Aurelia: Jurnal Penelitian dan Pengabdian Masyarakat Indonesia
E-ISSN: 2964-2493 P-ISSN: 2962-0430
Vol. 4 No. 1 Januari 2025

Strategi Pertahanan Non Konvensional Indonesia dalam Menangkal Ancaman Siber Asimetris: Studi Kasus Serangan terhadap Infrastruktur Kritis

Wiwik Mustikasari[1] Ahmad G Dohamid[2] Fauzia G Cempaka[3]
Program Studi Peperangan Asimetris, Fakultas Strategi Pertahanan, Universitas Pertahanan Republik Indonesia[1,2,3]
Email: wiwik.mustikasari@idu.ac.id[1]

Abstrak

Meningkatnya ancaman siber menjadi tantangan serius di Indonesia terkait perlindungan infrastruktur kritis. Sejak 2020, serangan siber yang terorganisir telah menargetkan sektor-sektor vital seperti lembaga pemerintah dan perbankan, mengakibatkan kerugian finansial dan gangguan layanan publik. Penelitian ini bertujuan untuk menganalisis strategi pertahanan non-konvensional yang diterapkan oleh pemerintah dalam menangkal ancaman ini. Dengan menggunakan teori keamanan siber dan manajemen risiko, penelitian menemukan meskipun kemajuan dalam kebijakan keamanan siber cukup signifikan, tantangan besar tetap ada dalam hal koordinasi antar lembaga dan kesadaran masyarakat. Oleh karena itu, diperlukan pendekatan yang menyeluruh untuk memperkuat pertahanan siber dan melindungi infrastruktur kritis di Indonesia dari serangan yang semakin kompleks. Selain itu, kerjasama antara pemerintah dan sektor swasta sangat penting untuk meningkatkan daya tangkal terhadap ancaman siber, serta membangun sistem keamanan yang lebih tangguh dan responsif.
Kata Kunci: Strategi Pertahanan, Ancaman Siber, Infrastruktur Kritis, Keamanan Siber, Non-Konvensional

Abstract

The increasing cyber threats are a serious challenge in Indonesia related to the protection of critical infrastructure. Since 2020, organized cyber attacks have targeted vital sectors such as government institutions and banking, resulting in financial losses and disruption of public services. This study aims to analyze the unconventional defense strategies implemented by the government in countering these threats. Using cybersecurity and risk management theories, the study found that although progress in cybersecurity policies has been quite significant, major challenges remain in terms of coordination between institutions and public awareness. Therefore, a comprehensive approach is needed to strengthen cyber defense and protect critical infrastructure in Indonesia from increasingly complex attacks. In addition, cooperation between the government and the private sector is essential to increase resilience to cyber threats, as well as build a more resilient and responsive security system.
Keywords: *Defense Strategy, Cyber Threats, Critical Infrastructure, Cybersecurity, Unconventional*

PENDAHULUAN

Ancaman siber telah menjadi isu global yang mempengaruhi stabilitas keamanan berbagai negara, termasuk Indonesia. Serangan terhadap infrastruktur kritis mengakibatkan kerugian besar, baik secara ekonomi maupun sosial. Dalam beberapa tahun terakhir, Indonesia telah menjadi salah satu target serangan siber terbesar di Asia Tenggara, dengan lebih dari 1,2 miliar ancaman siber terdeteksi pada tahun 2023[1]. Pada kuartal pertama tahun 2024, hampir 6 juta ancaman siber dilaporkan terjadi, menunjukkan tingginya risiko yang dihadapi ruang digital di Indonesia (Fadhila Inas Pratiwi et al, 2024). Perlindungan siber di Indonesia semakin mendesak untuk diperkuat, terutama setelah insiden peretasan besar-besaran yang mengakibatkan kebocoran data penting (Unair.ac.id, 2024). Dengan meningkatnya ketergantungan pada teknologi informasi, perlindungan terhadap ancaman ini menjadi

prioritas utama bagi pemerintah dan sektor swasta. Data Badan Siber dan Sandi Negara (BSSN) mencatat bahwa pada tahun 2022 saja, terdapat 370,02 juta serangan siber, dengan sektor administrasi pemerintahan sebagai target utama ((bpptik.kominfo.go.id, 2023).

