KAMPUS AKADEMIK PUBLISING
Jurnal Sains Student Research
Vol.2, No.6 Desember 2024
e-ISSN: 3025-9851; p-ISSN: 3025-986X, Hal 324-331
DOI: https://doi.org/10.61722/jssr.v2i6.2966

Ransomware pada Data PDN: Implikasi Etis dan Tanggung Jawab Profesional dalam Pengelolaan Keamanan Siber

Anastasya Simorangkir
Universitas Palangkaraya
Herlinda Sihombing
Universitas Palangkaraya
Putri Intani Sihite
Universitas Palangkaraya
Jadiaman Parhusip
Universitas Palangkaraya
Alamat: Jln. Yos Sudarso Palangka Raya Kalimantan Tengah, 73111
Korespondensi penulis: anatasyasimorangkir2020@gmail.com

Abstrak *Ransomware is a type of cyber attack that has become increasingly prevalent, particularly targeting sensitive data such as Personal Data and National Data (PDN). These attacks not only threaten the integrity and confidentiality of data but also raise significant ethical implications for professionals in the field of cybersecurity. This journal examines various aspects related to ransomware, from the mechanisms of attack to its impacts on individuals and organizations. Furthermore, it explores the professional responsibilities that cybersecurity experts must uphold in managing and preventing ransomware attacks. Through this analysis, the aim is to provide a better understanding of the importance of ethics in cybersecurity management and to encourage best practices for protecting PDN from evolving threats.*

Keywords: *Ransomware, Personal Data, Cybersecurity, Cyber Attacks*

Abstrak *Ransomware* merupakan salah satu jenis serangan siber yang semakin marak terjadi, terutama pada data penting seperti data Pribadi, Data Nasional (PDN). Serangan ini tidak hanya mengancam integritas dan kerahasiaan data, tetapi juga menimbulkan implikasi etis yang signifikan bagi para profesional di bidang keamanan siber. Jurnal ini membahas berbagai aspek terkait *ransomware*, mulai dari mekanisme serangan hingga dampaknya terhadap individu dan organisasi. Selain itu, jurnal ini mengeksplorasi tanggung jawab profesional yang harus diemban oleh para ahli keamanan siber dalam menangani dan mencegah serangan *ransomware.* Melalui analisis ini, diharapkan dapat memberikan pemahaman yang lebih baik mengenai pentingnya etika dalam pengelolaan keamanan siber, serta mendorong praktik terbaik untuk melindungi data PDN dari ancaman yang terus berkembang.

Kata Kunci*:* *Ransomware*, Data Pribadi, Keamanan Siber, Serangan Siber

PENDAHULUAN

Di era digital yang terus berkembang pesat, tantangan terhadap keamanan siber semakin kompleks dan beragam. Salah satu ancaman signifikan yang kini menjadi sorotan global adalah serangan ransomware. Ransomware adalah salah satu jenis malware yang bertujuan untuk mengenkripsi atau membatasi akses ke data maupun sistem komputer milik korban. Pelaku di balik serangan ini biasanya meminta tebusan dalam bentuk mata uang digital sebagai syarat untuk mengembalikan akses atau data kepada pemiliknya [1]. Kasus yang menggemparkan baru-baru ini adalah insiden serangan ransomware yang menargetkan Pusat Data Nasional (PDN) telah mengakibatkan terganggunya sejumlah layanan vital pemerintah, termasuk layanan keimigrasian [14].

Serangan ransomware terhadap Pusat Data Nasional (PDN) membawa dampak serius di berbagai aspek. Secara teknis, serangan ini menyebabkan hilangnya akses ke data penting,

Received September 30, 2024; Revised Oktober 31, 2024; Desember 02, 2024

gangguan pada layanan publik seperti administrasi kependudukan dan kesehatan, serta kerusakan pada infrastruktur IT, termasuk server dan jaringan. Dampak finansialnya mencakup tingginya biaya pemulihan data dan sistem, kerugian akibat gangguan operasional, serta potensi pembayaran tebusan yang hanya akan memperparah masalah dengan mendorong pelaku untuk mengulangi serangan. Dari sisi sosial, kepercayaan masyarakat terhadap keamanan data pemerintah terancam hilang, data sensitif terkait keamanan nasional menjadi rentan, dan gangguan layanan publik yang berkepanjangan dapat memicu ketidakstabilan sosial. Selain itu, reputasi pemerintah di mata internasional juga dapat terancam, sementara ketakutan akan serangan siber bisa menghambat pengembangan teknologi baru. [15]

