BUSINESS: Scientific Journal of Business and Entrepreneurship
e-ISSN: 3025-2571, Volume 3 Number 2 (2025)
https://journal.csspublishing.com/index.php/business

Analisis Pelanggaran Keamanan Siber pada Bisnis Menggunakan Metode Digital Forensik

Ahmad Albar[1], Tata Sutabri [2]
Universitas Bina Darma [1,2]
e-mail: ahmadalbar29922@gmail.com

Abstract
The rapid advancement of information technology has significantly accelerated the growth of online businesses; however, it has concurrently increased the risks associated with cybersecurity. Online enterprises face serious challenges from threats such as customer data theft, unauthorized access to transaction systems, phishing attacks, and the misuse or manipulation of digital information. This study aims to conduct a comprehensive analysis of cybersecurity breach incidents in online business environments by employing digital forensic methods as the primary approach for the identification, collection, and analysis of digital evidence. The investigative process follows a systematic procedure, including stages of identification, preservation, collection, analysis, and presentation of evidence, in accordance with established principles of digital forensics. The findings demonstrate that the application of digital forensic techniques is highly effective in revealing attack patterns, tracing the sources of cyber threats, detecting vulnerabilities, and ensuring the integrity and confidentiality of transaction data and customer information. These results provide a valuable foundation for developing robust strategies to respond to cybersecurity incidents, enhance preventive measures, and strengthen overall information security systems in online business operations.
Keywords: *Cybersecurity, Digital Forensics, Online Business, Incident Analysis.*

Abstrak
Perkembangan pesat teknologi informasi telah secara signifikan mempercepat pertumbuhan bisnis online; namun, hal ini juga secara bersamaan meningkatkan risiko yang terkait dengan keamanan siber. Perusahaan daring menghadapi tantangan serius dari berbagai ancaman, seperti pencurian data pelanggan, akses tidak sah ke sistem transaksi, serangan phishing, serta penyalahgunaan atau manipulasi informasi digital. Penelitian ini bertujuan untuk melakukan analisis komprehensif terhadap insiden pelanggaran keamanan siber dalam lingkungan bisnis online dengan memanfaatkan metode forensik digital sebagai pendekatan utama dalam identifikasi, pengumpulan, dan analisis bukti digital. Proses investigasi mengikuti prosedur sistematis yang mencakup tahapan identifikasi, preservasi, pengumpulan, analisis, dan penyajian bukti, sesuai dengan prinsip-prinsip forensik digital yang telah ditetapkan. Hasil penelitian menunjukkan bahwa penerapan teknik forensik digital sangat efektif dalam mengungkap pola serangan, melacak sumber ancaman siber, mendeteksi kerentanan, serta memastikan integritas dan kerahasiaan data transaksi dan informasi pelanggan. Temuan ini memberikan dasar yang berharga untuk pengembangan strategi yang kuat dalam merespons insiden keamanan siber, meningkatkan langkah-langkah pencegahan, dan memperkuat sistem keamanan informasi secara keseluruhan dalam operasional bisnis online.
Kata Kunci: Keamanan Siber, Digital Forensik, Bisnis Online, Analisis Insiden.

PENDAHULUAN

Dalam dua dekade terakhir ini perkembangan teknologi informasi dan komunikasi yang pesat telah mendorong pertumbuhan bisnis online secara signifikan. Hampir semua aspek operasional perusahaan e-commerce dan platform digital kini sangat bergantung pada sistem digital dan jaringan internet (Laudon & Traver, 2020). Transformasi digital ini menghadirkan berbagai kemudahan, seperti pengelolaan data pelanggan yang lebih efisien, percepatan proses transaksi, serta peningkatan produktivitas dan kualitas layanan. Namun, di balik berbagai keuntungan tersebut, muncul risiko serius berupa ancaman terhadap keamanan siber yang berpotensi menimbulkan kerugian material maupun non-material bagi perusahaan dan pelanggan (Von Solms & Van Niekerk, 2013).