Hal ini menunjukkan bahwa ancaman siber tidak hanya merusak data dan informasi pribadi tetapi juga dapat menghancurkan aktivitas ekonomi dan bisnis, serta mengganggu stabilitas pertahanan (Dwiyani Permatasari, 2021). Indonesia menghadapi tantangan yang signifikan seiring dengan pertumbuhan jumlah pengguna internet yang mencapai lebih dari 200 juta. Peningkatan ini tidak hanya meningkatkan volume data tetapi juga memperbesar risiko ancaman siber. Berbagai perangkat yang terhubung mulai dari individu hingga sektor publik membuka peluang bagi serangan siber dari banyak sumber, termasuk malware dan ransomware. Selain itu, kemunculan teknologi baru seperti Internet of Things (IoT) dan kecerdasan buatan memperluas kemungkinan vektor serangan. Oleh karena itu, tim CSIRT dan BSSN perlu meningkatkan kecepatan serta kecerdasan dalam mendeteksi dan merespons ancaman demi menjaga integritas sistem siber nasional. (Nikita Dewi Kurnia Salwa, 2024). Tingginya frekuensi serangan, termasuk serangan DDoS, ransomware, dan phishing, menunjukkan bahwa Indonesia kerap menjadi sasaran serangan siber yang merugikan. Oleh karena itu, penting bagi pemerintah dan sektor swasta untuk bekerja sama dalam meningkatkan kesadaran dan kesiapsiagaan terhadap ancaman ini (Topan Yuniarto, 2024).

Serangan siber ke lembaga pemerintah di Indonesia telah menunjukkan dampak yang signifikan dan kompleks. Serangan ransomware yang paling terkenal adalah serangan terhadap Pusat Data Nasional Sementara (PDNS) pada bulan Juni 2024. Serangan ini menggunakan malware Brain Chipper Ransomware dari kelompok Lockbit 3.0, yang mengenkripsi data dan menuntut tebusan sebesar 8 juta dolar AS atau sekitar Rp131 miliar (Melinda Kusuma Ningrum et al, 2024). Serangan ini tidak hanya mempengaruhi PDNS sendiri tapi juga menyebabkan efek domino pada beberapa lembaga publik lainnya. Lebih dari 210 instansi pemerintahan di tingkat pusat dan daerah dipengaruhi, termasuk Arsip Nasional RI, Badan Kepegawaian Negara, Badan Nasional Penanggulangan Bencana, dan lain-lain (Haekal Attar, 2024). Gangguan ini menyebabkan terganggunya layanan keimigrasian, terkurungnya data milik Badan Intelijen Strategis TNI dan POLRI, serta gangguan pada sistem manajemen penyediaan air minum dan pengelolaan keuangan daerah Pemerintah Indonesia saat itu tidak bersedia memenuhi permintaan peretas untuk membayar tebusan. Menteri Komunikasi dan Informatika Budi Arie Setiadi menyatakan bahwa pemerintah akan terus berusaha untuk memulihkan data dan mengatasi gangguan ini (Aryojati Ardipandanto, 2024). Badan Siber dan Sandi Negara (BSSN) sebagai lembaga utama keamanan siber, berfungsi untuk melindungi negara, masyarakat, pemerintah, dan institusi-institusi lain dari serangan siber. berpartisipasi dalam upaya pemulihan dan mitigasi serangan (indonesiabaik.id). Serangan siber ke lembaga pemerintah di Indonesia menunjukkan betapa pentingnya keamanan siber dalam menjaga integritas data dan operasional lembaga-lembaga publik. Dengan meningkatnya frekuensi serangan siber, pemerintah dan BSSN harus terus meningkatkan kesiapsiagaan dan infrastruktur pengamanan untuk mencegah dan mengatasi serangan-serangan tersebut. Oleh karena itu, penting untuk membangun kesadaran akan ancaman ini dan memperkuat pertahanan siber sebagai bagian dari strategi pertahanan nasional. Upaya ini meliputi pengembangan kebijakan pertahanan siber yang komprehensif dan integratif untuk melindungi infrastruktur kritis di Indonesia (Franziska Zeligke et. al, 2024).

