BIN : Bulletin Of Informatics
Volume 3, No. 1 Juli 2025
ISSN 3025-7417 (media online)
Hal 85-89

Studi Kasus Serangan *Ransomware Brain Cipher* pada Pusat Data Nasional Indonesia

Irfan Armansyah[1], Yusran Tabrani[2], Muhammad Sonadida Khoir[3], Dodo Wibowo Putra[4], Annisa Elfina Augustia[5]

[1-5] Prodi Teknik Informatika, Fakultas Teknik dan Ilmu Komputer, Universitas Indraprasta (PGRI)
Email: [1]Irfanarmansyah701@gmail.com, [2]yusrantabrani6@gmail.com, [3]Sonadida0@gmail.com, [4]dodowibowo1212@gmail.com, [5]annisa12elfina@gmail.com

Abstrak−Insiden *ransomware Brain Cipher* di Pusat Data Nasional Sementara (PDNS) Indonesia pada Juni 2024 adalah serangan siber terpenting yang mengincar infrastruktur penting pemerintah, menghentikan ratusan layanan publik krusial dan menunjukkan kelemahan serius dalam sistem data nasional. Studi kasus kualitatif ini bertujuan untuk menganalisis secara menyeluruh kronologi serangan, metode operasional *Brain Cipher* sebagai varian LockBit 3.0, serta menilai dampak finansial, sosial, dan implikasi kebijakan keamanan siber di Indonesia, dengan data yang diperoleh melalui analisis literatur, laporan resmi BSSN, dan artikel berita yang dapat dipercaya. Analisis menunjukkan bahwa serangan mampu menembus sistem karena kombinasi kerentanan perangkat lunak yang usang dan pengaturan keamanan yang tidak memadai, diperburuk oleh kekurangan mendasar dalam pengelolaan risiko, seperti tiadanya sistem pencadangan data yang efisien. Serangan ini menunjukkan bahwa ketahanan siber Indonesia berada pada tingkat rentan sistemik dan membutuhkan reformasi dalam pengelolaan yang mencakup investasi infrastruktur keamanan siber modern, penerapan protokol cadangan dan pemulihan bencana yang wajib, serta perbaikan kapasitas dan budaya keamanan siber di seluruh lembaga pemerintah.

Kata Kunci: *Brain Cipher Ransomware*; Pusat Data Nasional; keamanan siber; kasus studi; infrastruktur kritis.

Abstract−*The Brain Cipher ransomware event at Indonesia's Temporary National Data Center (NDCS) in June 2024 marks the most notable cyber assault on essential governmental infrastructure, immobilizing numerous crucial public services and revealing significant weaknesses in the national data framework. This qualitative case study thoroughly examines the timeline of the attack, the operational methods of Brain Cipher as a variant of LockBit 3.0, and assesses the financial, social, and policy impacts on Indonesia's cybersecurity, utilizing information obtained from literature review, official BSSN documents, and credible news sources. Analysis findings reveal that the attack successfully compromised the system due to a mix of outdated software vulnerabilities and inadequate security settings, worsened by inherent flaws in risk management, including insufficient data backup systems. The analysis determines that Indonesia's cyber resilience is characterized by systemic vulnerability and necessitates governance reforms, including immediate investment in advanced cybersecurity infrastructure, compulsory establishment of strong backup and disaster recovery procedures, and a considerable enhancement of cybersecurity capabilities and culture throughout all government departments.*

Keywords: *Brain Cipher Ransomware; National Data Hub; cybersecurity; case analysis; essential infrastructure*

1. PENDAHULUAN

Isu keamanan siber kini menjadi tantangan fundamental bagi transformasi *digital* secara global, dengan insiden ransomware meningkat secara signifikan baik dalam frekuensi maupun dampaknya, terutama yang menyasar infrastruktur penting negara (Syarifa, 2024). Keamanan informasi dan keberlangsungan layanan publik saat ini sangat tergantung pada posisi pertahanan siber nasional (Hendrawan, 2023). Di Indonesia, percepatan penerapan Sistem Pemerintahan Berbasis Elektronik (SPBE) sangat terikat pada keandalan serta keamanan Pusat Data Nasional (PDN) yang menjadi fondasi penyimpanan dan pengelolaan data strategis pemerintah (Perpres No. 82, 2022)