Keamanan siber menjadi isu krusial bagi perusahaan bisnis online mengingat tingginya ketergantungan pada sistem digital. Ancaman dapat muncul dalam berbagai bentuk, termasuk pencurian data pelanggan, peretasan sistem transaksi, penyebaran malware, serangan ransomware, phishing, hingga manipulasi data atau sabotase sistem kritis (Kshetri, 2017). Dampak dari serangan siber ini tidak hanya mengganggu kelancaran operasional, tetapi juga dapat merusak reputasi perusahaan dan mengancam kerahasiaan serta integritas data transaksi dan informasi pelanggan. Berdasarkan berbagai laporan global, tren insiden siber menunjukkan peningkatan dari tahun ke tahun, baik dari segi frekuensi serangan, kompleksitas teknik yang digunakan, maupun kerugian finansial yang ditimbulkan (ENISA, 2022). Hal ini menekankan perlunya penerapan strategi sistematis untuk mendeteksi, menganalisis, dan menanggulangi insiden siber secara efektif.

Digital forensik memegang peranan yang sangat penting. Digital forensik adalah cabang ilmu yang berfokus pada identifikasi, pengumpulan, analisis, dan penyajian bukti digital yang dapat digunakan untuk mengungkap pelanggaran keamanan siber (Casey, 2011). Perusahaan dapat menelusuri jejak aktivitas pelaku, mengidentifikasi sumber serangan, serta memastikan keabsahan bukti digital untuk dapat dipertanggungjawabkan secara hukum. Digital forensik tidak hanya berfungsi sebagai alat investigasi teknis, tetapi juga menjadi penghubung antara aspek teknologi dan regulasi hukum dalam penanganan insiden siber.

Penelitian ini bertujuan untuk menganalisis pelanggaran keamanan siber dalam lingkungan bisnis online dengan menggunakan metode digital forensik sebagai pendekatan utama dalam investigasi. Penekanan penelitian terletak pada penerapan tahapan forensik digital, yaitu identifikasi, preservasi, pengumpulan, analisis, dan penyajian bukti. Diharapkan dapat diperoleh pemahaman yang lebih mendalam mengenai mekanisme terjadinya pelanggaran siber, pola serangan, serta strategi mitigasi yang efektif (Raghavan

& Parthasarathy, 2019). Penelitian ini juga bertujuan untuk menunjukkan bagaimana hasil investigasi digital forensik dapat menjadi dasar bagi pengembangan sistem keamanan informasi dan penyusunan kebijakan mitigasi risiko siber pada perusahaan bisnis online. Penelitian ini diharapkan memberikan kontribusi signifikan dalam bidang keamanan siber, baik dari perspektif akademik maupun praktis. Temuan penelitian dapat menambah literatur terkait penerapan metode digital forensik dalam analisis pelanggaran siber. Penelitian ini dapat menjadi acuan bagi perusahaan dalam menyusun prosedur tanggap insiden (incident response) yang lebih efektif, memperkuat sistem pertahanan siber, serta meningkatkan kepercayaan pelanggan terhadap keamanan transaksi dan data digital.

TINJAUAN LITERATUR

Perkembangan pesat bisnis online telah mendorong penggunaan teknologi digital dalam operasional sehari-hari. Ancaman terhadap keamanan siber meningkat, mencakup pencurian data pelanggan, peretasan sistem transaksi, malware, ransomware, dan phishing (Kshetri, 2017). Ancaman ini bukan hanya menimbulkan kerugian finansial, tetapi juga dapat merusak reputasi perusahaan dan menurunkan kepercayaan pelanggan (Von Solms & Van Niekerk, 2013). Beberapa penelitian menekankan bahwa keamanan siber harus menjadi bagian integral dari strategi bisnis online. Menurut Laudon & Traver (2020), perusahaan e-commerce perlu mengimplementasikan kontrol keamanan yang komprehensif, termasuk enkripsi data, sistem autentikasi yang kuat, serta monitoring transaksi real-time. Kontrol ini tidak hanya berfungsi sebagai pencegahan, tetapi juga sebagai alat deteksi dini serangan siber.