Berdasarkan fakta tersebut dapat dianalisis bagaimana serangan siber yang terjadi pada infrastruktur kritis di Indonesia dan dampaknya, dengan fokus utama pada strategi pertahanan non-konvensional dalam menangkal ancaman tersebut. Dengan mempertimbangkan berbagai aspek, termasuk teknologi dan kebijakan, tulisan ini bertujuan untuk memberikan

rekomendasi kepada pemerintah dalam meningkatkan pertahanan siber. Pertanyaan penelitian yang diajukan adalah bagaimana strategi non-konvensional dapat diterapkan Indonesia dalam menghadapi ancaman siber asimetris? dan Bagaimana efektivitas strategi tersebut dalam melindungi infrastruktur kritis dari serangan siber? Ancaman siber dan strategi pertahanan telah menjadi fokus utama dalam beberapa tahun terakhir, mengingat meningkatnya frekuensi dan kompleksitas serangan yang dihadapi oleh berbagai negara, termasuk Indonesia. Berbagai studi telah dilakukan untuk menganalisis dampak serangan siber serta untuk mengembangkan strategi mitigasi yang efektif. Menurut Dwiyani serangan siber tidak hanya merusak data tetapi juga dapat menghancurkan aktivitas ekonomi dan bisnis. Tim CSIRT dan BSSN di Indonesia menghadapi berbagai tantangan signifikan yang perlu segera diatasi untuk memperkuat pertahanan siber negara. Dari tingginya frekuensi serangan siber, kurangnya kesadaran keamanan siber, keterbatasan sumber daya, hingga kekurangan tenaga ahli yang terlatih, semuanya memerlukan perhatian serius.Koordinasi antara lembaga-lembaga terkait, peningkatan kesadaran di kalangan masyarakat dan sektor bisnis, serta investasi dalam teknologi dan pelatihan SDM menjadi kunci dalam mengatasi tantangan ini dan membangun sistem pertahanan siber yang lebih baik untuk masa depan.

Hal tersebut disampaikan Nikita dengan menekankan pentingnya peningkatan kecepatan deteksi dan respons dalam menghadapi ancaman siber yang terus berkembang. Laporan dari Badan Siber dan Sandi Negara sektor administrasi pemerintahan menjadi target utama dengan lebih dari 370 juta serangan pada tahun 2022. Hasil Analisa mengungkapkan dampak signifikan dari serangan ransomware terhadap infrastruktur kritis, termasuk gangguan layanan publik. Secara keseluruhan, penelitian-penelitian terdahulu menunjukkan bahwa ancaman siber memiliki dampak yang luas dan kompleks terhadap berbagai sektor, terutama sektor publik. Selain itu, kolaborasi antara pemerintah dan sektor swasta penting untuk meningkatkan kesiapsiagaan dan respons terhadap serangan siber serta pengembangan kebijakan yang terintegrasi dan berkelanjutan menjadi kunci untuk memperkuat pertahanan siber nasional di Indonesia.

METODE PENELITIAN

Metode penelitian yang digunakan adalah deskriptif kualitatif, yang bertujuan untuk menggambarkan dan menganalisis fenomena ancaman siber terhadap infrastruktur kritis di Indonesia. Melalui pendekatan ini, peneliti mengumpulkan data dari berbagai sumber, artikel ilmiah, dan wawancara untuk mendapatkan pemahaman yang mendalam tentang karakteristik dan dampak serangan siber. Data dikumpulkan melalui kajian literatur yang mencakup studi-studi sebelumnya mengenai serangan siber di Indonesia, serta analisis data statistik dari Badan Siber dan Sandi Negara (BSSN) terkait frekuensi dan jenis serangan yang terjadi. Selain itu, wawancara dilakukan untuk mendapatkan perspektif langsung mengenai tantangan yang dihadapi dalam melindungi infrastruktur kritis. Setelah data terkumpul, analisis dilakukan dengan cara mengidentifikasi pola-pola yang muncul dari data tersebut dengan mengevaluasi bagaimana serangan siber mempengaruhi berbagai sektor, terutama sektor publik, serta menilai efektivitas strategi pertahanan yang ada. Pendekatan ini memungkinkan peneliti untuk memahami kompleksitas ancaman siber dan merumuskan rekomendasi yang relevan bagi pemerintah dan sektor swasta.