Akan tetapi, infrastruktur digital negara ini menghadapi kejutan besar pada pertengahan Juni 2024 saat Pusat Data Nasional Sementara (PDNS) diserang oleh serangan siber yang luas (CNN Indonesia, 25 Juni 2024). Serangan yang dikenali sebagai *Brain Cipher Ransomware (BCR)* sebuah varian lebih lanjut dari *LockBit* 3.0 telah berhasil mengacaukan lebih dari 210 lembaga pemerintah, termasuk layanan penting seperti imigrasi, serta meminta tebusan dalam angka yang signifikan (BSSN, 2024). Peristiwa ini tidak hanya menyebabkan kerugian finansial besar dan gangguan layanan publik secara luas (Kompas, 27 Juni 2024), tetapi juga secara mendasar menyingkap

BIN : Bulletin Of Informatics
Volume 3, No. 1 Juli 2025
ISSN 3025-7417 (media online)
Hal 85-89

kerentanan sistemik, baik dari segi teknis maupun manajerial, dalam pengelolaan keamanan siber nasional.

Walaupun laporan media dan analisis awal telah menjelaskan kronologi serangan serta dampak teknis yang tampak (Al Ihsan & Sekti, 2024), masih sedikit penelitian akademis yang secara menyeluruh mengkaji faktor-faktor sistemik yang menyebabkan kegagalan pertahanan siber PDN serta mengevaluasi akibat kebijakan jangka panjang terhadap ketahanan siber infrastruktur kritis di Indonesia (Syarifa, 2024). Penelitian studi kasus kualitatif ini bertujuan untuk mengatasi kesenjangan tersebut dengan mengeksplorasi cara kerja *Brain Cipher* serta pengaruh insiden ini terhadap perubahan kebijakan dan pengelolaan risiko keamanan siber dalam lingkungan pemerintah

Mengacu pada latar belakang, pentingnya isu, dan kekurangan penelitian yang telah dijelaskan, studi ini merumuskan isu-isu utama sebagai berikut:

1. Apa urutan peristiwa serangan *Brain Cipher Ransomware* dalam memanfaatkan kelemahan sistem yang ada?
2. Apa saja faktor-faktor sistemik (teknis dan manajerial) yang menyebabkan kegagalan pertahanan siber PDNS?
3. Apa dampak dari serangan ini terhadap reformasi manajemen dan strategi pengurangan risiko keamanan siber infrastruktur vital di Indonesia?

Tujuan dari penelitian ini meliputi: Menganalisis dengan mendetail urutan kejadian dan cara pelaksanaan serangan, mengidentifikasi faktor sistemik yang menyebabkan kegagalan keamanan siber pada PDNS, serta merumuskan rekomendasi kebijakan untuk meningkatkan ketahanan siber infrastruktur kritis di Indonesia setelah insiden.

2. METODE

Penelitian ini menggunakan pendekatan studi kasus tunggal dengan metode penelitian kualitatif. Metode ini dipilih karena bertujuan untuk memberikan pemahaman yang mendetail dan menyeluruh terhadap satu fenomena kontemporer yang unik dan penting, yaitu insiden serangan *Brain Cipher Ransomware* di Pusat Data Nasional Sementara (PDNS) Indonesia pada bulan Juni 2024. Studi kasus ini memungkinkan analisis penyebab utama, konteks sistemik, serta implikasi kebijakan yang lebih mendalam dibandingkan dengan pendekatan kuantitatif.

a. Satuan dan Lokasi Analisis
   Unit analisis dalam penelitian ini adalah Insiden Serangan *Ransomware Brain Cipher* terhadap PDNS. Lokus penelitian mengutamakan sistem keamanan siber dan struktur pengelolaan keamanan informasi pada infrastruktur informasi penting pemerintah Indonesia.
b. Asal dan Kategori Data
   Data yang dipakai dalam studi ini bersifat kualitatif dan dibedakan menjadi dua kategori:
   a. Data Primer (Dokumen Resmi): Termasuk laporan resmi dari Badan Siber dan Sandi Negara (BSSN) serta Kementerian Komunikasi dan Informatika (Kominfo) mengenai hasil penyelidikan insiden, serta dokumen regulasi pemerintah yang relevan (contohnya, Peraturan Presiden tentang SPBE dan Perlindungan Infrastruktur Informasi Vital).
   b. Data Sekunder (Kajian Literatur): Terdiri dari artikel jurnal akademik, prosiding konferensi, laporan analisis dari pakar keamanan siber, serta artikel berita dari media yang dapat dipercaya yang membahas urutan peristiwa, cara kerja *Brain Cipher* (varian LockBit 3.0), serta faktor-faktor sistemik dan konsekuensi hukum setelah serangan.
a. Metode Pengumpulan dan Analisis Data
   Metode pengumpulan data utama adalah Tinjauan Pustaka (*Literature Review*) dan Analisis Dokumen. Analisis data dilakukan secara terstruktur melalui tiga langkah utama yang diambil dari metode analisis kualitatif.
   1. Pengurangan Data (Data *Reduction*): Data faktual (kronologi serangan, jenis ransomware, dan pernyataan resmi) dipilah dan diarahkan pada penemuan yang berkaitan dengan tiga rumusan masalah: modus operandi, faktor sistemik (teknis/manajerial), serta akibat kebijakan.