Menurut (Casey, 2011), menjelaskan bahwa digital forensik adalah disiplin ilmu yang menggabungkan prosedur teknis dan hukum untuk mengidentifikasi, mengamankan, menganalisis, dan menyajikan bukti digital. Proses ini biasanya mengikuti tahapan identifikasi, preservasi, pengumpulan, analisis, dan penyajian bukti. Raghavan & Parthasarathy (2019) menambahkan bahwa metode digital forensik efektif dalam melacak asal serangan, mengidentifikasi pola aktivitas pelaku, serta memastikan integritas dan validitas bukti yang dikumpulkan. Penelitian terbaru juga menyoroti pentingnya integrasi digital forensik dengan strategi mitigasi risiko dan manajemen keamanan informasi. Kumar et al. (2021) menunjukkan bahwa perusahaan yang menggunakan pendekatan forensik secara proaktif mampu mendeteksi kelemahan sistem sebelum terjadi insiden besar, meningkatkan kemampuan respons terhadap serangan, serta meminimalkan kerugian operasional. Integrasi digital forensik dengan sistem keamanan siber berbasis AI dan machine learning diyakini dapat mempercepat analisis bukti dan mendeteksi anomali yang tidak teridentifikasi oleh metode tradisional (ENISA, 2022). Tantangan dalam penerapan digital forensik juga perlu diperhatikan. Beberapa studi menunjukkan bahwa kompleksitas infrastruktur TI, resistensi karyawan

terhadap perubahan digital, dan kurangnya standar prosedur internal dapat menghambat efektivitas investigasi forensik (Kshetri, 2017; Von Solms & Van Niekerk, 2013). Berdasarkan kajian literatur ini, dapat disimpulkan bahwa digital forensik memiliki peranan strategis dalam keamanan bisnis online, baik sebagai alat investigasi teknis maupun sebagai dasar pengembangan kebijakan mitigasi risiko siber. Integrasi antara kontrol keamanan, proses digital forensik, dan pelatihan SDM menjadi kombinasi yang esensial untuk meningkatkan ketahanan perusahaan terhadap ancaman siber.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan metode studi kasus untuk memahami secara mendalam proses analisis pelanggaran keamanan siber dalam bisnis online melalui metode digital forensik. Fokus penelitian terletak pada pengumpulan, analisis, dan interpretasi bukti digital untuk mengidentifikasi penyebab dan pelaku insiden siber. Objek penelitian berupa kasus pelanggaran keamanan siber yang umum terjadi di lingkungan bisnis online, seperti pencurian data pelanggan, modifikasi file sistem, dan pemasangan malware. Penelitian dilakukan secara simulatif di laboratorium digital forensik untuk menjaga keamanan data dan mematuhi etika penelitian, dengan skenario yang meniru kejadian nyata di dunia siber. Data penelitian mencakup data primer, yaitu artefak digital, log sistem, file jaringan, dan bukti digital dari simulasi insiden, serta data sekunder berupa literatur ilmiah, jurnal, buku, dan laporan terkait keamanan siber, digital forensik, dan insiden pelanggaran data dalam bisnis online.

HASIL DAN PEMBAHASAN

Karakteristik Pelanggaran Keamanan Siber

Hasil penelitian menunjukkan bahwa pelanggaran keamanan siber di bisnis online memiliki beberapa karakteristik yang saling terkait. Pertama, akses tidak sah ke sistem target umumnya terjadi melalui pemanfaatan kredensial lemah, penggunaan kata sandi default, atau eksploitasi kerentanan jaringan yang belum diperbarui. Hal ini memungkinkan pelaku untuk menembus pertahanan awal tanpa terdeteksi. Kedua, setelah berhasil masuk, pelaku melakukan pergerakan lateral untuk memperluas kontrolnya dalam sistem. Aktivitas ini memungkinkan mereka untuk mengakses database sensitif, menanamkan backdoor, atau memodifikasi konfigurasi sistem agar mempermudah akses di masa mendatang. Ketiga, terdapat modifikasi artefak digital, termasuk penghapusan atau perubahan log sistem, pemasangan malware tersembunyi, dan skrip otomatis yang dapat berjalan tanpa terdeteksi. Keempat, aktivitas eksfiltrasi data dilakukan untuk mengambil informasi pelanggan, data transaksi, dan dokumen penting perusahaan secara diam-diam.

