Jurnal Ilmu Komputer dan Sistem Informasi
JIKSI, Vol. 02, No. 03, Oktober 2021: 116-120
Received: 5 Agustus 2021; Revised: 29 September 2021; Accepted: 30 Oktober 2021

Peretas dan Identifikasi Pencurian: Analisis Etis dan Strategis Keamanan Siber dalam Melindungi Infrastruktur Kritis Studi Kasus Insiden FAA 2023

Faliandy

Program Magister Teknik Informatika
Universitas Bina Darma
email : fali.faliandy@gmail.com
Jl. A. Yani No. 12, Palembang 30624, Indonesia

Abstract

This research aims to analyze the ethical implications of cybersecurity breaches, focusing on an incident involving the United States Federal Aviation Administration (FAA) in January 2023. Although the cause was not officially confirmed as a cyberattack, the resulting impact and response provide important insights into the vulnerability of critical infrastructure to digital threats and the ethical dilemmas involved in protecting it. A qualitative approach was used, employing literature analysis and case studies to examine the dimensions of cybersecurity breaches, including types of attacks, social and economic impacts, and ethical responsibilities in prevention and response. The analysis revealed that protecting critical infrastructure requires a comprehensive and adaptive cybersecurity strategy that integrates technical, policy, and professional ethics considerations. This research underscores the importance of balancing security and privacy in achieving sustainable cyber governance.

Kata kunci: *cybersecurity, technology ethics, critical infrastructure, FAA incidents, data breaches.*

Abstrak

Penelitian ini bertujuan untuk menganalisis implikasi etis dari pelanggaran keamanan siber dengan fokus pada insiden yang melibatkan Federal Aviation Administration (FAA) Amerika Serikat pada Januari 2023. Meskipun penyebabnya tidak secara resmi dikonfirmasi sebagai serangan siber, dampak dan respons yang ditimbulkan memberikan wawasan penting tentang kerentanan infrastruktur kritis terhadap ancaman digital dan dilema etika dalam melindunginya. Penelitian ini menggunakan pendekatan kualitatif melalui analisis literatur dan studi kasus untuk menelaah dimensi pelanggaran keamanan siber, termasuk jenis serangan, dampak sosial dan ekonomi, serta tanggung jawab etis dalam pencegahan dan penanggulangan. Hasil analisis menunjukkan bahwa perlindungan infrastruktur kritis memerlukan strategi keamanan siber yang komprehensif dan responsif, mencakup aspek teknis, kebijakan, dan etika profesional. Penelitian ini menegaskan pentingnya keseimbangan antara keamanan dan privasi dalam tata kelola siber yang berkelanjutan.
Kata kunci: *keamanan siber, etika teknologi, infrastruktur kritis, insiden FAA, pelanggaran data.*

1. PENDAHULUAN (12 pt)

Kemajuan teknologi informasi telah membawa perubahan besar terhadap sistem sosial, ekonomi, dan politik global. Namun, perkembangan ini juga disertai dengan meningkatnya ancaman keamanan siber (cybersecurity threats) yang semakin kompleks. Serangan siber tidak lagi terbatas pada individu atau perusahaan, tetapi juga menyasar infrastruktur kritis negara seperti sektor transportasi, energi, dan kesehatan (Clark & Hakim, 2017).

Ancaman siber mencakup berbagai bentuk, seperti malware, phishing, ransomware, dan data breaches. Dampaknya meliputi kerugian ekonomi, gangguan operasional, hingga ancaman terhadap keselamatan publik. Menurut Stiennon (2020), pelanggaran keamanan siber terhadap infrastruktur kritis merupakan ancaman terbesar bagi stabilitas nasional pada dekade ini.

Salah satu insiden yang menyoroti isu tersebut adalah gangguan sistem FAA pada Januari 2023. Gangguan ini menyebabkan ribuan penerbangan di seluruh Amerika Serikat tertunda. Meskipun penyebabnya tidak dikonfirmasi sebagai serangan siber, insiden tersebut memperlihatkan urgensi penguatan keamanan digital dan etika dalam perlindungan infrastruktur vital.