HASIL PENELITIAN DAN PEMBAHASAN

Indonesia mengalami lebih dari 1,2 miliar ancaman siber pada tahun 2023. Pada kuartal pertama tahun 2024, hampir 6 juta serangan dilaporkan, menunjukkan bahwa ancaman siber terus meningkat seiring dengan pertumbuhan pengguna internet yang mencapai lebih dari 221

juta orang (Mohamad Mamduh, 2024). Sebagian besar serangan siber yang terjadi di Indonesia berasal dari wilayah domestik.. Jakarta dan daerah penyangga merupakan daerah yang konsisten dengan sumbangsih serangan siber tertinggi. Sebagai pusat bisnis, industri, dan tempat kompilasi big data dari seluruh Indonesia, Jakarta menjadi sentra serangan di dalam negeri karena didukung infrastruktur digital yang lengkap, demikian pula daerah satelit penyangga Jakarta. Jumlah serangan siber di Indonesia meningkat drastis, mencapai lebih dari 2,4 miliar selama semester pertama tahun 2024, yang berarti rata-rata hampir 13,7 juta serangan per hari atau sekitar 158 serangan per detik. Di Jakarta juga ditemukan menjadi objek serangan siber dari tahun ke tahun, karena pusat ekonomi, bisnis, dan sentral data penting terjadi di sana (Kumparan.tech, 2024).

Pada tanggal 20 Juni 2024, Pusat Data Nasional (PDN) Indonesia mengalami serangan siber yang parah menggunakan teknik ransomware, yang mengakibatkan data milik kementerian, lembaga, dan pemerintah daerah terkunci oleh peretas. Serangan ini mengganggu sejumlah layanan publik krusial, menimbulkan kekhawatiran serius mengenai keamanan data pemerintah. Tim dari Kementerian Komunikasi dan Informatika (Kemenkominfo), Badan Siber dan Sandi Negara (BSSN), Polri, dan Telkom sebagai pengelola PDN berupaya keras untuk memulihkan data yang terenkripsi, namun upaya tersebut gagal. Herlan Wijanarko, Direktur Network dan IT Solution Telkom, menyatakan bahwa data yang terkena ransomware tidak dapat dipulihkan dan tetap berada di server PDN. Peretas menuntut tebusan sebesar 8 juta dolar AS (sekitar Rp 131 miliar) untuk membuka kembali akses ke data tersebut, tetapi pemerintah Indonesia menolak untuk membayar, dengan alasan bahwa pembayaran tidak menjamin pemulihan data dan dapat berisiko lebih lanjut. Usman Kansong dari Kemenkominfo mengonfirmasi bahwa server PDN telah diisolasi untuk mencegah akses lebih lanjut dari peretas. Meskipun beberapa layanan publik telah berhasil dipulihkan, seperti layanan keimigrasian dan sistem informasi kinerja penyedia, masih banyak layanan lain yang belum beroperasi sepenuhnya. Serangan ini menunjukkan kerentanan infrastruktur siber pemerintah Indonesia dan menekankan perlunya peningkatan keamanan siber di semua tingkatan pemerintahan (Rita Puspitasari, 2024).

Serangan siber ransomware yang dikenal sebagai Brain Cipher, yang berdampak signifikan terhadap layanan publik di seluruh negeri, termasuk layanan keimigrasian yang terpaksa pindah ke Amazon Web Services untuk tetap beroperasi. Selain itu, layanan Kementerian Pendidikan dan Kebudayaan juga mengalami kendala, termasuk sistem pengadaan dan beasiswa pendidikan. Menteri Komunikasi dan Informatika, Budi Arie Setiadi, menyatakan bahwa dampak dari serangan ini berada pada level kritikal dan mayor, dengan gangguan total atau parsial pada fungsi utama layanan. Meskipun probabilitas kebocoran data relatif rendah karena perlindungan sistem VMware, gangguan operasional yang ditimbulkan sangat signifikan. Insiden ini menyoroti perlunya perhatian lebih terhadap keamanan siber di seluruh sektor pemerintahan dan mendorong peningkatan investasi dalam teknologi keamanan serta pelatihan staf untuk mencegah serangan serupa di masa mendatang (Andika Dwi, 2024).

Serangan DDoS kini semakin menjadi perbincangan hangat di kalangan publik dan media, terutama setelah insiden terbaru yang melibatkan platform X, yang mengalami serangan DDoS bersamaan dengan wawancara antara Donald Trump dan Elon Musk. Kejadian ini menyoroti betapa rentannya infrastruktur digital kita ketika dua tokoh besar berbicara di tempat yang sama, memicu kekhawatiran tentang keamanan komunikasi digital di era modern. Selain itu, serangan DDoS telah mengancam banyak perusahaan sepanjang tahun 2024, menciptakan ketidakpastian dalam dunia usaha yang semakin bergantung pada teknologi. Laporan dari Radar Gcore menunjukkan peningkatan signifikan dalam frekuensi serangan ini, dengan jumlah

