TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 2, Tahun 2025
ISSN 3024-8256 (media online)
Hal 302-305

Kebocoran Data BPJS sebagai Studi Kasus Kelemahan Keamanan Lembaga Publik

Aris Munandar [1*], Desi Listiani[2], Farid Abdul Malik[3], Bimo Aria Pratama[4], Annisa Elfina Augustia[5]

[1,2,3,4,5]Fakultas Teknik dan Ilmu Komputer, Teknik Informatika, Universitas Indraprasta PGRI, Jakarta, Indonesia
Email: [1*]arismunandar868am@gmail.com, [2]dlistiani08@gmail.com, [3]fabdulmalik75@gmail.com, [4]bimogans28@gmail.com, [5]annisa12elfina@gmail.com
(* : coressponding author)

Abstrak−Insiden kebocoran data massal yang menimpa Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan telah mengungkap kerapuhan sistemik dalam arsitektur keamanan siber lembaga publik Indonesia. Peristiwa yang diduga mengkompromikan data sensitif puluhan juta peserta ini bukan hanya sekadar pelanggaran privasi, tetapi merupakan gejala dari masalah mendalam yang mencakup aspek teknis, manajerial, regulasi, dan sumber daya manusia. Penelitian ini bertujuan untuk melakukan analisis komprehensif terhadap akar penyebab kebocoran data BPJS Kesehatan melalui pendekatan studi literatur dan analisis konten kritis terhadap laporan investigasi, pemberitaan media, dan studi kasus serupa. Hasil penelitian mengidentifikasi multifaktor kegagalan, termasuk infrastruktur teknologi yang kedaluwarsa, tata kelola data yang lemah, rendahnya kesadaran keamanan siber, serta lingkungan regulasi yang belum sepenuhnya efektif. Temuan penelitian ini menyoroti urgensi penerapan kerangka kerja *governance, risk, and compliance* (GRC) yang terintegrasi, peningkatan kapabilitas digital resilience, dan pembangunan budaya keamanan siber di seluruh level organisasi publik. Studi ini diharapkan dapat menjadi bahan pertimbangan bagi pembuat kebijakan dan praktisi TI dalam merancang strategi pertahanan siber yang lebih proaktif dan holistik untuk lembaga publik di Indonesia.

Kata Kunci: Kebocoran Data; BPJS Kesehatan; Keamanan Siber; Tata Kelola Data; Lembaga Publik.

Abstract−*The massive data breach incident experienced by the Social Security Administering Body (BPJS) for Health has revealed systemic fragility in the cybersecurity architecture of Indonesian public institutions. This incident, which allegedly compromised the sensitive data of tens of millions of participants, is not merely a privacy violation but a symptom of profound problems encompassing technical, managerial, regulatory, and human resource aspects. This study aims to conduct a comprehensive analysis of the root causes of the BPJS Health data breach through a literature study approach and critical content analysis of investigation reports, media coverage, and similar case studies. The results identify multifactor failures, including outdated technological infrastructure, weak data governance, low cybersecurity awareness, and a regulatory environment that is not yet fully effective. The findings highlight the urgency of implementing an integrated governance, risk, and compliance (GRC) framework, enhancing digital resilience capabilities, and building a cybersecurity culture at all levels of public organizations. This study is expected to be a consideration for policymakers and IT practitioners in designing more proactive and holistic cyber defense strategies for public institutions in Indonesia.*

Keywords: *Data Breach, BPJS Health, Cybersecurity, Data Governance, Public Institutions.*

1. PENDAHULUAN

Era digital dan ekonomi data telah mentransformasi cara negara memberikan pelayanan publik. Lembaga-lembaga publik, seperti Badan Penyelenggara Jaminan Sosial (BPJS) Kesehatan, kini menjadi repositori data pribadi dalam skala masif, menyimpan informasi sensitif jutaan warga negara. Data yang dikelola tidak hanya terbatas pada nama dan alamat, tetapi mencakup Nomor Induk Kependudukan (NIK), riwayat kesehatan, dan data biometrik yang memiliki nilai sangat tinggi di pasar gelap siber (CISSReC, 2023). Nilai strategis data ini menjadikan lembaga publik sebagai target primer serangan siber yang semakin sophisticated.