Serangan *ransomware* pada PDN membawa implikasi etis yang mendalam. Di satu sisi, pemerintah memiliki tanggung jawab moral untuk melindungi data masyarakat yang dipercayakan kepada mereka. Namun, di sisi lain, kegagalan dalam mengelola risiko keamanan siber menunjukkan adanya celah dalam pengelolaan data dan infrastruktur IT. Hal ini memunculkan pertanyaan kritis tentang sejauh mana tanggung jawab profesional para pengelola IT dalam memastikan keamanan data. Kegagalan seperti ini tidak hanya berdampak pada kepercayaan masyarakat, tetapi juga pada reputasi pemerintah di tingkat internasional.

Penelitian ini bertujuan untuk analisis mendalam tentang implikasi etis dan tanggung jawab profesional yang menyertai serangan *ransomware* pada data PDN. Fokus utama penelitian ini adalah untuk menggali dampak serangan *ransomware* dari berbagai dimensi, termasuk dimensi teknis, sosial, dan etis, serta untuk menyoroti pentingnya pengelolaan risiko siber yang proaktif dalam mencegah insiden serupa di masa depan.

KAJIAN TEORITIS

Ransomware merupakan jenis perangkat lunak berbahaya yang mengenkripsi data dan menuntut pembayaran tebusan [4]. Serangan *ransomware* sering kali menargetkan data sensitif, termasuk data pribadi dan data nasional, yang dapat memiliki dampak luas terhadap keamanan dan privasi. Data pribadi mencakup informasi yang dapat digunakan untuk mengidentifikasi individu, seperti nama, alamat, nomor identitas, dan informasi keuangan.

Keamanan siber adalah praktik melindungi sistem komputer, jaringan, dan data dari serangan, kerusakan, atau akses yang tidak sah. Keamanan siber mencakup berbagai aspek, termasuk perlindungan data, manajemen risiko, dan respons terhadap insiden. Dalam konteks *ransomware*, keamanan siber berfokus pada pencegahan serangan, deteksi dini, dan pemulihan data yang terpengaruh [5].

Implikasi etis dalam keamanan siber mencakup tanggung jawab moral para profesional untuk melindungi data dan privasi individu. Etika dalam keamanan siber melibatkan pertimbangan tentang bagaimana teknologi dapat digunakan untuk kebaikan dan bagaimana risiko dapat diminimalkan. Para profesional di bidang ini harus mempertimbangkan dampak dari keputusan mereka terhadap individu dan masyarakat secara keseluruhan [6].

Tanggung jawab profesional dalam pengelolaan keamanan siber mencakup kewajiban untuk menjaga integritas dan kerahasiaan data, serta untuk melaporkan dan menangani insiden keamanan dengan cara yang transparan dan etis. Menurut kode etik yang ditetapkan oleh organisasi profesional seperti (ISC)² dan ISACA, para profesional

keamanan siber diharapkan untuk berkomitmen pada praktik terbaik dan untuk terus meningkatkan pengetahuan dan keterampilan mereka dalam menghadapi ancaman yang terus berkembang [6].

Praktik terbaik dalam mengelola ransomware meliputi penerapan kebijakan keamanan yang ketat, pelatihan karyawan tentang kesadaran keamanan, dan penggunaan teknologi enkripsi dan cadangan data. Menurut Cybersecurity & Infrastructure Security Agency (CISA), organisasi harus memiliki rencana respons insiden yang jelas dan melakukan simulasi untuk memastikan kesiapan dalam menghadapi serangan ransomware [7].

METODE PENELITIAN

Metode yang digunakan dalam penelitian Implikasi Etis dan Tanggung Jawab Profesional dalam Pengelolaan Keamanan Siber ini adalah metode kualitatif, karena metode kualitatif adalah pendekatan penelitian yang bertujuan untuk memahami fenomena sosial atau isu-isu kompleks dari sudut pandang yang mendalam dan beragam atau analisis konten. Metode ini berfokus pada eksplorasi, pemahaman, dan interpretasi makna di balik suatu kejadian atau perilaku. Dalam konteks penelitian "Ransomware pada Data PDN: Implikasi Etis dan Tanggung Jawab Profesional dalam Pengelolaan Keamanan Siber", metode ini membantu peneliti memahami bagaimana para profesional keamanan siber dan ahli etika berinteraksi dengan isu-isu etis dan tanggung jawab mereka ketika menghadapi ancaman siber, khususnya *ransomware*. Pendekatan dengan metode analisis konten digunakan untuk menganalisis data sekunder yang berasal dari sumber-sumber yang terpercaya, seperti jurnal-jurnal, buku, artikel dan situs website. Sampel sumber data yang digunakan dalam penelitian ini adalah jurnal jurnal, artikel dan situs yang terpercaya.

