JISCO(Journal of Information System and Computing) *ISSN :*
Volume 2, Nomor 1, Juni 2024 laman 27-41 e-ISSN :

ANALISIS PERKEMBANGAN KEAMANAN SIBER DAMPAK DARI KEBOCORAN DATA PUSAT DATA NASIONAL SEMENTARA 2 SURABAYA

ASSESSING AND UNDERSTANDING THE CURRENT SITUATION: ANALYSIS OF CYBER SECURITY DEVELOPMENTS THE IMPACT OF THE TEMPORARY NATIONAL DATA CENTER DATA LEAKS 2 SURABAYA

Oleh:

Ghalib Y.W., Gilang E.F., Zumi M., Abdhe F., Nanda A., Serly D.A., Zurkiyah A.

Program Studi Sistem Informasi, Universitas Islam Negeri Sulthan Thaha Saifuddin Jambi, Indonesia

Information Systems Study Program, Sulthan Thaha Saifuddin State Islamic University of Jambi, Indonesia

*e-mail: ghalibyudowijoyo24@gmail.com

Abstrak

Penelitian ini membahas serangan siber yang terjadi pada Pusat Data Nasional (PDNS) 2 Surabaya pada Juni 2024, yang disebabkan oleh ransomware Braincipher, varian dari Lockbit 3.0. Serangan ini mengakibatkan gangguan pada layanan publik, termasuk layanan keimigrasian, dengan dampak serius bagi aktivitas masyarakat dan kerugian finansial yang signifikan. Pemerintah melalui Badan Siber dan Sandi Negara (BSSN) dan Kementerian terkait menanggapi insiden ini dengan serangkaian langkah pemulihan yang terdiri dari zona karantina, pembersihan, dan pemulihan. Selain itu, penguatan regulasi keamanan siber diambil dengan mewajibkan cadangan data, peningkatan infrastruktur, serta kerja sama lintas instansi untuk memperbaiki tata kelola data. Analisis SWOT yang dilakukan mengidentifikasi kekuatan pada pemulihan layanan dan implementasi strategi backup 3-2-1, namun mengungkap kelemahan dalam respons keamanan yang masih bersifat reaktif. Di sisi lain, peluang untuk memperkuat klasifikasi data dan peningkatan kerja sama digital forensik diharapkan dapat meningkatkan ketahanan sistem. Namun demikian, ancaman terkait keterbatasan sumber daya, kesiapan server cadangan, dan potensi celah pada infrastruktur tetap perlu diwaspadai. Penelitian ini terbatas pada data sekunder dari sumber berita, sehingga wawancara dengan aktor dan pemangku kepentingan diperlukan untuk memperkaya analisis.

Kata kunci: Sistem Informasi, Kebocoran Data, Keamanan Siber, Pusat Data Nasional Surabaya 2 (PDNS 2).

Abstract

This study discusses the cyber attack on the National Data Center (PDNS) 2 in Surabaya in June 2024, caused by the Braincipher ransomware, a variant of Lockbit 3.0. The attack disrupted public services, including immigration services, with significant impact on public activities and considerable financial losses. The government, through the National Cyber and Encryption Agency (BSSN) and relevant ministries, responded to the incident with a series of

*recovery measures involving quarantine, cleanup, and restoration zones. Additionally, cybersecurity regulations were strengthened, mandating data backups, infrastructure improvements, and cross-agency collaboration to enhance data governance. The SWOT analysis identifies strengths in service recovery and the implementation of a 3-2-1 backup strategy but reveals weaknesses in the reactive nature of security responses. On the other hand, opportunities for strengthening data classification and enhancing digital forensic collaboration are expected to improve system resilience. However, threats related to resource limitations, backup server readiness, and potential vulnerabilities in infrastructure remain concerning. This study is limited to secondary data from news sources; therefore, interviews with stakeholders and involved parties are recommended to enrich the analysis.**Keywords: Information System, Data Leakage, Cyber Security, Surabaya National Data Center 2 (PDNS 2).*

1 PENDAHULUAN

Dalam era digital yang semakin berkembang, keamanan siber menjadi perhatian utama bagi pemerintah dan institusi di seluruh dunia. Serangan siber tidak hanya mengancam keamanan data, tetapi juga dapat berdampak langsung pada layanan publik yang vital. Salah satu insiden terbaru yang mencerminkan tantangan tersebut adalah serangan siber yang terjadi pada Pusat Data Nasional (PDNS) 2 Surabaya pada Juni 2024. Serangan ini melibatkan ransomware Braincipher, yang merupakan varian dari ransomware Lockbit 3.0, dan menyebabkan gangguan signifikan pada berbagai layanan publik, termasuk layanan keimigrasian.

Kronologi peristiwa serangan ini menunjukkan bagaimana ancaman siber dapat dengan cepat merusak sistem yang ada, mengakibatkan kerugian finansial yang besar dan hilangnya kepercayaan publik terhadap keamanan layanan pemerintah. Tindak lanjut dari insiden ini melibatkan berbagai langkah pemulihan yang dilakukan oleh pemerintah, termasuk audit keamanan siber dan penguatan infrastruktur. Upaya ini tidak hanya bertujuan untuk memperbaiki kerusakan yang ditimbulkan, tetapi juga untuk mencegah terulangnya kejadian serupa di masa depan.