Ironisnya, di balik tanggung jawab besar tersebut, tingkat kematangan keamanan siber di banyak lembaga publik Indonesia masih tertinggal. Insiden kebocoran data BPJS Kesehatan yang terungkap pada tahun 2023 merupakan sebuah *wake-up call* yang menggemparkan. Data puluhan juta peserta diduga dieksfiltrasi dan diperjualbelikan secara bebas di forum-forum *dark web*, menimbulkan kepanikan dan rasa tidak aman di tingkat masyarakat (Kompas, 2023). Dampak dari insiden ini bersifat multidimensi: secara individu, korban rentan terhadap penipuan, pemalsuan

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 2, Tahun 2025
ISSN 3024-8256 (media online)
Hal 302-305

identitas, dan pemerasan; secara kolektif, insiden ini menggerogoti kepercayaan publik (*public trust*) terhadap kapasitas negara dalam melindungi aset digital warganya (Prasetyo, 2024).

Beberapa analisis awal menunjuk pada kelemahan teknis sebagai biang keladi. Namun, pendekatan yang hanya berfokus pada aspek teknis dinilai terlalu simplistis. Penelitian oleh Whitman & Mattord (2022) menegaskan bahwa keamanan informasi adalah masalah manajemen, bukan semata-mata masalah teknologi. Kegagalan seringkali berakar dari tata kelola yang buruk, prosedur yang lemah, dan budaya organisasi yang mengabaikan prinsip-prinsip keamanan. Oleh karena itu, diperlukan pendekatan holistik untuk memahami mengapa insiden serupa dapat terulang.

2. METODE PENELITIAN

2.1 Tahapan Model Penelitian

Penelitian ini menggunakan paradigma kualitatif dengan pendekatan studi kasus intrinsik, di mana kasus kebocoran data BPJS Kesehatan dipelajari secara mendalam untuk memahami dinamika dan kompleksitasnya yang unik (Creswell, 2014). Pendekatan ini dipilih karena mampu mengungkap konteks dan makna di balik sebuah fenomena sosial-teknis.

2.2 Sumber dan Teknik Pengumpulan Data

Mengingat sensitivitas data primer, penelitian ini mengandalkan data sekunder yang kredibel dan terpublikasi. Teknik pengumpulan data dilakukan melalui:

1. Dokumentasi: Meliputi laporan analisis forensik digital dari lembaga independen seperti CISSReC, siaran pers resmi dari BPJS Kesehatan dan Kementerian Kominfo, serta artikel investigasi dari media massa terpercaya (Kompas, Tempo).
2. Kajian Literatur Akademik: Tinjauan terhadap jurnal-jurnal nasional dan internasional yang membahas tata kelola keamanan informasi, manajemen risiko siber di sektor publik, dan studi kasus kebocoran data serupa di negara lain.
3. Analisis Kebijakan:* Mengkaji regulasi yang relevan, terutama Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP) dan peraturan turunannya, serta standar keamanan informasi seperti SNI ISO/IEC 27001.

2.3 Teknik Analisis Data

Data yang telah terkumpul dianalisis menggunakan teknik analisis isi kualitatif (*qualitative content analysis*) model Miles dan Huberman (1994), yang meliputi tiga tahap utama:

1. Reduksi Data: Menyeleksi, memfokuskan, dan menyederhanakan data dari berbagai sumber untuk mendapatkan informasi yang paling relevan dengan pertanyaan penelitian.
2. Penyajian Data: Menyusun data yang telah direduksi ke dalam matriks atau narasi yang terstruktur berdasarkan tema-tema kunci, seperti: Faktor Teknologi, Faktor Manajemen, Faktor Hukum dan Regulasi, serta Faktor Manusia.
3. Penarikan Kesimpulan dan Verifikasi: Menarik kesimpulan awal berdasarkan pola yang ditemukan, kemudian melakukan verifikasi melalui triangulasi sumber (membandingkan temuan dari media, laporan ahli, dan literatur akademik) untuk memastikan validitas dan reliabilitas temuan.

3. ANALISA DAN PEMBAHASAN

3.1 Kerentanan Infrastruktur Teknologi dan Keamanan yang Fatal

Pada lapisan teknis, beberapa kelemahan kritis teridentifikasi. Pertama, diduga kuat terdapat penggunaan sistem dan basis data yang sudah kedaluwarsa (*legacy systems*) yang tidak lagi mendukung patch keamanan terbaru. Sistem seperti ini memiliki *vulnerability* yang telah diketahui luas oleh komunitas peretas (Majalah TI, 2023). Kedua, penerapan enkripsi data, khususnya untuk data yang *at-rest* (disimpan) dan *in-transit* (dikirim), diduga tidak optimal atau bahkan tidak diimplementasikan pada segmen data tertentu. Hal ini mempermudah penyerang untuk membaca data yang berhasil dieksfiltrasi. Ketiga, kurangnya sistem pemantauan keamanan (*Security Operations Center*/SOC) yang proaktif membuat ancaman tidak terdeteksi dalam waktu yang lama,

TEKNOBIS : Teknologi, Bisnis Dan Pendidikan
Volume 3, No. 2, Tahun 2025
ISSN 3024-8256 (media online)
Hal 302-305

memberikan ruang gerak yang luas bagi pelaku untuk mengakses dan mencuri data (Shorouq & Hammad, 2024).

