TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 3, Tahun 2025
ISSN 3024-8256 (media online)
Hal 573-576

Etika Profesi TI dalam Menghadapi Serangan Ransomware: Studi Kasus Bank Syariah Indonesia 2023

Muhammad Rafi'al Tsaqif[1], Achmad Iqbal Fathoni[2], Nur Rahma Andini[3], Annisa Elfina Augustia[4]

[1-4]Teknik dan Ilmu Komputer, Teknik Informatika, Universitas Indraprasta PGRI, Jakarta, Indonesia
Email :[1]rafialtsaqif@gmail.com, [2]fathoniiqbal4@gmail.com, [3]nurraa.0311@gmail.com, [4]annisa12elfina@gmail.com
(*: corresponding author)

Abstrak− Serangan ransomware yang menimpa Bank Syariah Indonesia (BSI) pada tahun 2023 menjadi salah satu insiden siber terbesar di sektor perbankan nasional. Insiden ini tidak hanya mengakibatkan gangguan operasional dan kerugian finansial, tetapi juga menimbulkan persoalan moral dan etika bagi para profesional teknologi informasi (TI) dalam merespons situasi krisis. Penelitian ini bertujuan untuk menganalisis penerapan etika profesi TI dalam menghadapi serangan ransomware, dengan menggunakan pendekatan kualitatif deskriptif melalui studi kasus pada Bank Syariah Indonesia. Data diperoleh dari sumber sekunder seperti laporan resmi, pemberitaan media, dan kajian akademik terkait etika profesi serta keamanan siber. Hasil penelitian menunjukkan bahwa para profesional TI dihadapkan pada dilema etika, antara menjaga transparansi publik dan melindungi kerahasiaan data perusahaan. Selain itu, ditemukan bahwa penerapan kode etik profesi seperti tanggung jawab, integritas, dan kejujuran menjadi landasan penting dalam pengambilan keputusan selama proses penanganan insiden. Penelitian ini diharapkan dapat memberikan kontribusi terhadap penguatan kesadaran etika profesi TI di Indonesia, khususnya dalam menghadapi ancaman siber yang semakin kompleks.

Kata Kunci: etika profesi TI; ransomware; keamanan siber; Bank Syariah Indonesia; tanggung jawab profesional

Abstract− *The ransomware attack that hit Bank Syariah Indonesia (BSI) in 2023 became one of the biggest cyber incidents in the national banking sector. This incident not only resulted in operational disruptions and financial losses, but also caused moral and ethical problems for information technology (IT) professionals in responding to crisis situations. This research aims to analyse the application of IT professional ethics in dealing with ransomware attacks, by using a descriptive qualitative approach through a case study at Bank Syariah Indonesia. Data is obtained from secondary sources such as official reports, media coverage, and academic studies related to professional ethics and cyber security. Research results show that IT professionals are faced with an ethical dilemma, between maintaining public transparency and protecting the confidentiality of company data. In addition, it was found that the implementation of a professional code of ethics such as responsibility, integrity, and honesty became an important foundation in decision-making during the incident handling process. This research is expected to contribute to the strengthening of ethical awareness of the IT profession in Indonesia, especially in facing increasingly complex cyber threats.*

Keywords*: IT profesional ethics; ransomware; cyber security; Indonesian Syariah Bank; profesional responsibility*

1. PENDAHULUAN

Perkembangan teknologi informasi yang pesat membawa kemudahan sekaligus risiko baru di sektor perbankan, terutama dalam hal keamanan data nasabah. Bank Syariah Indonesia sebagai institusi keuangan berbasis syariah menghadapi tantangan besar dalam menjaga integritas dan kerahasiaan informasi. Serangan siber berupa ransomware yang terjadi pada tahun 2023 menguji sistem pertahanan keamanan serta kesiapan manajemen risiko bank dalam menghadapi ancaman digital. Ransomware adalah salah satu jenis malware yang dapat mengenkripsi data penting, sehingga mengharuskan korban untuk membayar tebusan guna memulihkan akses terhadap data tersebut. Fenomena ini tidak hanya menimbulkan kerugian finansial, tetapi juga mengancam kepercayaan nasabah dan reputasi bank syariah secara keseluruhan (Polim, 2023; Merkurius Journal, 2024).