Di tengah tantangan ini, penting untuk menganalisis bagaimana respon pemerintah, regulasi yang diterapkan, dan langkah-langkah pemulihan yang diambil dapat meningkatkan keamanan siber secara keseluruhan. Penelitian ini bertujuan untuk menggali kronologi serangan, cara kerja ransomware yang terlibat, serta dampak dan respon yang diambil oleh pemerintah dalam menghadapi ancaman siber. Dengan pemahaman yang lebih mendalam tentang insiden ini, diharapkan dapat ditemukan solusi yang lebih efektif untuk memperkuat sistem keamanan siber di Indonesia dan meningkatkan ketahanan nasional dalam menghadapi ancaman siber di masa depan.

2 TINJAUAN LITERATUR

2.1 Budaya Keamanan Siber

Menurut Alvarez-Dionisi dan Urrego-Baquero (2019) budaya keamanan siber adalah "pengetahuan, keyakinan, persepsi, sikap, asumsi, norma, dan nilai masyarakat mengenai keamanan siber dan bagaimana hal tersebut terwujud dalam perilaku masyarakat terhadap teknologi informasi." Pada kenyataannya, tujuan utama budaya keamanan siber adalah untuk mengembangkan dan menerapkan ekosistem budaya keamanan siber untuk mendukung keamanan siber. Berbagi pengalaman dalam membangun landasan sosial dan psikologis yang canggih dapat membantu mendukung keamanan siber .

Budaya Keamanan Siber mencakup topik-topik umum termasuk kesadaran keamanan siber dan kerangka kerja keamanan informasi, namun cakupan dan penerapannya lebih luas, karena berkaitan dengan menjadikan pertimbangan keamanan informasi sebagai bagian integral dari pekerjaan, kebiasaan, dan perilaku karyawan, serta menanamkannya dalam keseharian mereka. tindakan" (Oltsik, 2024).

2.2 Information Security Awareness

Information security awareness (ISA) mengacu pada kondisi kesadaran dimana *user* secara ideal berkomitmen pada aturan, mengenali potensi, memahami pentingnya tanggung jawab, dan bertindak sesuai dengan itu. Meskipun banyaknya kasus pelanggaran keamanan informasi, khususnya pada *knowledge-based institution*, yang diakibatkan oleh keengganan pengguna untuk mematuhi pedoman keamanan dan tindakan efektif seperti penerapan *incident response plan* (RCP), *disaster recovery plan* (DRP), dan *business continuity plan* (BCP) yang harus dilakukan untuk mengantisipasi dampak negatifnya (Ahlan, Lubis dan Lubis, 2015).

Menurut Ashraf (2005) *information security awareness* adalah pendidikan dan kesadaran pengguna untuk menangani ancaman keamanan informasi dan meminimalkan dampaknya. Program kesadaran pada dasarnya memusatkan perhatian pada masalah keamanan informasi seperti *confidentiality, integrity, and availability*. Ini menyoroti pentingnya faktor-faktor ini, perannya dalam bisnis dan akhirnya berkonsentrasi pada bagaimana berperilaku dengan faktor-faktor tersebut dengan cara yang percaya diri.

3 METODOLOGI PENELITIAN

Metodologi Analisis SWOT

- **Analisis SWOT**
  - **Kekuatan (Strengths)**:
    - Identifikasi dan analisis faktor internal yang memberikan keunggulan dalam keamanan siber, seperti:
      - Pengumpulan backup server dan pemulihan layanan.
      - Peningkatan keamanan siber oleh BSSN.

- Aktivasi CSIRT untuk pemantauan berkelanjutan.
- Implementasi strategi backup 3-2-1.

- **Kelemahan (Weaknesses)**:
  - Identifikasi dan analisis faktor internal yang menghambat kinerja keamanan siber, seperti:
    - Kekurangan sumber daya manusia yang terampil dalam keamanan siber.
    - Kurangnya kesadaran dan pelatihan di kalangan pegawai pemerintah.
    - Potensi infrastruktur yang rentan atau usang.
- **Peluang (Opportunities)**:
  - Identifikasi faktor eksternal yang dapat dimanfaatkan untuk meningkatkan keamanan siber, seperti:
    - Kerjasama internasional dalam keamanan siber.
    - Peningkatan investasi dalam teknologi keamanan siber.
    - Kebutuhan masyarakat akan perlindungan data yang lebih baik.
- **Ancaman (Threats)**:
  - Identifikasi faktor eksternal yang dapat mengancam keamanan siber, seperti:
    - Serangan siber yang semakin canggih dan beragam.
    - Ketidakpastian regulasi di bidang keamanan siber.
    - Ancaman dari kelompok hacker yang terorganisir.