3.2 Tata Kelola dan Manajemen Risiko yang Tidak Efektif

Kelemahan teknis seringkali hanya merupakan gejala dari penyakit manajerial yang lebih dalam. Hasil analisis menunjukkan praktik tata kelola data (*data governance*) yang lemah di BPJS Kesehatan.

1. Kebijakan Akses yang Longgar: Prinsip *least privilege* (memberikan akses seminimal mungkin yang diperlukan untuk menjalankan tugas) tidak diterapkan secara konsisten. Banyak pengguna, termasuk pihak ketiga (vendor), yang memiliki akses berlebih ke basis data utama.
2. Manajemen Identitas dan Akses yang Buruk: Praktik berbagi kredensial login (*username/password*) diduga masih terjadi, sehingga menyulitkan proses audit dan akuntabilitas ketika terjadi insiden (Dewanta, 2024).
3. Audit Keamanan yang Tidak Rutin dan Superfisial:* Kegiatan audit internal dan eksternal mungkin tidak menjangkau aspek keamanan secara mendalam, sehingga celah-celah kritis tidak teridentifikasi dan tidak diperbaiki tepat waktu. Kerangka *Governance, Risk, and Compliance* (GRC) belum diadopsi secara menyeluruh untuk mengelola risiko siber secara terstruktur.

3.3 Tantangan dalam Penerapan Regulasi dan Penegakan Hukum

Keberadaan Undang-Undang Pelindungan Data Pribadi (UU PDP) merupakan langkah maju, namun efektivitasnya di lapangan masih dipertanyakan. Pada saat insiden terjadi, peraturan pelaksanaan (PP) dari UU PDP belum sepenuhnya rampung, menimbulkan ketidakpastian dalam implementasi. Selain itu, kapasitas institusi pengawas, seperti Otoritas Pelindungan Data Pribadi, masih dalam tahap penguatan. Sanksi yang tegas dan proses penegakan hukum yang cepat terhadap pelanggaran data juga belum terlihat, sehingga belum menimbulkan efek jera (*deterrent effect*) yang signifikan bagi organisasi yang lalai.

3.4 Faktor Manusia sebagai Mata Rantai Terlemah

Terlepas dari semua teknologi dan regulasi, faktor manusia tetap menjadi komponen paling rentan. Rendahnya *cybersecurity awareness* di kalangan pegawai dan mitra kerja menjadi pintu masuk serangan social engineering, seperti *phishing* yang dirancang untuk mencuri kredensial. Pelatihan keamanan siber yang berkelanjutan dan program simulasi *phishing* belum menjadi budaya wajib dalam organisasi. Akibatnya, kewaspadaan terhadap ancaman siber yang terus berkembang sangat minim (Hadlington, 2024).

3.5 Dampak Sosial dan Ekonomi yang Berkepanjangan

Dampak dari kebocoran ini melampaui dunia digital. Secara sosial, timbul rasa ketidakpercayaan dan kekecewaan masyarakat terhadap negara. Secara ekonomi, data kesehatan yang bocor dapat disalahgunakan oleh perusahaan asuransi untuk menolak nasabah dengan riwayat penyakit tertentu (*pre-existing condition*), atau oleh pihak tertentu untuk memeras individu yang memiliki riwayat penyakit sensitif. Pemulihan kepercayaan publik (*public trust*) membutuhkan waktu dan usaha yang jauh lebih besar daripada memulihkan sistem yang diretas.

4. KESIMPULAN

Berdasarkan analisis komprehensif yang telah dilakukan, dapat disimpulkan bahwa kebocoran data BPJS Kesehatan merupakan hasil dari kegagalan sistemik multidimensi. Kerentanan pada lapisan infrastruktur teknologi diperparah oleh tata kelola data dan manajemen risiko yang lemah, diperburuk oleh lingkungan regulasi yang belum matang, dan dimanfaatkan melalui celah kelemahan sumber daya manusia. Insiden ini bukanlah sebuah kejadian yang terisolasi, melainkan cerminan dari tantangan keamanan siber yang dihadapi oleh banyak lembaga publik di Indonesia.