Dalam konteks tersebut, penerapan etika profesi teknologi informasi menjadi sangat penting. Etika profesi mengatur perilaku dan standar moral profesional TI dalam melindungi data nasabah, menjunjung transparansi, serta bertanggung jawab atas pengelolaan sistem informasi. Prinsip-prinsip etika seperti integritas, tanggung jawab profesional, dan transparansi menjadi landasan bagi

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 3, Tahun 2025
ISSN 3024-8256 (media online)
Hal 573-576

pengambilan keputusan dalam pengelolaan risiko keamanan informasi. Penerapan etika ini bukan hanya aspek teknis, tetapi juga mencakup aspek sosial dan hukum yang harus diindahkan untuk menjaga kredibilitas institusi perbankan syariah (Gunawan, 2025; Zebua, 2025; LinuxHackingID, 2025).

Sejumlah studi telah menunjukkan bahwa kesiapan organisasi dalam mengintegrasikan nilai-nilai etika profesi TI berdampak positif pada ketahanan sistem terhadap serangan siber dan perlindungan data nasabah. Penelitian ini bertujuan untuk mengkaji secara mendalam bagaimana Bank Syariah Indonesia mengaplikasikan prinsip etika profesi TI dalam merespons serangan ransomware pada tahun 2023 serta implikasi dari penerapan etika tersebut terhadap kepercayaan dan perlindungan konsumen (Anugrah, 2025; Azarine, 2023).

Dengan memperpanjang analisis dan kajian pada aspek ini, diharapkan penelitian ini dapat memberikan kontribusi berupa rekomendasi yang konkret bagi institusi perbankan dalam mengelola risiko serangan siber secara etis dan profesional, khususnya di sektor perbankan syariah yang memiliki nilai dan prinsip berbeda dengan perbankan konvensional.

2. METODE PENELITIAN

Penelitian ini menerapkan metode *Systematic Literature Review* (SLR) yang dikombinasikan dengan studi kasus empiris untuk mengevaluasi fungsi etika profesional teknologi informasi dalam menghadapi ancaman ransomware di Bank Syariah Indonesia (BSI) pada tahun 2023. Metode ini dipilih karena dapat menghasilkan temuan penelitian yang terstruktur, terbuka, dan dapat diulang. Teknik SLR diterapkan untuk menyelidiki hubungan antara prinsip etika profesional dan perlindungan data organisasi, sementara studi kasus BSI berfungsi sebagai data praktis untuk mendukung sintesis konseptual hasil tinjauan literatur. Proses penelitian mengikuti pedoman PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*), yang memastikan bahwa pemilihan literatur dilakukan secara objektif dan terukur.

2.1 Tahapan Penelitian

Proses penelitian dimulai dengan identifikasi awal karya ilmiah yang relevan. Pencarian literatur dilakukan menggunakan berbagai basis data, seperti Google Scholar, DOAJ, ScienceDirect, dan Garuda. Kata kunci yang digunakan meliputi "etika profesional teknologi informasi," "ransomware," "keamanan informasi perbankan," "Bank Syariah Indonesia," dan "etika siber." Periode publikasi dibatasi pada tahun 2020–2025 untuk memastikan bahwa konteks penelitian sejalan dengan perkembangan terbaru dalam ancaman siber. Dari pencarian awal, diperoleh 120 artikel ilmiah potensial.

2.2 Teknik Analisis

Analisis data dilakukan menggunakan pendekatan analisis konten kualitatif pada lima belas artikel terpilih. Analisis ini berfokus pada empat kategori utama, yaitu: (1) prinsip etika profesional teknologi informasi, (2) sistem manajemen keamanan informasi, (3) serangan ransomware dan dampaknya terhadap organisasi, serta (4) regulasi dan kepatuhan organisasi terhadap keamanan data. Setiap artikel dievaluasi untuk mengidentifikasi pola tematik, perbedaan pendekatan, dan celah penelitian yang dapat digunakan sebagai dasar rekomendasi. Hasil analisis literatur ini kemudian diintegrasikan dengan kasus serangan ransomware 2023 terhadap Bank Syariah Indonesia (BSI), yang digunakan sebagai ilustrasi empiris. Analisis kasus BSI dilakukan untuk mengevaluasi penerapan nilai-nilai etika seperti tanggung jawab, akuntabilitas, dan integritas dalam konteks manajemen keamanan informasi. Insiden kebocoran data yang disebabkan oleh serangan ransomware LockBit 3.0 pada tahun 2023, yang mengakibatkan hilangnya lebih dari 1,5 TB data pelanggan, digunakan sebagai bahan evaluasi untuk menilai sejauh mana pelanggaran prinsip etika profesional mempengaruhi keamanan organisasi. Pendekatan ini juga memungkinkan peneliti untuk membandingkan teori dalam literatur akademik dengan praktik nyata di lapangan.

