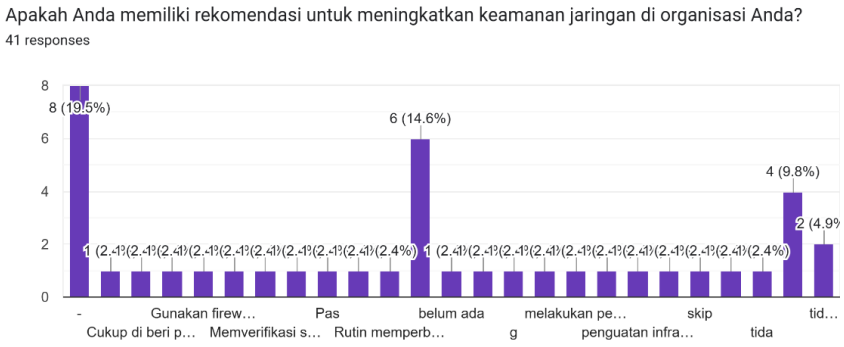
3.3 Tantangan Utama Dalam Menjaga Keamanan Jaringan

Tantangan utama dalam menjaga keamanan jaringan mencakup kompleksitas serangan siber yang terus berkembang dengan teknik yang semakin canggih, dimana para penyerang menggunakan metode seperti ransomware, phishing, dan malware yang terus bermutasi, ditambah dengan keterbatasan sumber daya manusia yang memiliki keahlian khusus di bidang keamanan siber serta kendala anggaran untuk investasi teknologi keamanan terkini.

Sumber: Hasil Penelitian (2024)

Gambar 10. Diagram Tantangan Utama Untuk Menjaga Keamanan Jaringan

Pada Gambar 10 menunjukan hasil survei dari 41 responden mengenai tantangan utama dalam menjaga keamanan jaringan menunjukkan bahwa keterbatasan pengetahuan menjadi kendala terbesar dengan 43.9% (18 responden), diikuti keterbatasan anggaran sebesar 26.8% (11 responden), kurangnya dukungan manajemen sebesar 22% (9 responden), dan teknologi usang sebesar 7.3% (3 responden), yang mengindikasikan bahwa pengembangan kompetensi tim dan alokasi sumber daya masih menjadi isu kritis dalam implementasi keamanan jaringan di berbagai organisasi.



Sumber: Hasil Penelitian (2024)

Gambar 11. Grafik Rekomendasi Untuk Meningkatkan Keamanan Jaringan Di Organisasi

Pada Gambar 11 menunjukan hasil survei dari 41 responden mengenai rekomendasi untuk meningkatkan keamanan jaringan organisasi, terdapat beberapa tanggapan utama dimana 8 responden (19.5%) menyatakan cukup dengan prosedur yang ada, 6 responden (14.6%) mengindikasikan belum memiliki rekomendasi spesifik, dan 4 responden (9.8%) menyarankan untuk melakukan skip atau melewati beberapa prosedur, sementara sisanya memberikan berbagai

rekomendasi seperti penggunaan firewall, verifikasi sistem, pemeliharaan rutin, dan penguatan infrastruktur dengan masing-masing mendapat 1 responden (2.4%), yang menunjukkan bahwa mayoritas organisasi masih perlu mengembangkan strategi yang lebih komprehensif dalam meningkatkan keamanan jaringan mereka.

4. Kesimpulan

Keamanan jaringan menjadi elemen yang sangat penting dalam menghadapi ancaman siber yang semakin kompleks di era digital. Berdasarkan penelitian, pemahaman terhadap konsep keamanan siber dan jaringan di kalangan mahasiswa cukup baik, namun implementasi perlindungan di berbagai organisasi masih menghadapi sejumlah tantangan. Ancaman seperti phishing, malware, dan ransomware terus berkembang, memerlukan pendekatan strategis yang lebih terintegrasi. Hasil survei menunjukkan bahwa penggunaan teknologi seperti enkripsi data, firewall, serta edukasi dan pelatihan keamanan masih menjadi kebutuhan utama untuk mengoptimalkan keamanan jaringan.

Daftar Pustaka

Adawiyyah, R., Fauzi, A., Indriyanah, A., safitri, A., Putri Nabila, E., Maidani, M., & Nurul Izati A, S. (2023). Pengaruh Keamanan Informasi dan Perkembangan Teknologi di Era Revolusi 4.0 Terhadap Kinerja Perusahaan (Literature Review Manajemen Kinerja). *Jurnal Ilmu Multidisplin*, *2*(1), 50–57. https://doi.org/10.38035/jim.v2i1.238

Azzahrah, B. T., Naufal, M., Hamdi, R., Raynee, R., & Layla, Z. (2024). Tantangan Pertahanan dan Keamanan Data Cyber dalam Era Digital : Studi Kasus dan Implementasi. *Jurnal Pendidikan Tambusai*, *8*(2), 23934–23943.

Hafsah, A., Irwan, M., Nasution, P., Ekonomi, F., Bisnis, D., Manajemen, P., Islam, U., & Sumatera, N. (2024). *Issn : 3025-9495*. *10*(9).

Khairunnisa, P. A., Annisa, N., & Parhusip, Y. J. (2024). *Perancangan Sistem Keamanan Jaringan Berbasis Cybersecurity untuk Mitigasi Ancaman Siber pada Infrastruktur TI : Studi Kasus di Indonesia*. *4*, 9–16.

Pengabdian, J., Waradin, M., Sawah, S., Jakarta, K., Khusus, D., & Kota, I. (2024). *Alamat: Jl. Lenteng Agung Raya No.56, RT.1/RW.3, Srengseng Sawah, Jagakarsa, Kota Jakarta Selatan, Daerah Khusus Ibu Kota Jakarta, 12630*. *4*(September).

Putra, J. L., Raharjo, M., & Fitri, E. (2024). *Analisis Ancaman Siber dan Persiapan Pemuda Karang Taruna Kelurahan Rengas dalam Menghadapi Risiko Keamanan Siber*. *6*(02), 151–163.

Rosy, A. F. (2020). Kerjasama Internasional Indonesia: Memperkuat Keamanan Nasional di Bidang Keamanan Siber. *Journal of Government Science (GovSci) : Jurnal Ilmu Pemerintahan*, *1*(2), 118–129. https://doi.org/10.54144/govsci.v1i2.12

Soesanto, E., Romadhon, A., Dwi Mardika, B., & Fahmi Setiawan, M. (2023). Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File. *SAMMAJIVA : Jurnal Penelitian Bisnisdan Manajemen*, *1*(2), 186.

Syaifuddin, F. A., Maulana, D. A., & Amrulloh, M. F. (2024). *Analisis Keamanan Jaringan Menggunakan Firewall untuk Mencegah Serangan Brute Force dan Fraud*. *4*(2), 895–902.

Vimy, T., Wiranto, S., Rudiyanto, R., Widodo, P., & ... (2022). Ancaman Serangan Siber Pada Keamanan Nasional Indonesia. *Jurnal …*, *6*(1), 2319–2327. http://journal.upy.ac.id/index.php/pkn/article/view/2989