Untuk membangun ketahanan siber (*cyber resilience*) yang tangguh dan mencegah terulangnya insiden serupa, berikut adalah rekomendasi yang dapat dipertimbangkan:

1. Untuk Lembaga Publik (Khususnya BPJS Kesehatan):

a. Modernisasi Infrastruktur: Melakukan percepatan migrasi dari *legacy systems* ke platform yang lebih modern dan aman, dengan menerapkan enkripsi end-to-end dan sistem deteksi intrusi yang canggih.
b. Memperkuat Tata Kelola Data: Menerapkan kerangka *Data Governance* yang jelas, termasuk penerapan prinsip *least privilege dan segregation of duties*, serta melakukan audit keamanan secara berkala dan independen.
c. Membangun Budaya Keamanan Siber: Menyelenggarakan program pelatihan dan kesadaran keamanan siber yang berkelanjutan dan wajib bagi semua pegawai dan mitra, termasuk simulasi serangan phishing.

2. Untuk Pemerintah dan Regulator:
   a. Mempercepat Implementasi UU PDP: Segera menyelesaikan dan mensosialisasikan seluruh peraturan pelaksanaan UU PDP, serta memperkuat kapasitas dan kewenangan Otoritas Pelindungan Data Pribadi.
   b. Mewajibkan Standar Keamanan: Mewajibkan penerapan standar keamanan informasi seperti SNI ISO/IEC 27001 untuk semua lembaga publik yang mengelola data dalam skala besar.
   c. Mendorong Kolaborasi: Memfasilitasi sharing intelligence ancaman siber antar lembaga pemerintah dan dengan *Computer Security Incident Response Team* (CSIRT) nasional.

Dengan implementasi rekomendasi yang komprehensif dan berkelanjutan, diharapkan lembaga-lembaga publik di Indonesia dapat bertransformasi menjadi entitas yang tidak hanya efisien dalam pelayanan, tetapi juga tangguh dan terpercaya dalam melindungi aset data digital warganya.

UCAPAN TERIMA KASIH

Puji syukur penulis panjatkan kehadirat Tuhan Yang Maha Kuasa, yang dengan Rahmat dan Ridha-nya, sehingga dapat menyelesaikan penyusunan *paper* dengan judul "Kebocoran Data BPJS sebagai Studi Kasus Kelemahan Keamanan Siber Lembaga Publik" dengan lancar.

Penulis juga mengucapkan Terimakasih banyak kepada dosen mata kuliah Etika Profesi, yang telah banyak memberikan membantuan dikala penulis buntu, ilmu dan segala masukan selama proses pembelajaran hingga tersusunnya *paper* ini, terimakasih juga kepada seluruh rekan dan keluarga yang terlah memberikan dukungan, berupa referensi, ide ,dan motivasi yg membantu dalam penyusunan *paper* ini.

Penulis sangat menyadari bahwa masih banyak kekurangan dalam *paper* ini. Oleh karena itu, penulis menerima kritik dan saran yang diharapkan dapat memperbaiki kekurangan kedepannya. Semoga *paper* ini dapat bermanfaat dan berguna bagi pembaca dan menambah wawasan dalam memahami tragedi kebocoran data ini.

REFERENCES

CISSReC. (2023). *Laporan Analisis Akhir Insiden Kebocoran Data BPJS Kesehatan 2023*. Pusat Studi Keamanan Siber dan Forensik Digital.

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (4th ed.). SAGE Publications.

Dewanta, A. S. (2024). *Human Factor dalam Keamanan Siber: Analisis Perilaku Pegawai pada Lembaga Pemerintah*. Jurnal Teknologi dan Ilmu Komputer, 5(1), 112-125.

Hadlington, L. (2024). *The "Human Factor" in Cybersecurity: Exploring the Role of Personality, Attitudes, and Behavior*. In Psychology of Cybersecurity (pp. 45-62). Academic Press.

Kompas. (2023). *Data BPJS Kesehatan Diduga Bocor, Berisi Informasi Sensitif Jutaan Peserta*. Kompas.com

Majalah TI. (2023). *Membedah Kerentanan Sistem yang Diduga Picu Kebocoran Data BPJS.* MajalahTI.co.id.

Miles, M. B., & Huberman, A. M. (1994*). Qualitative Data Analysis: An Expanded Sourcebook* (2nd ed.). SAGE Publications.

Prasetyo, A. (2024). *Tata Kelola Keamanan Informasi di Sektor Publik: Refleksi dari Kasus BPJS*. Jurnal Sistem Informasi Indonesia, 10(2), 45-60.

Shorouq, F., & Hammad, R. (2024). *The Role of Security Operations Centers (SOCs) in Mitigating Data Breach Risks in Healthcare Institutions*. *International Journal of Advanced Computer Science and Applications*, 15(3), 200-208.

Whitman, M. E., & Mattord, H. J. (2022). *Principles of Information Security* (7th ed.). Cengage Learning.