HASIL PENELITIAN DAN PEMBAHASAN

Pada bulan Juni 2024, Pusat Data Nasional (PDN) Indonesia mengalami serangan *ransomware* yang signifikan, yang mengakibatkan dampak luas terhadap berbagai layanan publik. Serangan ini dimulai dengan infiltrasi ke dalam sistem PDN dan berlanjut dengan proses enkripsi data penting. *Brain Cipher* adalah varian *ransomware* yang telah menyebabkan kerusakan besar pada Pusat Data Nasional (PDN) Indonesia. *Ransomware* ini memanfaatkan beragam metode untuk menembus sistem dan mengenkripsi data yang ada. Berikut adalah alur kerjanya:

No	Langkah	Deskripsi
1	Infeksi Awal	Brain Cipher masuk ke sistem target melalui metode infiltrasi seperti email phishing atau lampiran berbahaya [12].
2	Penonaktifan Keamanan	Setelah infiltrasi, ransomware menonaktifkan fitur keamanan seperti Windows Defender, memungkinkan aktivitas berbahaya berjalan tanpa terdeteksi [8].
3	Enkripsi Data	Ransomware mulai mengenkripsi file di komputer korban menggunakan algoritma enkripsi yang kuat, sehingga data menjadi tidak dapat diakses [12].

4	Penghapusan File Sistem	Menghapus filesystem penting untuk menghilangkan jejak dan mencegah pemulihan data oleh korban [10].
5	Permintaan Tebusan	Setelah semua file dienkripsi, Brain Cipher menampilkan pesan tebusan yang meminta pembayaran dalam bentuk cryptocurrency untuk mendapatkan kunci dekripsi [12].
6	Eksfiltrasi Data	Ransomware mencuri informasi sensitif dan kredensial dari sistem, memberikan penyerang akses lebih lanjut ke jaringan [11].
7	Ancaman Publikasi	Jika tebusan tidak dibayarkan, penyerang mengancam akan merilis data yang dicuri ke publik, meningkatkan tekanan pada korban untuk membayar [13].

Berikut kronologi peristiwa tersebut.

Tanggal & Waktu	Aktivitas
17 Juni 2024, 23:15 WIB	Upaya awal untuk menonaktifkan fitur keamanan Windows Defender dilakukan, membuka celah bagi aktivitas berbahaya [3].
18 Juni 2024, 03:21 WIB	Serangan ransomware memasuki tahap awal dengan penambahan akun pengguna baru pada sistem PDN [5].
19 Juni 2024, 22:18 WIB	Kegiatan serangan terus berlanjut melalui berbagai metode infiltrasi ke dalam sistem PDN [5].
20 Juni 2024, 00:54 WIB	Fitur *directory backup* dinonaktifkan oleh pengguna baru yang telah berhasil masuk ke dalam sistem [5].
20 Juni 2024, 00:57 WIB	Ransomware kemudian dijalankan pada perangkat *backup* di PDN, mengenkripsi data penting yang tersimpan [5].
20 Juni 2024	Pelaku menuntut uang tebusan sebesar USD 8 juta sebagai syarat untuk memulihkan akses terhadap data yang telah terkunci [6].
23 Juni 2024	Serangan ini mulai berdampak pada gangguan layanan publik, termasuk layanan imigrasi dan kesehatan [9].
27 Juni 2024	Pemerintah melaporkan bahwa beberapa tenant yang terdampak telah berhasil memulihkan layanan mereka secara bertahap [5].

Serangan *ransomware* ini memiliki dampak signifikan, memengaruhi lebih dari 200 lembaga pemerintah dengan konsekuensi yang meluas. Layanan publik seperti kesehatan, imigrasi, dan pendidikan mengalami gangguan besar, termasuk tertundanya akses ke data pasien di rumah sakit yang menyebabkan keterlambatan perawatan. Selain itu, proses pengurusan dokumen imigrasi terhenti, mengganggu perjalanan internasional. Dari sisi ekonomi, serangan ini menyebabkan kerugian finansial yang diperkirakan mencapai miliaran rupiah, mencakup biaya pemulihan sistem, hilangnya pendapatan akibat terganggunya layanan, serta risiko denda karena pelanggaran perlindungan data. Tak hanya itu, data pribadi warga negara, termasuk informasi kesehatan dan keuangan, berada dalam risiko bocor. Pelaku serangan menambah tekanan dengan ancaman merilis data tersebut jika tuntutan tebusan tidak dipenuhi, memberikan tantangan besar bagi pemerintah dalam menangani situasi ini [7].