serangan meningkat hampir 46% pada paruh pertama tahun 2024 dibandingkan periode yang sama tahun sebelumnya. Pada kuartal kedua 2024, tercatat 445.000 insiden serangan DDoS, meningkat sekitar 34% dari enam bulan sebelumnya. Tidak hanya jumlah serangan yang meningkat, tetapi juga tingkat keparahannya, dengan banyak serangan dirancang untuk mengeksploitasi kelemahan tertentu dalam sistem. Gcore melaporkan bahwa serangan terkuat mencapai 1,7 Tbps, sedikit lebih tinggi dibandingkan tahun 2023. Sektor industri game dan perjudian menjadi yang paling terpukul oleh serangan ini, sementara sektor teknologi dan layanan keuangan juga mencatatkan lonjakan serangan yang signifikan. Dalam konteks ini, penting bagi organisasi untuk mengembangkan rencana komprehensif yang mencakup deteksi dan respons cepat terhadap ancaman DDoS yang terus berkembang (Bahtiar Nur Faizi, 2024).

Indonesia, seperti negara lainnya, bergantung pada teknologi informasi dan digital, menjadikan perlindungan terhadap ancaman keamanan siber sebagai prioritas utama. Dalam era digital, kejahatan siber atau cybercrime tidak hanya berpotensi merusak data dan informasi pribadi, tetapi juga dapat menghancurkan aktivitas ekonomi, infrastruktur, dan stabilitas keamanan nasional. Cybercrime meliputi berbagai jenis serangan siber, termasuk phishing, yang berusaha mendapatkan informasi pribadi seperti kata sandi dan nomor kartu kredit; ransomware, yang mengenkripsi data dan meminta tebusan untuk pemulihan; serta malware, perangkat lunak berbahaya yang merusak sistem dan mencuri data. Selain itu, serangan DDoS membanjiri server dengan lalu lintas palsu, membuatnya tidak tersedia bagi pengguna yang sah. Serangan Man in the Middle (MITM) mencegat komunikasi antara dua pihak untuk mencuri informasi yang ditransmisikan, sementara serangan Zero-Day mengeksploitasi kerentanan perangkat lunak yang belum terdeteksi. Data dari Badan Siber dan Sandi Negara (BSSN) menunjukkan bahwa pada tahun 2022 terjadi 370,02 juta serangan siber di Indonesia, meningkat 38,72% dibandingkan tahun sebelumnya. Sektor administrasi pemerintahan menjadi target utama dengan 284,09 juta serangan. Untuk melindungi sistem komputer dari serangan digital atau akses ilegal, pemerintah Indonesia telah mengeluarkan peraturan seperti Undang-Undang Informasi Transaksi Elektronik (UU ITE), yang bertujuan untuk melindungi masyarakat di dunia digital dan menetapkan aturan bagi aktivitas di ruang siber (BPPTIK.kominfo.go.id)

Indonesia, sebagai salah satu negara dengan ekonomi terbesar di Asia Tenggara, menghadapi tantangan besar dalam mengelola keamanan siber, yang semakin mendesak mengingat tingginya frekuensi serangan, kurangnya kesadaran masyarakat dan sektor bisnis, keterbatasan sumber daya, serta munculnya ancaman baru. Jumlah pengguna internet yang terus berkembang pesat, mencapai lebih dari 221 juta pada tahun 2024, menambah kompleksitas pengawasan dan perlindungan terhadap infrastruktur kritis, sementara serangan siber seperti DDoS dan ransomware semakin meningkat. Kesadaran terhadap pentingnya keamanan siber masih rendah, dengan survei menunjukkan bahwa sebagian besar masyarakat tidak menyadari mereka mungkin telah menjadi korban peretasan. Selain itu, tim CSIRT dan BSSN dihadapkan pada keterbatasan anggaran dan kekurangan tenaga ahli yang terampil dalam bidang keamanan siber, serta kurangnya koordinasi antar lembaga yang memperlambat respons terhadap serangan. Perkembangan teknologi baru seperti AI dan IoT juga membawa tantangan tambahan, memperbesar permukaan serangan dan memerlukan pendekatan keamanan yang lebih canggih. Infrastruktur kritis di Indonesia masih rentan karena kurangnya investasi dalam sistem keamanan yang memadai, menjadikannya sasaran empuk bagi pelaku kejahatan siber (Nikita Dewi, 2024).