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 3, Tahun 2025
ISSN 3024-8256 (media online)
Hal 573-576

3. ANALISA DAN PEMBAHASAN

3.1 Analisa Insiden Serangan Ransomware

Serangan ransomware yang menimpa Bank Syariah Indonesia (BSI) pada tahun 2023 menjadi salah satu insiden siber terbesar di sektor keuangan syariah di Indonesia. Serangan ini mengakibatkan gangguan layanan transaksi, keterlambatan proses operasional, serta kebocoran data pada beberapa sistem internal. Dari perspektif etika profesi TI, insiden ini menunjukkan bahwa pengelolaan keamanan informasi masih memiliki celah yang perlu diperkuat, terutama terkait kesiapan sistem, budaya keamanan, serta manajemen respons insiden.

Analisis teknis memperlihatkan bahwa serangan dilakukan melalui eksploitasi celah *vulnerability* pada server dan kurangnya lapisan deteksi ancaman berbasis *behavioral analysis*. Hal ini mengindikasikan perlunya penerapan standar etika profesi TI yang menekankan tanggung jawab, kompetensi, dan kewaspadaan dalam mengelola sistem informasi kritikal

3.2 Tinjauan Etika Profesi TI dalam Konteks Keamanan Sibe

Etika profesi TI mengatur bagaimana profesional teknologi informasi harus berperilaku dalam menjalankan tugasnya. Prinsip-prinsip utama seperti tanggung jawab, integritas, kompetensi profesional, dan kerahasiaan informasi menjadi fondasi dalam menghadapi ancaman seperti ransomware.

Pada kasus BSI, prinsip etika TI diuji ketika perusahaan harus menjaga kepercayaan publik sekaligus melindungi data nasabah. Etika menuntut profesional TI untuk:

a. Mengantisipasi risiko melalui penerapan *best practices* keamanan.
b. Menjaga ketepatan informasi dan transparansi kepada pemangku kepentingan.
c. Mengambil keputusan yang cepat, tepat, dan sesuai regulasi.

Kegagalan dalam menerapkan prinsip-prinsip tersebut tidak hanya berdampak teknis tetapi juga berdampak pada reputasi lembaga keuangan.

3.3 Dampak Pelanggaran Etika dan Keamanan terhadap Layanan Perbankan Syariah

Serangan ransomware pada BSI memperlihatkan betapa pentingnya integritas dan profesionalisme dalam pengelolaan TI. Gangguan layanan selama beberapa hari mengakibatkan:

a. Tidak berfungsinya layanan ATM, mobile banking, dan *counter service*.
b. Ketidaknyamanan nasabah dan turunnya tingkat kepercayaan publik.
c. Potensi pelanggaran ketentuan OJK terkait perlindungan data nasabah.

Dari perspektif etika TI, dampak ini terjadi ketika kontrol keamanan tidak diimplementasikan secara optimal. Profesional TI dituntut untuk selalu mematuhi *code of conduct* dalam menjaga keberlangsungan layanan dan melindungi kepentingan masyarakat

3.4 Implementasi Etika Profesi TI dalam Respons Insiden

Respons insiden siber di perbankan harus mengacu pada standar internasional seperti ISO/IEC 27035, yang menekankan pendekatan sistematis dalam deteksi, analisis, penanganan, dan pemulihan. Pada kasus BSI, upaya yang dilakukan meliputi:

a. Pemutusan sementara sistem yang terdampak guna mencegah eskalasi serangan.
b. Koordinasi dengan Badan Siber dan Sandi Negara (BSSN).
c. Komunikasi kepada publik mengenai proses pemulihan.