Temuan ini sejalan dengan studi Aghili, Khaleghi, & Dehghantanha (2020), yang menyatakan bahwa berbagai jenis serangan, seperti DDoS, SQL injection,

dan insider threat, semakin kompleks dan membutuhkan pendekatan forensik jaringan yang spesifik. Hal ini menunjukkan bahwa attack surface organisasi semakin luas, dan pelaku kini melakukan serangkaian tindakan tersembunyi dan berkelanjutan, yang tidak hanya menargetkan satu titik lemah, tetapi memanfaatkan kelemahan pada berbagai sistem secara simultan.

Efektivitas Tahapan Digital Forensik

Metode digital forensik yang diterapkan dalam penelitian mengikuti lima tahapan utama: identifikasi, preservasi, pengumpulan, analisis, dan penyajian.

Pada tahap identifikasi, penelitian menemukan bahwa indikator awal insiden dapat berupa gagal login berulang, trafik jaringan tidak biasa, perubahan file sistem, atau anomali pada log aplikasi. Identifikasi ini menjadi dasar untuk menentukan titik awal investigasi. Literatur menekankan bahwa deteksi dini sangat penting untuk meminimalkan kerusakan yang lebih luas (Raghavan & Thuraisingham, 2019). Tahap preservasi dilakukan dengan membuat imaging disk secara bit-by-bit, snapshot memori, dan hashing data untuk menjaga integritas bukti. Proses ini memastikan bahwa artefak digital tetap utuh dan sah secara hukum, yang penting dalam audit atau proses litigasi (Casey, 2011). Dalam penelitian ini, preservasi dilakukan pada seluruh storage sistem target dan log jaringan secara real-time untuk mencegah kehilangan bukti akibat aktivitas anti-forensik. Tahap pengumpulan mencakup pengambilan artefak digital, log sistem, memori RAM, trafik jaringan (packet capture), dan file konfigurasi yang relevan. Pengumpulan bukti dilakukan sesuai standar operasional prosedur (SOP) agar hasilnya dapat dipertanggungjawabkan. Teknik ini memungkinkan peneliti memperoleh gambaran komprehensif tentang serangan, termasuk jalur akses, aktivitas pelaku, dan data yang dieksfiltrasi (Nelson, Phillips & Steuart, 2014).

Tahap analisis merupakan inti dari forensik digital. Data yang dikumpulkan diinterpretasikan untuk menjawab pertanyaan “apa yang terjadi”, “siapa pelakunya”, “bagaimana pelanggaran terjadi”, “kapan”, dan “mengapa”. Penelitian ini menemukan bahwa pelaku menggunakan kredensial yang sah untuk mengakses server setelah mengeksploitasi kerentanan SMB, melakukan privilege escalation untuk mendapatkan hak admin, dan mengunduh file sensitif dari database dalam waktu kurang dari dua jam. Analisis juga menunjukkan adanya aktivitas anti-forensik, seperti penghapusan log dan perubahan timestamp file, yang digunakan untuk menutupi jejak. Studi terbaru menyebutkan bahwa machine learning dan AI kini mulai diterapkan untuk mempercepat identifikasi pola serangan dan deteksi anomali secara otomatis (Chandola, Banerjee & Kumar, 2020).