Indonesia saat ini menghadapi krisis serius dalam keamanan siber, dengan lebih dari 400.000 serangan siber baru terjadi setiap hari, termasuk 97.226 serangan ransomware yang terdeteksi pada tahun 2023, menunjukkan peningkatan dramatis dalam aktivitas siber

berbahaya. Serangan ransomware, yang mengenkripsi data dan meminta tebusan untuk pemulihannya, menjadi salah satu ancaman paling signifikan di negara ini, dengan teknologi yang semakin canggih dan sulit dideteksi. Dony Koesmandarin dari Kaspersky menyatakan bahwa transformasi digital yang pesat membuka peluang bagi pelaku industri dan penjahat siber untuk mengeksploitasi kelemahan sistem. Selain ransomware, serangan phishing finansial mencapai 97.465 kasus, dan insiden lokal dengan berbagai jenis malware mencatatkan angka sangat tinggi, yaitu 16,4 juta. Tingginya jumlah serangan ini disebabkan oleh perubahan lanskap ancaman yang cepat, kesenjangan dalam alat pemantauan keamanan, dan kurangnya keterampilan staf keamanan siber. Untuk menghadapi ancaman ini, penting bagi organisasi dan individu untuk meningkatkan kesadaran serta langkah-langkah keamanan siber mereka melalui pendidikan dan pelatihan yang lebih baik, penerapan perangkat lunak keamanan terbaru, serta kolaborasi antara pemerintah, sektor swasta, dan masyarakat. Keamanan siber memerlukan usaha bersama dari seluruh lapisan masyarakat untuk menjaga keamanan informasi di tengah meningkatnya frekuensi dan kompleksitas serangan (Pabila Syaftahan, 2024).

Seiring dengan pesatnya digitalisasi, ancaman siber menjadi isu krusial yang harus dihadapi oleh perusahaan di seluruh dunia, termasuk Indonesia, yang diprediksi akan mengalami peningkatan intensitas dan kompleksitas serangan siber pada tahun 2025. Saat ini, Indonesia menjadi salah satu target serangan siber di Asia Tenggara, meliputi malware, ransomware, dan serangan phishing. Namun, hanya 39% organisasi di Indonesia yang siap menghadapi risiko keamanan siber modern, meskipun angka ini lebih tinggi dibandingkan rata-rata global. Demikian pula dengan sektor keuangan, manufaktur, dan kesehatan yang merupakan tulang punggung ekonomi juga menjadi target utama serangan siber. Di sektor keuangan, meskipun ada regulasi dari Bank Indonesia dan OJK untuk meningkatkan keamanan, implementasinya masih bervariasi. Sektor manufaktur menghadapi risiko akibat transformasi digital yang membuka celah bagi peretas, sementara sektor kesehatan semakin rentan dengan digitalisasi rekam medis yang dapat membahayakan data pasien. Kesiapan perusahaan-perusahaan di Indonesia untuk menghadapi tantangan ini masih terhambat oleh kurangnya kesadaran di tingkat manajemen dan keterbatasan sumber daya dalam hal anggaran dan tenaga ahli. Untuk itu, kerjasama antara pemerintah, sektor swasta, dan masyarakat sangat diperlukan guna menciptakan strategi efektif dalam mengatasi ancaman siber yang semakin kompleks dan terorganisir (Rita Puspitasari, 2024).

Tahun 2025 diprediksi akan menjadi tahun yang penuh tantangan bagi dunia siber, demikian pula dengan Indonesia, di mana ancaman siber semakin meningkat seiring dengan kemajuan teknologi, termasuk penggunaan Artificial Intelligence (AI). Alex Budiyanto, Founder Indonesia Cyber Security Hub, mengungkapkan bahwa Indonesia menghadapi risiko serius akibat lemahnya regulasi dan minimnya kesadaran keamanan siber di berbagai lini. Meskipun sudah ada beberapa regulasi seperti Undang-Undang Perlindungan Data Pribadi, Rancangan Undang-Undang Keamanan Siber masih terhambat di DPR dan belum menunjukkan perkembangan yang signifikan. Selain itu, pentingnya meningkatkan kesadaran keamanan siber di kalangan top manajemen juga ditekankan, karena kurangnya pemahaman terhadap risiko siber sering kali mengakibatkan investasi keamanan yang dianggap tidak mendesak. Alex menyoroti bahwa pelatihan cyber security awareness harus diberikan kepada seluruh karyawan untuk menjadikan mereka garis pertahanan pertama dalam menghadapi serangan. Ancaman phishing berbasis AI menjadi semakin berbahaya, dengan penyerang mampu menciptakan pesan yang tampak otentik dan sulit dikenali sebagai ancaman. Oleh karena itu, literasi keamanan di semua level organisasi sangat penting untuk melindungi data dan sistem dari serangan yang semakin canggih (Rita Puspitasari, 2024).