BIN : Bulletin Of Informatics
Volume 3, No. 1 Juli 2025
ISSN 3025-7417 (media online)
Hal 85-89

2. Penyajian Data (Data *Presentation*): Hasil disajikan secara naratif dan deskriptif untuk menjelaskan alur logis dari kejadian, faktor sistemik, serta saran yang diberikan.
3. Penarikan Kesimpulan (*Drawing Conclusions/Verification*): Peneliti menginterpretasikan dan memverifikasi temuan dengan membandingkannya dengan kerangka teori yang telah ada (seperti, teori Manajemen Risiko Keamanan Informasi dan prinsip Manajemen Kelangsungan Bisnis). Metode analisis yang diterapkan adalah Analisis Isi untuk mengenali pola-pola kegagalan dan Analisis Tematik untuk mengategorikan faktor-faktor sistemik (teknis, manajerial, kebijakan) yang berperan dalam insiden tersebut, dengan tujuan menghasilkan rekomendasi yang sahih.

3. ANALISA DAN PEMBAHASAN

3.1 Kronologi dan Metode Operasi *Ransomware Brain Cipher*

Analisis kronologis yang dilakukan (berdasarkan laporan BSSN, 2024 dan Al Ihsan & Sekti, 2024) membuktikan bahwa serangan yang menyasar PDNS di Surabaya pada Juni 2024 dilakukan oleh *Brain Cipher Ransomware (BCR)*, adalah varian terbaru dari grup kejahatan siber LockBit 3.0. Peristiwa ini terjadi dalam beberapa fase penting:

1. Akses Awal (*Initial Access*): Akses awal diduga diperoleh melalui eksploitasi kerentanan pada sistem warisan (*legacy system*) yang tidak diperbarui (*unpatched*) atau melalui protokol *Remote Desktop Protocol (RDP)* yang rentan (CNN Indonesia, 2024). Berbagai laporan juga menekankan kemungkinan fungsi Initial Access Brokers (IABs) dalam memberikan kredensial untuk akses internal (Kompas, 2024).
2. Penetapan Keberadaan dan Disabilitas Keamanan: Setelah berhasil mengakses, malware BCR dilaporkan menonaktifkan perlindungan siber dalam sistem, termasuk fitur penting seperti *Windows Defender*, untuk memastikan pergerakan lateral tanpa terdeteksi.
3. Eksfiltrasi Data dan Enkripsi: BCR menerapkan metode Pemerasan Ganda. Langkah awal mencakup pengambilan data sensitif (ekfiltrasi). Tahap kedua melibatkan enkripsi menyeluruh data di PDNS, mengakibatkan ratusan layanan publik terhenti sepenuhnya.

Cara kerja BCR menunjukkan perkembangan ancaman *ransomware* dari sekadar enkripsi menjadi kombinasi antara pencurian dan penguncian data. Keberhasilan penetrasi mengindikasikan adanya kelemahan pada lapisan keamanan yang paling luar dan paling dalam. Kejadian ini sejalan dengan pola serangan yang dicatat dalam kerangka MITRE ATT&CK, khususnya pada teknik Menonaktifkan Alat Keamanan dan Menonaktifkan Pemulihan Sistem (Syarifa, 2024), yang menunjukkan bahwa pertahanan siber PDNS tidak dapat mendeteksi atau menghentikan aktivitas pasca-eksploitasi dari pelaku.

3.2 Analisis Elemen Sistemik Kegagalan Keamanan Siber PDNS

Temuan studi kasus mengindikasikan bahwa ketidakmampuan PDNS dalam menghadapi serangan *Brain Cipher Ransomware* tidak disebabkan oleh satu kerentanan teknis, melainkan merupakan akibat dari kelemahan sistemik yang terkonsolidasi di tiga bidang: teknis, manajerial, dan tata kelola. Secara teknis, hasil penelitian menunjukkan adanya pemakaian sistem operasi dan perangkat lunak lama yang rawan serta tidak berhasil dalam melakukan pembaruan keamanan secara rutin. Keadaan ini secara mendasar melanggar prinsip Manajemen Kerentanan yang ketat, yang merupakan penyimpangan besar dari standar keamanan informasi yang diwajibkan, seperti ISO 27001.