Penelitian ini bertujuan untuk mengidentifikasi bentuk serta karakteristik pelanggaran keamanan siber yang terjadi terhadap infrastruktur kritis. Infrastruktur kritis merupakan komponen utama dalam sistem nasional yang menopang fungsi vital seperti energi, transportasi, komunikasi, dan layanan publik. Pelanggaran terhadap infrastruktur tersebut tidak hanya berpotensi menimbulkan kerugian ekonomi yang signifikan, tetapi juga dapat mengancam stabilitas sosial dan keamanan negara. Oleh karena itu, pemahaman yang mendalam mengenai pola, motif, serta kerentanan sistem menjadi langkah awal yang penting dalam upaya merumuskan kebijakan keamanan yang adaptif dan berkelanjutan.

Selain itu, penelitian ini menganalisis implikasi etis serta tanggung jawab sosial dalam konteks keamanan siber. Perkembangan teknologi informasi yang semakin pesat telah memunculkan tantangan moral yang kompleks, terutama terkait isu privasi, hak atas data, dan kewajiban profesional para pelaku di bidang teknologi digital. Dalam kerangka etika profesional, keamanan siber tidak hanya dipandang sebagai persoalan teknis, tetapi juga sebagai tanggung jawab sosial yang menuntut kesadaran akan dampak tindakan individu maupun organisasi terhadap masyarakat luas. Analisis etis ini menjadi relevan untuk menegaskan pentingnya keseimbangan antara inovasi teknologi dan perlindungan nilai-nilai kemanusiaan.

Selanjutnya, penelitian ini mengevaluasi strategi pencegahan dan kebijakan keamanan siber berbasis etika profesional. Evaluasi dilakukan dengan mempertimbangkan prinsip-prinsip transparansi, akuntabilitas, dan integritas yang menjadi landasan utama dalam tata kelola keamanan digital. Melalui pendekatan tersebut, penelitian ini diharapkan dapat memberikan kontribusi terhadap pengembangan model kebijakan yang tidak hanya berfokus pada mitigasi risiko teknis, tetapi juga memperkuat dimensi moral dan tanggung jawab sosial dalam praktik keamanan siber. Dengan demikian, hasil penelitian ini diharapkan dapat menjadi rujukan bagi pembuat kebijakan, praktisi teknologi informasi, serta peneliti dalam memperkuat sistem keamanan nasional yang etis, berkeadilan, dan berkelanjutan.

2. METODOLOGI PENELITAN

Penelitian ini menggunakan pendekatan kualitatif deskriptif melalui studi literatur dan analisis kasus. Pendekatan ini dipilih karena mampu memberikan pemahaman mendalam terhadap fenomena keamanan siber serta dimensi etika yang melingkupinya.

2.1 Tahapan Penelitian

1. Pengumpulan Data Sekunder Data diperoleh dari artikel ilmiah, laporan lembaga keamanan siber (CERT, ENISA, NIST), dan media kredibel seperti Reuters dan CNN.
2. Pemilihan Studi Kasus Kasus yang dikaji meliputi insiden FAA (2023) serta beberapa pelanggaran keamanan siber pada infrastruktur kritis, seperti serangan Colonial Pipeline (2021) dan WannaCry (2017).
3. Analisis Data Analisis dilakukan secara tematik, mencakup: Jenis dan mekanisme serangan. Dampak sosial, ekonomi, dan etis. Strategi pencegahan dan kebijakan keamanan.
4. Validasi Data Validasi dilakukan dengan triangulasi sumber serta pembandingan dengan publikasi akademik dan laporan lembaga internasional (Goodrich & Rampolla, 2020; Mansfield-Devine, 2018).

3. HASIL DAN PEMBAHASAN

3.1 Jenis dan Karakteristik Serangan Siber

Berdasarkan analisis literatur, terdapat enam jenis utama serangan siber yang sering menargetkan infrastruktur kritis.