Tahap penyajian melibatkan pembuatan laporan forensik yang mendokumentasikan timeline kejadian, artefak bukti, interpretasi analisis, dan

rekomendasi mitigasi. Laporan disusun agar dapat dipahami oleh teknisi, manajemen, maupun pihak hukum. Dalam penelitian ini, penyajian juga mencakup diagram alur serangan, daftar sistem terdampak, dan saran perbaikan prosedur keamanan, yang membantu perusahaan memahami celah dan potensi risiko yang harus ditangani (Grispos, Storer & Glisson, 2014).

Temuan Utama dan Interpretasi

Temuan penelitian mengungkapkan bahwa pelaku memanfaatkan kombinasi akses sah dan teknik anti-forensik untuk melakukan eksfiltrasi data. Aktivitas login dari akun pengguna biasa ditingkatkan ke akun admin melalui privilege escalation. Paket jaringan menunjukkan trafik keluar yang tidak biasa ke server eksternal melalui port non-standar, menandakan pengambilan data sensitif. Selain itu, perubahan timestamp file dan penghapusan log event menunjukkan upaya pelaku untuk menghindari deteksi, yang sesuai dengan literatur mengenai teknik anti-forensik (Grispos et al., 2014). Analisis juga mengungkap bahwa perusahaan belum memiliki monitoring aktivitas jaringan real-time maupun retensi log memadai, sehingga pelaku dapat bergerak dalam sistem lebih lama sebelum terdeteksi. Interpretasi ini menegaskan pentingnya tahapan preservasi dan pengumpulan bukti yang kuat agar bukti tidak hilang atau sulit ditelusuri.

Tantangan dan Keterbatasan

Beberapa tantangan utama dalam penerapan metode digital forensik meliputi waktu respon terbatas, keterbatasan alat untuk mendeteksi serangan canggih seperti file-less malware, kompleksitas volume data yang besar, serta aspek hukum dan etika terkait privasi dan chain of custody (Baryamureeba & Tushabe, 2004). File-less malware, misalnya, hampir tidak meninggalkan artefak pada disk, sehingga sulit dideteksi dengan metode tradisional. Volume log jaringan yang sangat besar membutuhkan sumber daya signifikan untuk dianalisis, khususnya jika menggunakan teknik AI atau machine learning yang belum sepenuhnya diintegrasikan.

Implikasi untuk Praktik Keamanan Siber dan Forensik

Penelitian ini menekankan perlunya forensic readiness, yaitu kesiapan organisasi dalam hal sistem dan prosedur untuk melakukan forensik digital saat terjadi insiden. Kolaborasi antara tim keamanan operasional dan tim forensik digital juga penting agar investigasi cepat dilakukan dan bukti tidak hilang. Investasi pada teknologi forensik modern dan pelatihan personel sangat diperlukan agar organisasi mampu merespons insiden secara cepat dan akurat. Selain itu, prosedur retensi log, pemantauan real-time, dan otomatisasi analisis forensik menjadi faktor utama untuk meminimalkan waktu pergerakan pelaku tanpa terdeteksi (Bejtlich, 2013). Hasil forensik sebaiknya digunakan untuk memperbaiki kebijakan keamanan, prosedur tanggap insiden, serta strategi pencegahan di masa depan.

Rekomendasi Penelitian dan Praktik Selanjutnya

Beberapa rekomendasi dari penelitian ini meliputi pengembangan metode digital forensik yang terintegrasi dengan machine learning dan AI untuk menangani volume data besar serta mendeteksi pola serangan secara otomatis. Studi kasus di perusahaan besar dengan kolaborasi antara tim keamanan dan forensik penting untuk memperoleh bukti empiris yang lebih mendalam. Selain itu, perlu dikembangkan kerangka kerja investigasi khusus untuk pelanggaran data pada lingkungan cloud dan IoT, karena karakteristiknya berbeda dengan sistem tradisional. Pengembangan standar prosedur forensik digital yang sesuai dengan regulasi lokal, termasuk di Indonesia, juga penting agar bukti digital yang diperoleh sah secara hukum.