KESIMPULAN

Indonesia mengalami lonjakan signifikan dalam serangan siber, dengan lebih dari 1,2 miliar ancaman terdeteksi pada tahun 2023 dan hampir 6 juta serangan pada kuartal pertama tahun 2024. Sektor administrasi pemerintahan menjadi target utama, dengan 370 juta serangan pada tahun 2022. Lonjakan ini mencerminkan meningkatnya ketergantungan pada teknologi informasi dan digital, yang berpotensi merusak data, infrastruktur, dan stabilitas keamanan nasional. Serangan siber di Indonesia mencakup berbagai jenis, termasuk ransomware, DDoS, dan phishing, yang menunjukkan kompleksitas ancaman yang dihadapi. Serangan ransomware terhadap Pusat Data Nasional pada Juni 2024 adalah contoh nyata dampak serius dari ancaman ini, mengganggu layanan publik dan menyebabkan kerugian besar. Dengan lebih dari 221 juta pengguna internet di Indonesia, tantangan pengelolaan keamanan siber semakin mendesak. Selama serangan ransomware di PDN, berbagai institusi pemerintah terpengaruh, termasuk layanan imigrasi yang mengalami keterlambatan parah akibat downtime sistem. Hal ini menyebabkan proses pengeluaran visa, paspor, dan izin tinggal terhambat, bahkan harus kembali menggunakan sistem manual untuk sementara waktu. Gangguan yang disebabkan oleh serangan ransomware ini mengakibatkan penurunan produktivitas di berbagai lembaga pemerintah. Insiden ini dapat mengurangi kepercayaan publik terhadap kemampuan pemerintah dalam melindungi data dan menjaga sistem yang andal, yang berpotensi merusak reputasi. Kerugian ekonomi sekitar 29% perusahaan yang terkena serangan serupa mengalami penurunan pendapatan yang signifikan akibat biaya pemulihan dan kehilangan peluang bisnis.

Investasi dalam keamanan siber menjadi sangat penting bagi perusahaan, dan salah satu cara efektif untuk melindungi diri dari serangan siber adalah melalui penetration testing. Penetration testing melibatkan simulasi serangan oleh tim keamanan untuk mengidentifikasi celah keamanan yang dapat dieksploitasi oleh penyerang. Dengan melaksanakan pentest, perusahaan dapat menilai keefektifan sistem keamanan mereka, mengidentifikasi dan mengatasi kerentanan potensial, serta meningkatkan ketahanan terhadap ancaman siber. Untuk meningkatkan keamanan siber di Indonesia, langkah-langkah konkret perlu diambil, termasuk meningkatkan pendidikan dan pelatihan untuk menciptakan sumber daya manusia yang kompeten di bidang keamanan siber, memperkuat kebijakan dan regulasi terkait keamanan siber, serta meningkatkan investasi dalam teknologi dan infrastruktur keamanan. Selain itu, kolaborasi antara pemerintah dan sektor swasta sangat penting untuk membangun sistem yang lebih aman dan responsif terhadap ancaman siber yang terus berkembang. Masyarakat juga perlu diberikan edukasi mengenai pentingnya keamanan siber agar lebih sadar akan risiko yang ada. Dengan upaya bersama ini, Indonesia dapat memperkuat pertahanan sibernya dan melindungi data serta informasi penting dari ancaman yang semakin kompleks (Ria Puspita Sari, 2024).