Serangan *ransomware* pada PDNI mengungkap kelemahan utama dalam keamanan siber Indonesia, terutama kurangnya sistem deteksi dini yang efektif. Keberhasilan serangan *phishing* menunjukkan rendahnya kesadaran karyawan terhadap ancaman siber dan kurang optimalnya prosedur keamanan email. Faktor penyebabnya meliputi minimnya pelatihan keamanan siber, rendahnya prioritas keamanan di berbagai instansi, serta investasi teknologi yang terbatas. Selain itu, lemahnya regulasi dan kebijakan keamanan memperburuk situasi, sementara ketergantungan pada teknologi tanpa dukungan infrastruktur yang memadai, seperti sistem yang jarang diperbarui dan pemantauan ancaman yang kurang, meningkatkan risiko serangan. Upaya seperti penguatan regulasi, pelatihan rutin, dan investasi dalam teknologi keamanan menjadi langkah penting untuk mengurangi ancaman di masa depan [6].

Pemerintah Indonesia memberikan respons cepat dalam menangani krisis serangan *ransomware* ini dengan mengambil berbagai langkah strategis. Salah satunya adalah pembentukan tim tanggap darurat khusus yang bertugas menangani insiden, termasuk melakukan investigasi forensik guna mengidentifikasi kelemahan dalam sistem keamanan. Selain itu, pemerintah juga menjalin koordinasi dengan lembaga internasional untuk membantu melacak pelaku serangan serta mencegah ancaman serupa di masa depan. Sebagai upaya jangka panjang, pemerintah meningkatkan alokasi anggaran untuk memperkuat infrastruktur keamanan siber di seluruh lembaga pemerintah, memastikan perlindungan yang lebih baik terhadap data dan sistem vital negara .

Implikasi Etis

Serangan *ransomware* ini menimbulkan sejumlah pertanyaan etis yang penting mengenai tanggung jawab profesional dalam pengelolaan data sensitif:

1. Integritas Data

   Dalam era digital, integritas data adalah hal yang sangat penting. Serangan semacam ini menunjukkan bahwa data dapat dengan mudah dimanipulasi atau dihapus oleh pihak yang tidak bertanggung jawab. Para profesional keamanan siber harus berkomitmen untuk menjaga integritas data agar tetap akurat dan dapat diandalkan.
2. Kerahasiaan Informasi

   Kerahasiaan informasi pribadi warga negara adalah hal yang sangat penting. Ketika data sensitif jatuh ke tangan penyerang, risiko pencurian identitas meningkat secara signifikan. Profesional keamanan siber harus mengambil langkah proaktif untuk melindungi informasi ini melalui enkripsi dan kontrol akses yang ketat.
3. Tanggung Jawab Sosial

   Profesional di bidang keamanan siber memiliki tanggung jawab sosial untuk melindungi masyarakat dari potensi bahaya yang ditimbulkan oleh kebocoran data. Mereka harus berupaya keras untuk mendidik pengguna tentang praktik keamanan terbaik serta mengembangkan solusi teknologi yang lebih aman.

Tanggung Jawab Profesional

Prinsip etika dalam keamanan siber mencakup:

- Integritas: Memastikan bahwa data dikelola dengan cara yang jujur dan transparan.
- Kerahasiaan: Melindungi informasi sensitif dari akses yang tidak sah.
- Tanggung jawab: Mengakui konsekuensi dari tindakan yang diambil dalam melindungi sistem informasi.
- Profesionalisme: Menjaga standar tinggi dalam praktik keamanan siber.

Dalam konteks serangan *ransomware* ini, para profesional keamanan siber perlu mempertimbangkan dampak dari tindakan mereka terhadap masyarakat luas. Mereka harus berkomitmen untuk meningkatkan standar etika dan profesionalisme dalam setiap aspek pekerjaan mereka.