KESIMPULAN

Berdasarkan hasil penelitian, metode digital forensik terbukti efektif dalam mengungkap pelanggaran keamanan siber pada bisnis online secara sistematis dan akurat. Melalui tahapan identifikasi, preservasi, pengumpulan, analisis, dan penyajian, peneliti dapat menelusuri jejak serangan, mengenali pola aktivitas pelaku, serta memastikan integritas bukti digital. Temuan menunjukkan bahwa serangan siber biasanya dimulai dari eksploitasi celah keamanan, diikuti oleh akses tidak sah dan eksfiltrasi data, serta indikasi manipulasi file dan penghapusan log yang menunjukkan upaya anti-forensik. Hal ini menekankan pentingnya penerapan forensic readiness dan kesiapan sistem untuk mendeteksi aktivitas abnormal sejak dini.

Digital forensik tidak hanya berfungsi sebagai alat investigasi teknis, tetapi juga strategis dalam pembentukan kebijakan keamanan siber, penguatan kolaborasi antara tim keamanan operasional dan forensik digital, serta peningkatan ketahanan sistem informasi untuk mencegah insiden serupa di masa depan. Beberapa rekomendasi dari penelitian ini meliputi penguatan forensic readiness melalui sistem log terpusat dan penyimpanan bukti digital yang aman, pelatihan dan sertifikasi personel forensik digital, integrasi AI dan machine learning dalam analisis bukti digital, serta kerja sama lintas lembaga untuk pengembangan standar prosedur forensik digital sesuai konteks hukum dan teknologi di Indonesia. Penelitian selanjutnya disarankan mengkaji penerapan digital forensik pada lingkungan cloud computing dan IoT, mengingat kompleksitas dan dinamika ancaman yang terus berkembang.

DAFTAR PUSTAKA

Aghili, S., Khaleghi, A. & Dehghantanha, A., 2020. Network Attacks Classification for Network Forensics Investigation. Journal of Cybersecurity and Digital Forensics, 8(2), pp.45–60.

Baryamureeba, V. & Tushabe, F., 2004. The Enhanced Digital Investigation Process Model. Digital Forensics Research Workshop, pp.1–12.

Bejtlich, R., 2013. The Practice of Network Security Monitoring: Understanding Incident Detection and Response. 2nd ed. Boston: No Starch Press.

Casey, E., 2011. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. 3rd ed. Waltham: Academic Press.

Chandola, V., Banerjee, A. & Kumar, V., 2020. Anomaly Detection for Cybersecurity: A Machine Learning Perspective. ACM Computing Surveys, 50(3), pp.1–36.

ENISA, 2022. ENISA Threat Landscape 2022. [online] Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 [Accessed 30 December 2025].

Grispos, G., Storer, T. & Glisson, W., 2014. Using Anti-Forensics Techniques to Avoid Detection of Malicious Activities in Digital Investigations. Computers & Security, 45, pp.91–106.

Kshetri, N., 2017. Cybersecurity Issues in E-Commerce. In: N. Kshetri, ed. The Economics of Cybersecurity. Cham: Springer, pp.13–28.

Kumar, S., Sharma, P. & Singh, R., 2021. Cybersecurity in Online Businesses: Threats, Challenges, and Digital Forensic Approaches. Journal of Information Security, 12(3), pp.112–126.

Laudon, K.C. & Traver, C.G., 2020. E-commerce 2020: Business, Technology, Society. 16th ed. Boston: Pearson.

Nelson, B., Phillips, A. & Steuart, C., 2014. Guide to Computer Forensics and Investigations. 5th ed. Boston: Cengage Learning.

Raghavan, S. & Parthasarathy, S., 2019. Digital Forensics for Cybersecurity. New York: Springer.

Raghavan, S. & Thuraisingham, B., 2019. Digital Forensics for Network and Database Security. Springer.

Von Solms, R. & Van Niekerk, J., 2013. From Information Security to Cyber Security. Computers & Security, 38, pp.97–102.