Akan tetapi, sumber permasalahan yang paling penting terdeteksi dalam ranah manajemen dan pengelolaan. Faktor utama adalah tidak adanya sistem cadangan data yang terpisah dan terisolasi (*backup air-gapped atau immutable*). Kegagalan ini mencerminkan rendahnya penerapan Manajemen Risiko dan Kelangsungan Bisnis (*Business Continuity Management/BCM*). Informasi yang didapat menunjukkan bahwa dasar prinsip backup 3-2-1 diabaikan, dengan data cadangan tetap terhubung ke jaringan utama sehingga terpengaruh enkripsi (Syarifa, 2024). Ini menjadikan pemulihan data tidak mungkin dilakukan tanpa membayar tebusan dan menunjukkan bahwa manajemen risiko PDNS tidak menganggap skenario serangan *ransomware* sebagai ancaman serius

BIN : Bulletin Of Informatics
Volume 3, No. 1 Juli 2025
ISSN 3025-7417 (media online)
Hal 85-89

3.3 Dampak Kebijakan dan Strategi Pengurangan Risiko Jangka Panjang

Temuan dari studi kasus ini menunjukkan tiga implikasi kebijakan strategis yang mendesak untuk keamanan siber nasional setelah serangan *Brain Cipher*.

1. Kegagalan Regulasi BCM: Insiden ini menunjukkan adanya celah dalam regulasi yang ada, di mana Perpres No. 82 Tahun 2022 mengenai Perlindungan Infrastruktur Informasi Vital (IIV) belum secara jelas mewajibkan dan memastikan penerapan BCM yang ketat, terutama backup yang terpisah, untuk data penting.
2. Erosi Kepercayaan Publik: Gangguan layanan publik yang meluas dan berkepanjangan telah secara signifikan merusak kepercayaan masyarakat terhadap kemampuan pemerintah dalam mengelola serta melindungi data sensitif mereka (Djafar, 2024). Ini menimbulkan pertanyaan mendalam tentang tanggung jawab data.
3. Kesalahan Prioritas Investasi: Insiden ini menegaskan bahwa pengalokasian anggaran dan prioritas investasi dalam keamanan siber selama ini bersifat reaktif dan tidak cukup untuk melindungi infrastruktur setara PDN.

Untuk menangani implikasi yang muncul tersebut, Indonesia perlu melakukan perubahan mendasar dari filosofi berbasis kepatuhan (hanya memenuhi aturan) ke filosofi ketahanan siber (berbasis ketahanan). Strategi mitigasi jangka panjang tidak boleh hanya fokus pada perbaikan teknis, melainkan perlu mencakup reformasi tata kelola dan investasi yang berkelanjutan.

a. Mandat *Resilience* dan Cadangan *Air-Gapped*: Diperlukan evaluasi ulang peraturan untuk mewajibkan penggunaan teknologi *immutable* atau cadangan *air-gapped* secara hukum untuk semua Infrastruktur Informasi Vital (IIV). Tanggung jawab ini harus dilaksanakan dengan audit independen secara rutin untuk memastikan kepatuhan yang ketat.
b. Peningkatan Kapasitas SDM dan Budaya Siber: Mengingat bahwa aspek manusia tetap menjadi kelemahan utama, alokasi dana untuk pelatihan mendalam bagi ASN dan Administrator Sistem harus diprioritaskan, dengan penekanan pada deteksi anomali, respons insiden yang cepat, dan kesadaran terhadap ancaman *phishing* serta ancaman dari dalam.
c. Integrasi Keamanan Lintas Sektor: Diperlukan sistem koordinasi yang lebih solid dan terpusat antara BSSN, Kominfo, dan lembaga pengelola data untuk menjamin adanya pertukaran *threat intelligence* yang efisien serta respons insiden yang terkoordinasi.

Melalui penerapan strategi mitigasi yang menyeluruh ini, serangan *Brain Cipher* bisa menjadi peluang signifikan untuk memperkuat basis digital nasional, bukan sekadar krisis yang berlalu begitu saja. Diskusi ini akan diakhiri dan disarankan dengan lebih rinci pada bagian akhir penelitian.