Implikasi Hukum

Dalam konteks hukum, Undang-Undang Informasi dan Transaksi Elektronik (UU ITE) serta Undang-Undang Perlindungan Data Pribadi (UU PDP) memberikan kerangka hukum untuk perlindungan data di Indonesia. Namun, implementasi hukum ini masih menghadapi tantangan, termasuk:

- Kurangnya Audit Keamanan Rutin: Banyak lembaga pemerintah tidak melakukan audit keamanan secara berkala, sehingga kerentanan tidak terdeteksi sebelum menjadi masalah besar [1].
- Penegakan Hukum yang Lemah: Meskipun ada undang-undang yang mengatur perlindungan data, penegakan hukum terhadap pelanggaran sering kali lemah, membuat pelaku kejahatan siber merasa kebal hukum.

Penelitian ini menunjukkan bahwa serangan *ransomware* terhadap Personal Data dan National Data (PDN) memiliki dampak yang serius pada berbagai aspek. Secara teknis, *ransomware* menyebabkan hilangnya akses terhadap data penting dan mengganggu operasional layanan publik seperti administrasi kependudukan dan kesehatan. Dampak ini diperparah oleh potensi biaya pemulihan yang tinggi serta risiko pembayaran tebusan yang hanya mendorong pelaku untuk melakukan serangan serupa. Dari sisi sosial, serangan ini melemahkan kepercayaan masyarakat terhadap kemampuan pemerintah dalam melindungi data mereka dan dapat merusak reputasi pemerintah, baik di tingkat nasional maupun internasional. Selain itu, insiden semacam ini memunculkan implikasi etis yang signifikan, di mana pemerintah memiliki tanggung jawab moral untuk melindungi data masyarakat. Kegagalan dalam pengelolaan risiko keamanan siber mencerminkan kelalaian yang dapat berdampak pada kesejahteraan masyarakat.

Penelitian ini juga menyoroti pentingnya pengelolaan risiko siber yang proaktif sebagai upaya mencegah serangan ransomware di masa depan. Upaya ini meliputi penerapan kebijakan keamanan yang ketat, pelatihan untuk meningkatkan kesadaran keamanan, penggunaan teknologi seperti enkripsi dan cadangan data, serta rencana respons insiden yang matang. Di sisi lain, tanggung jawab profesional dalam keamanan siber menjadi sorotan penting. Para profesional memiliki kewajiban untuk menjaga kerahasiaan dan integritas data, mengikuti kode etik yang ditetapkan, dan terus meningkatkan kompetensi mereka dalam menghadapi ancaman yang semakin kompleks. Dengan pendekatan kolaboratif antara pemerintah, profesional IT, dan masyarakat, ekosistem keamanan siber yang lebih aman dan bertanggung jawab dapat diwujudkan.

KESIMPULAN

serangan ransomware terhadap Individual Information dan National Information (PDN) memiliki dampak yang serius pada berbagai aspek. Secara teknis, ransomware menyebabkan hilangnya akses terhadap information penting dan mengganggu operasional layanan publik seperti administrasi kependudukan dan kesehatan. serangan ini melemahkan kepercayaan masyarakat terhadap kemampuan pemerintah dalam melindungi information mereka dan dapat merusak reputasi pemerintah,Selain itu, insiden semacam ini memunculkan implikasi etis yang signifikan, di mana pemerintah memiliki tanggung jawab ethical untuk melindungi information masyarakat. Penelitian ini juga menyoroti pentingnya pengelolaan risiko siber yang proaktif sebagai upaya mencegah serangan ransomware di masa depan. Upaya ini meliputi penerapan kebijakan keamanan yang ketat, pelatihan untuk meningkatkan kesadaran keamanan, penggunaan teknologi seperti enkripsi dan cadangan information, serta rencana respons insiden yang matang. Para profesional memiliki kewajiban untuk menjaga kerahasiaan dan integritas

information, mengikuti kode etik yang ditetapkan, dan terus meningkatkan kompetensi mereka dalam menghadapi ancaman yang semakin kompleks. Dengan pendekatan kolaboratif antara pemerintah, profesional IT, dan masyarakat, ekosistem keamanan siber yang lebih aman dan bertanggung jawab dapat diwujudkan. Aspek Finansial: Biaya pemulihan information dan sistem yang tinggi, termasuk kebutuhan untuk membayar tebusan atau meningkatkan infrastruktur keamanan, memberikan beban signifikan pada organisasi. Aspek Etis dan Tanggung Jawab Profesional: Serangan ransomware menyoroti pentingnya tata kelola information yang transparan dan aman sebagai tanggung jawab ethical dan profesional. Adopsi kebijakan keamanan siber yang ketat serta regulasi perlindungan information yang komprehensif Penelitian ini menunjukkan bahwa pendekatan holistik, melibatkan teknologi, kebijakan, dan etika profesional, sangat penting untuk menghadapi ancaman ransomware secara efektif.