DAFTAR PUSTAKA

Andika Dwi (2024). 6 Dampak Serangan Ransomware ke Server PDNS. https://www.tempo.co/digital/6-dampak-serangan-ransomware-ke-server-pdns-44346

Aryojati Ardipandanto (2024). Lemahnya Pengamanan Pusat Data Nasional Sementara Terhadap Serangan Siber. Kajian Singkat Terhadap Isu Aktual Dan Strategis. Vol. XVI, No. 13/I/Pusaka/Juli/2024

Dwiyani Permatasari (2021), Tantangan Cyber Security di Era Revolusi Industri 4.0 https://www.djkn.kemenkeu.go.id/kanwil-sulseltrabar/baca-artikel/14190/tantangan-cyber-security-di-era-reavolusi-industri-40.html

Franziska Zeligke et. al (2024). Kebijakan Pertahanan Untuk Mencapai Sistem Keamanan Nasional. Jurnal Kebijakan Stratejik Keamanan Nasional. Volume 7 Number 1. https://scholarhub.ui.ac.id/jksknHaekal Attar (2024). Ini Daftar Lembaga Negara yang Terkena Dampak dari Serangan Ransomware. https://www.nu.or.id/nasional/ini-daftar-lembaga-negara-yang-terkena-dampak-dari-serangan-
https://bpptik.kominfo.go.id/Publikasi/detail/jenis-jenis-serangan-siber-di-era-digital
https://indonesiabaik.id/infografis/bssn-lindungi-indonesia-dari-serangan-siber
https://kumparan.com/kumparantech/serangan-siber-ke-ri-naik-6-kali-lipat-pada-h1-2024-mayoritas-dari-dalam-negeri-23PnYQpafrf
https://widyasecurity.com/2024/02/05/investasi-cyber-security-untuk-keamanan-terbaik-bagi-perusahaan-di-tahun-2024/
https://www.cnnindonesia.com/teknologi/20240603103200-185-1105033/indonesia-digempur-6-juta-ancaman-siber-di-awal-2024-cek-modusnya
Melinda Kusuma Ningrum, Michelle Gabriela, Andika Dwi (2024). Daftar Lengkap Lembaga Negara yang Terdampak Serangan Ransomware. https://www.tempo.co/politik/daftar-lengkap-lembaga-negara-yang-terdampak-serangan-ransomware-45424
Mohamad Mamduh (2024). Q3 2024: Lonjakan 75% dalam Serangan Siber di Seluruh Dunia. https://www.medcom.id/teknologi/news-teknologi/VNxlqVgN-q3-2024-lonjakan-75-dalam-serangan-siber-di-seluruh-dunia
Muhamad Bahtiar Nur Faizi (2024). Serangan DDoS Meningkat, Industri Game dan Judi Tetap Jadi Target. https://cyberhub.id/berita/serangan-ddos-meningkat
Nikita Dewi Kurnia Salwa, 2024. Tantangan & Hambatan Besar yang Dihadapi CSIRT-BSSN Indonesia. https://csirt.or.id/pengetahuan-dasar/tantangan-csirt-bssn
Nikita Dewi Kurnia Salwa, 2024. Willow: Tonggak Sejarah Baru dalam Quantum Computing. https://csirt.or.id/berita/willow-quantum-computing
Pabila Syaftahan (2024). Ratusan Ribu Serangan Siber Baru Terjadi Setiap Hari di Indonesia. https://cyberhub.id/berita/serangan-siber-di-indonesia#google_vignette
Pratiwi, F. I., Hennida, C., Soesilowati, S., Berliantin, N., Ekasari, D. Y., Dewi, C. S., & Intan, A. A. (2024). Cybersecurity Challenges in Indonesia: Threat and Responses Analysis. Perspectives on Global Development and Technology, 22(3-4), 239-264. https://doi.org/10.1163/15691497-12341660.
Rita Puspita Sari (2024). PDN diserang Hacker, Seberapa Lemah Keamanan Siber Indonesia? https://www.cloudcomputing.id/berita/keamanan-siber-indonesia
Rita Puspita Sari (2024). Pemerintah Pasrah Kehilangan Data Berharga Akibat Serangan Siber. https://www.cloudcomputing.id/berita/pemerintah-kehilangan-data
Rita Puspita sari (2024). Siapkah Perusahaan Indonesia Hadapi Ancaman Siber 2025? https://www.cloudcomputing.id/berita/siapkah-indonesia-hadapi-siber-2025
Rita Puspitasari (2024). Ancaman Siber 2025: Pemerintah Didesak Percepat Regulasi. https://csirt.or.id/berita/pemerintah-didesak-percepat-regulasi
Topan Yuniarto (2024). Tantangan Keamanan Siber Indonesia: Ancaman dan Dampaknya. https://kompaspedia.kompas.id/baca/paparan-topik/tantangan-keamanan-siber-indonesia-ancaman-dan-dampaknya