4. KESIMPULAN

Studi kasus kualitatif mengenai insiden serangan *Brain Cipher Ransomware* di Pusat Data Nasional Sementara (PDNS) pada Juni 2024 menegaskan bahwa kejadian ini bukan hanya kegagalan teknis, tetapi juga merupakan manifestasi dari kelemahan sistemik yang serius dalam pengelolaan keamanan siber nasional. Tiga poin utama yang menjawab pertanyaan dalam penelitian ini adalah:

1. Mengenai Kronologi dan Modus Operandi: Serangan dilakukan oleh *Brain Cipher Ransomware*, jenis *LockBit* 3.0, yang mengimplementasikan modus *Double Extortion* (pencurian data dan enkripsi). Kronologi memperlihatkan suksesnya pelaku dalam memanfaatkan sistem yang rentan (*unpatched legacy system*) serta dengan cermat menonaktifkan sistem pertahanan siber, yang menunjukkan adanya kelemahan besar pada lapisan pertahanan paling luar dan paling dalam infrastruktur PDNS.
2. Mengenai Faktor Sistemik Kegagalan: Penyebab utama yang berkontribusi pada kegagalan keamanan siber adalah isu manajerial dan pengelolaan, bukan hanya aspek teknis. Tidak adanya sistem pencadangan data yang terpisah (*air-gapped* atau immutable) menjadi masalah utama yang kritis, mencerminkan kegagalan mendasar dalam pelaksanaan Manajemen Keberlangsungan Bisnis (BCM) dan pengelolaan risiko yang kurang baik di level pengambilan keputusan. Kegagalan ini bertentangan dengan prinsip fundamental ketahanan siber.

BIN : Bulletin Of Informatics
Volume 3, No. 1 Juli 2025
ISSN 3025-7417 (media online)
Hal 85-89

3. Terkait dengan Implikasi Kebijakan dan Strategi Mitigasi: Serangan ini menunjukkan adanya kebutuhan mendesak untuk kebijakan, yang menggarisbawahi kekurangan regulasi yang khusus dan ketat terkait kewajiban ketahanan dan BCM pada Infrastruktur Informasi Vital (IIV). Untuk mitigasi jangka panjang, dibutuhkan pergeseran paradigma dari sekadar kepatuhan (*compliance*) menjadi ketahanan (*resilience*), dengan investasi wajib dalam cadangan yang terpisah, peningkatan anggaran keamanan siber yang bersifat proaktif, dan reformasi menyeluruh terhadap budaya keamanan siber di kalangan Aparatur Sipil Negara (ASN) serta pengelola data pemerintah.

Secara keseluruhan, kasus PDNS berperan sebagai tanda peringatan bagi Indonesia untuk menjadikan keamanan siber sebagai bagian penting dari kebijakan nasional dan reformasi digital

REFERENCES

Al Ihsan, R., & Sekti, B. A. (2024). Pentingnya Keamanan Data Dalam Era Digital: Refleksi Terhadap Serangan Hacker Pada Pusat Data Nasional Indonesia. *Prosiding SISFOTEK*, *8*(1), 45-58.

BSSN. (2024). *Laporan Singkat Hasil Investigasi Insiden Ransomware PDNS*. Badan Siber dan Sandi Negara.

CNN Indonesia. (2024, Juni 25). Kronologi hacker rebut kendali pusat data nasional diungkap. https://www.cnnindonesia.com/.

Djafar, W. (2024, Juni 27). *Serangan siber PDN dinilai semakin menggerus kepercayaan publik*. Kompas.com. [URL: https://nasional.kompas.com/read/2024/06/27/13590071/serangan-siber-pdn-dinilai-semakin-menggerus-kepercayaan-publik]

Hendrawan, K. (2023). Analisis Strategi Keamanan Siber Pada Infrastuktur Pemerintah Indonesia: Studi Kasus Pusat Data Nasional. *Jurnal Teknologi Informasi Dan Keamanan Siber*, *15*(3), 112-125.

Khoironi, S. C. (2020). Pengaruh analisis kebutuhan pelatihan budaya keamanan siber sebagai upaya pengembangan kompetensi bagi aparatur sipil negara di era digital. *Jurnal Studi Komunikasi dan Media*, *24*(1), 37–56.

Perpres No. 82 Tahun 2022 tentang Perlindungan Infrastruktur Informasi Vital (IIV). *Lembaran Negara Republik Indonesia Tahun 2022 Nomor 160*.

Syarifa, A. (2024). Evaluasi Manajemen Risiko Keamanan Siber pada Infrastruktur Digital Pemerintah: Studi Kasus Pusat Data Nasional (PDN). *Jurnal Manajemen dan Ekonomi Bisnis*, *10*(4), 88-102.