Tindakan ini merupakan implementasi etika TI karena menunjukkan akuntabilitas dan transparansi. Namun demikian, etika menuntut lebih dari sekadar respons; pencegahan dan evaluasi berkala merupakan bagian penting dari profesionalisme TI.

4. KESIMPULAN

Insiden ransomware yang dialami oleh Bank Syariah Indonesia (BSI) pada tahun 2023 menunjukkan bahwa tantangan keamanan siber di sektor perbankan semakin kompleks dan memerlukan persiapan teknis maupun moral dari para ahli teknologi informasi. Berdasarkan evaluasi yang dilakukan, dapat disimpulkan bahwa penerapan etika profesional teknologi informasi memainkan peran krusial dalam mencegah, menangani, dan mengatasi insiden keamanan digital.

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 3, Tahun 2025
ISSN 3024-8256 (media online)
Hal 573-576

Nilai-nilai seperti akuntabilitas, kejujuran, keahlian, dan perlindungan informasi harus menjadi landasan setiap kegiatan pengelolaan sistem data, terutama di lembaga keuangan yang sangat bergantung pada kepercayaan publik.

Insiden BSI menunjukkan bahwa meskipun langkah-langkah keamanan dasar telah diterapkan, masih terdapat celah dalam hal pengenalan ancaman, pengendalian kerentanan, dan kesiapan tanggap insiden. Hal ini menekankan bahwa spesialis TI tidak hanya diharapkan memiliki keterampilan teknis, tetapi juga dedikasi moral untuk memastikan kelangsungan operasional dan melindungi kepentingan pelanggan. Langkah-langkah pemulihan yang diambil oleh BSI, seperti kerja sama dengan lembaga pemerintah, isolasi sistem yang terdampak, dan penyebaran informasi kepada publik, merupakan manifestasi penerapan etika profesional IT yang menekankan tanggung jawab.

Oleh karena itu, memperkuat budaya moral, meningkatkan kemampuan sumber daya manusia di bidang IT, menerapkan standar keamanan sesuai dengan praktik terbaik, dan melakukan audit

UCAPAN TERIMA KASIH

Penulis mengucapkan syukur ke hadirat Tuhan Yang Maha Esa atas rahmat dan kemudahan yang diberikan sehingga penelitian ini dapat diselesaikan dengan baik. Penulis juga menyampaikan terima kasih kepada para dosen, pembimbing, dan seluruh pihak di lingkungan Program Studi Teknologi Informasi yang telah memberikan dukungan, arahan, serta masukan berharga selama proses penyusunan artikel ini. Ucapan terima kasih turut penulis sampaikan kepada rekan-rekan peneliti, praktisi, keluarga, dan sahabat yang senantiasa memberikan bantuan, motivasi, serta doa sehingga penelitian ini dapat terselesaikan dengan baik. Semoga kontribusi seluruh pihak menjadi amal yang bermanfaat dan penelitian ini dapat memberikan nilai tambah bagi pengembangan ilmu pengetahuan di bidang Teknologi Informasi.

REFERENCES

Anugrah, S. (2025). Prinsip etika profesi TI pada kasus serangan ransomware Bank Syariah Indonesia. Jurnal Universitas Komputer Indonesia.

Azarine, A. M. (2023). Bank BSI pasca serangan siber: Mengungkap potensi kompensasi bagi nasabah. LK2 FH UI.

Badan Siber dan Sandi Negara (BSSN). (2023). *Laporan Tahunan Keamanan Siber Indonesia 2023*. Jakarta: BSSN

Baldwin, A., Beresford, A., & Heath, R. (2021). *Ransomware: Understanding, Preventing, and Mitigating the Threats*. Journal of Cybersecurity, 7(1).

Gunawan, Y. (2025). Etika profesi dan kasus cyber crime di Indonesia. [Dokumen PDF].

Ismail, R., & Ramadhan, F. (2022). *Analisis Serangan Ransomware di Sektor Perbankan Indonesia*. Jurnal Keamanan Siber Nasional, 3(1), 14–25

Polim, P. (2023). Dampak serangan ransomware pada Bank Syariah Indonesia KCP Panglima Polim 1: Studi kasus. UPN Veteran Jakarta Repository.

Zebua, D. Y. (2025). Tantangan etika dalam profesi teknologi informasi. Siho Jurnal.