Jenis Serangan	Deskripsi Singkat	Contoh Kasus
Phishing	Upaya memperoleh data sensitif melalui email atau situs palsu.	Serangan pada lembaga keuangan global.
Ransomware	Enkripsi data korban disertai permintaan tebusan.	Serangan *WannaCry* (2017).
DDoS (*Distributed Denial of Service*)	Pembanjiran lalu lintas palsu ke server hingga layanan lumpuh.	Serangan terhadap penyedia DNS Dyn.
Man-in-the-Middle	Penyadapan komunikasi antar pengguna.	Penyerangan sistem transaksi daring.
SQL Injection	Manipulasi basis data melalui perintah SQL berbahaya.	Serangan pada situs e-commerce.
Zero-Day Attack	Eksploitasi celah keamanan yang belum diperbaiki.	Eksploitasi sistem SCADA industri.

Serangan-serangan tersebut memperlihatkan bahwa keamanan siber memerlukan sistem pertahanan berlapis serta kesadaran etis dalam pengelolaan data digital.

3.2 Studi Kasus: Insiden FAA 2023

Kronologi KejadianPada 11 Januari 2023, sistem Notice to Air Missions (NOTAM) milik Federal Aviation Administration (FAA) mengalami gangguan besar yang menyebabkan seluruh penerbangan domestik di Amerika Serikat dihentikan sementara (Shepardson et al., 2023). Akibat insiden ini, lebih dari 10.000 penerbangan tertunda, menimbulkan kerugian ekonomi signifikan serta ketidaknyamanan masyarakat (Muntean & Wallace, 2023).

Analisis Teknis dan DampakWalaupun penyebabnya belum dikonfirmasi sebagai serangan siber, insiden ini menunjukkan potensi kerentanan sistem penerbangan digital. Gangguan pada sistem semacam ini dapat mengancam keselamatan publik dan menurunkan kepercayaan terhadap keamanan infrastruktur penerbangan (Wald, 2023).

Evaluasi Etis Dari perspektif etika, FAA menghadapi dilema antara transparansi informasi publik dan perlindungan data sensitif. Lembaga ini memiliki tanggung jawab moral untuk:Menyampaikan informasi faktual tanpa menimbulkan kepanikan.Melindungi data dari potensi eksploitasi.Menjalankan langkah korektif secara cepat dan proporsional.

3.3 Implikasi Sosial dan Etika

1. Dampak Sosial dan EkonomiGangguan pada infrastruktur kritis dapat menimbulkan efek domino terhadap sektor ekonomi, mobilitas masyarakat, dan stabilitas publik.
2. Tanggung Jawab EtisInstitusi publik wajib menjamin keamanan sistem digital yang berdampak pada keselamatan masyarakat. Ketidakmampuan mengelola risiko siber dapat dikategorikan sebagai pelanggaran tanggung jawab sosial (social accountability).
3. Dilema Privasi dan KeamananPenguatan keamanan siber sering kali berbenturan dengan hak privasi pengguna. Diperlukan pendekatan etis yang menyeimbangkan antara keamanan nasional dan hak asasi digital.

Pembahasan

Nye (2017) menegaskan bahwa keamanan siber tidak semata-mata merupakan persoalan teknis, melainkan juga berkaitan erat dengan dimensi moral dan etika. Dalam konteks ini, kebijakan keamanan siber harus mempertimbangkan prinsip-prinsip dasar seperti hak atas privasi, keadilan, dan proporsionalitas dalam setiap tindakan atau kebijakan yang diambil. Misalnya, pengumpulan data untuk kepentingan keamanan perlu dilakukan secara transparan serta berdasarkan persetujuan pengguna agar tidak melanggar hak individu. Etika profesional dalam bidang keamanan siber juga menuntut para praktisi untuk menjaga kerahasiaan data dan informasi pengguna, menghindari penyalahgunaan akses terhadap sistem, serta mengedepankan prinsip do no harm dalam setiap tindakan. Dengan demikian, penerapan etika profesional menjadi landasan fundamental untuk memastikan bahwa praktik keamanan siber dijalankan secara bertanggung jawab, tidak hanya efektif secara teknis, tetapi juga sesuai dengan nilai moral dan sosial.