DAFTAR PUSTAKA

[1] B. Hartono, "Ransomware: Memahami Ancaman Keamanan Digital," *Bincang Sains dan Teknologi*, vol. 2, no. 02, pp. 55–62, 2023.

[2] T. G. Laksana and S. Mulyani, "Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber Untuk Mencegah Pembobolan Data Perusahaan," *Jurnal Ilmiah Multidisiplin*, vol. 3, no. 01, pp. 109–122, 2024.

[3] F. X. Watkat, M. T. Ingratubun, M. H. Ingsaputro, and A. T. Hartantyo, "PERTANGGUNGJAWABAN PIDANA PENGENDALI DATA PRIBADI TERHADAP KEBOCORAN DATA PRIBADI WARGA NEGARA INDONESIA," *Jurnal Hukum Ius Publicum*, vol. 5, no. 2, pp. 177–198, 2024.

[4] F. Gunawan, A. Fadhilah, and E. M. S. Sakti, "Membangun Benteng Digital Untuk Memperkuat Etika Cyber Security Melawan Ancaman Cyber Crime," *Jurnal Ilmiah Teknik Informatika (TEKINFO)*, vol. 25, no. 1, pp. 154–167, 2024.

[5] Novina Putri Bestari (2024). Kronologi Hacker Rebut Kendali Pusat Data Nasional Diungkap BSSN. Avaliable at: https://www.cnbcindonesia.com/tech/20240627170323-37-549971/kronologi-hacker-rebut-kendali-pusat-data-nasional-diungkap-bssn

[6] Yudhistira Azhar Haryono Putra (2024). Serangan Ransomware Melumpuhkan Pusat Data Nasional Sementara (PDNS). Avaliable at: https://arek.its.ac.id/hmsi/2024/07/01/serangan-ransomware-melumpuhkan-pusat-data-nasional-sementara-pdns/

[7] Sukma Kanthi Nurani (2024). Kronologi Pusat Data Nasional Jebol hingga Desakan Menkominfo Budi Arie Mundur dari Jabatannya. Avaliable at: https://www.tempo.co/politik/kronologi-pusat-data-nasional-jebol-hinggadesakan-menkominfo-budi-arie-mundur-dari-jabatannya-44552

[8] Suhandoko (2024). Memahami Cara Bekerja Brain Cipher Ransomware yang Menyerang Pusat Data Nasional. Avaliable at: https://wisata.viva.co.id/berita/10516-memahami-cara-bekerja-brain-cipher-ransomware-yang-menyerang-pusat-data-nasional

[9] Maksum Rangkuti (2024). "Dampak" yang Ditimbulkan dari Peretasan Data Nasional oleh Ransomware 3.0 Tahun 2024 Avaliable at: https://fahum.umsu.ac.id/blog/dampak-yang-ditimbulkan-dari-peretasan-data nasional-oleh-ransomware-3-0-tahun-2024/

[10] Suhandoko (2024). Memahami Cara Bekerja Brain Cipher Ransomware yang Menyerang Pusat Data Nasional. Avaliabke at: https://wisata.viva.co.id/berita/10516-memahami-cara-bekerja-brain-cipher-ransomware-yang-menyerang-pusat-data-nasional

[11] Rifki (2024). Serang Pusat Data Nasional, Begini Cara Kerja Brain Cipher Ransomware. Avaliable at: https://infokomputer.grid.id/read/124111050/serang-pusat-data-nasional-begini-cara-kerja-brain-cipher-ransomware#google_vignette

[12] Meddy (2024). Mengenal Brain Chiper. Avaliable at: https://primakara.ac.id/blog/info-teknologi/mengenal-brain-cipher-ransomware-yang-guncang-pusat-data-nasional

[13] Budiman (2024). Apa itu Ransomware yang Serang Pusat Data Nasional? Avaliable at: https://umj.ac.id/just_info/apa-ransomware-yang-serang-pusat-data-nasional/

[14] Balqis Fallahnda (2024). Apa yang termasuk data PDN dan dampaknya jika terkena ransomware?.Available at: //tirto.id/apa-yang-termasuk-data-pdn-dan-dampaknya-jika-kena-ransomware-gZ6G

[15] Redaksi. (2024). Ransomware Serang PDN, Ini Pesan Pakar dari ITS Surabaya. Jurnal Security. Available at: https://jurnalsecurity.com/ransomware-serang-pdn-ini-pesan-pakar-dari-its-surabaya/, diakses tanggal 21 November 2024