Perlindungan terhadap infrastruktur kritis menuntut adanya kombinasi antara kebijakan publik yang kuat dan strategi teknis yang adaptif. Upaya perlindungan tersebut dapat diwujudkan melalui penguatan jaringan serta penerapan sistem deteksi ancaman otomatis yang mampu mengenali potensi serangan sejak dini. Selain itu, manajemen kerentanan harus dilakukan secara proaktif melalui kegiatan audit serta pembaruan sistem secara berkala untuk mengurangi potensi risiko eksploitasi. Peningkatan literasi keamanan digital bagi seluruh pemangku kepentingan menjadi hal yang esensial dalam membangun kesadaran kolektif terhadap pentingnya perlindungan data dan informasi. Dalam skala yang lebih luas, kerja sama internasional dalam pertukaran intelijen siber, sebagaimana diungkapkan oleh Theohary dan Rollins (2019), berperan penting dalam memperkuat ketahanan digital suatu negara menghadapi ancaman lintas batas.

Serangan siber memiliki karakter lintas batas yang kompleks, sehingga penanganannya memerlukan kerangka hukum internasional yang adaptif dan inklusif. Kallberg dan Thuraisingham (2016) menegaskan bahwa Budapest Convention on Cybercrime merupakan contoh nyata harmonisasi kebijakan global yang berperan penting dalam penanggulangan kejahatan digital. Konvensi tersebut mendorong kerja sama antarnegara dalam penyelidikan, penegakan hukum, dan pengembangan standar keamanan bersama di tingkat global. Dengan adanya keselarasan kebijakan dan hukum internasional, negara-negara dapat memperkuat sistem keamanan siber mereka tanpa mengabaikan prinsip etika, hak asasi manusia, serta kedaulatan digital. Pendekatan global ini menegaskan bahwa keamanan siber bukan hanya tanggung jawab nasional, melainkan agenda kolektif yang diperlukan untuk menjaga stabilitas, kepercayaan, dan keadilan di era digital yang saling terhubung.

4. KESIMPULAN

1. Tanggung Jawab EtisPerlindungan terhadap infrastruktur kritis menuntut tanggung jawab etis tinggi, termasuk akuntabilitas, transparansi, dan integritas dalam pengelolaan sistem digital.
2. Keseimbangan Keamanan dan PrivasiKebijakan keamanan siber perlu mengedepankan keseimbangan antara kepentingan nasional dan hak privasi individu.
3. Pendidikan dan Kesadaran SiberPenguatan literasi keamanan digital menjadi langkah preventif penting dalam mengurangi risiko serangan siber.
4. Kerja Sama GlobalKolaborasi antarnegara merupakan kunci dalam menghadapi ancaman siber berskala global.

Referensi

Clark, R. M., & Hakim, S. (Eds.). (2017). *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level.* Springer.

Goodrich, K., & Rampolla, J. (2020). *Implications of Cyber Threats on National Security. National Security Journal.*

Kallberg, J., & Thuraisingham, B. (2016). *Cyber Operations and the Use of Force in International Law.* Oxford University Press.

Liu, L., & Chang, V. (2017). *The Role of AI in the Future of Cybersecurity. Computer Fraud & Security, 2017*(9), 17–20.

Mansfield-Devine, S. (2018). *The Growing Threat to Critical Infrastructure. Computer Fraud & Security, 2018*(11), 17–20.

Muntean, P., & Wallace, G. (2023). *Flight Departures Halted Across the United States Due to FAA System Outage.* CNN.

Nye, J. S. (2017). *Deterrence and Dissuasion in Cyberspace. International Security, 41*(3), 44–71.

Shepardson, D., Singh, R. K., & Ganapavaram, A. (2023). *U.S. Flights Beginning to Resume After FAA System Outage.* Reuters.

Stiennon, R. (2020). *Threats to Critical Infrastructure: The Next Cyber Battleground. Journal of Cyber Policy, 5*(1), 104–117.

Theohary, C. A., & Rollins, J. (2019). *Cyberwarfare and Cyberterrorism: In Brief. Congressional Research Service Report.*

Wald, M. (2023). *Assessing Cybersecurity Risks in the Aviation Sector: FAA Case Study. Aviation Safety Journal.*

Zetter, K. (2014). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon.* Crown.