Metodologi analisis SWOT ini diharapkan dapat memberikan wawasan mendalam mengenai keadaan keamanan siber di Indonesia, serta membantu dalam merumuskan langkah-langkah strategis untuk meningkatkan perlindungan data dan infrastruktur digital di masa depan.

Tabel 1. Spesifikasi Data

Spesifikasi	Deskripsi
Sumber Data	Berita *online* dari berbagai sumber (Anggraeni, 2024b, 2024a; CNN Indonesia, 2024b, 2024a; Fadilah, 2024; Hadyan, 2024; Kure, 2024; Rahmawati, 2024; Safitri, 2024; Wakang, 2024); Rita P. S. (2024); Mohammad H. M.(2024); Andri S. (2024)

Kategori Penilaian	Kebijakan, pelatihan, insiden, kepatuhan, sikap pengguna, dimensi budaya dll.
Rentang Waktu	Tanggal publikasi sampel berita (26 Juni 2024 – 30 Oktober 2024).
Format Data	Teks deskriptif
Metodologi	Analisis konten berita terkait budaya keamanan siber dan penilaian dari berita.

HASIL DAN PEMBAHASAN

Kronologi Serangan Siber PDNS 2 Surabaya

Berdasarkan informasi yang dihimpun dari (Aranditio, 2024; Luthfiani, 2024) maka kronologi serangan siber PDNS 2 Surabaya tersaji pada tabel 1 dibawah ini:

Tabel 1. Kronologi serangan siber di pusat data nasional 2 surabaya

Tanggal dan Waktu	Uraian Peristiwa
Kamis, 20 Juni 2024 Pukul 00.54 WIB	Terjadi gangguan pada PDNS berupa instalasi *filemalicious* yang menghapus sistem file penting dan menonaktifkan layanan yang sedang berjalan.
Kamis, 20 Juni 2024 Pukul 00.55 WIB	Windows Defender mengalami *crash* dan tidak bisa beroperasi.
Kamis, 20 Juni 2024 Pukul 04.00 WIB	Instansi pertama yang melaporkan dampak gangguan adalah Direktorat Jenderal Imigrasi Kementerian Hukum dan HAM mengenai layanan keimigrasian.
Kamis, 20 Juni 2024 Sore	Direktur Jenderal Aplikasi Informatika Kementerian Komunikasi dan Informatika Semuel Abrijani Pangerapan membenarkan adanya gangguan pada Pusat Data Nasional yang berdampak pada sejumlah layanan publik.
Minggu, 23 Juni 2024	Badan Siber dan Sandi Negara (BSSN) menyatakan tengah melakukan analisis berdasarkan bukti digital masih terus dilakukan, tetapi akar masalah belum juga ditemukan.
Senin, 24 Juni 2024	Kepala BSSN mengatakan gangguan PDNS disebabkan oleh serangan siber perangkat keras perusak atau *ransomware brain chipper*, varian dari

	ransomware Lockbit 3.0. Pelaku peretasan Pusat Data Nasional (PDN) meminta uang sebanyak USD 8 juta atau sekitar Rp 131 miliar dalam kurs Rp 16.399 kepada Pemerintah Indonesia.
Selasa, 25 Juni 2024	Direktur Jenderal Aplikasi Informatika Kementerian Kominfo Semuel Abrijani Pangerapan mengatakan pihaknya masih memulihkan layanan di 282 instansi layanan publik yang menggunakan PDNS.

Cara Kerja Braincipher

Menurut (Ibnu , 2024) cara kerja Ransomware brainchipher adalah sebagai berikut:

1. **Infeksi Awal**: Braincipher dapat menginfeksi sistem melalui berbagai cara, seperti email *phishing*, tautan berbahaya, atau kerentanan perangkat lunak.
2. **Enkripsi File**: Setelah berhasil menginfeksi sistem, Braincipher akan mulai mengenkripsi file-file penting korban, seperti dokumen, foto, video, dan database.
3. **Tuntutan Tebusan**: Setelah file-file dienkripsi, Braincipher akan menampilkan pesan yang menuntut tebusan dalam bentuk mata uang *kripto*. Korban biasanya diberi waktu terbatas untuk membayar tebusan, jika tidak, file-file mereka akan hilang secara permanen.

Dampak Serangan Braincipher

Serangan Braincipher pada PDNS menyebabkan gangguan pada berbagai layanan publik, termasuk layanan imigrasi. Gangguan ini berdampak pada aktivitas masyarakat dan menimbulkan kerugian finansial. Selain itu, serangan ransomware juga dapat merusak reputasi organisasi dan menyebabkan hilangnya kepercayaan publik.(Ibnu , 2024).

PERKEMBANGAN KEAMANAN SIBER SEMENJAK KEBOCORAN DATA PDNS 2

Regulasi Dan Kebijakan Pemerintah

Menteri Koordinator Bidang Politik, Hukum, dan Keamanan (Menko Polhukam) Hadi Tjahjanto menyatakan pemerintah mewajibkan kementerian dan lembaga mempunyai data cadangan sebagai langkah tindak lanjut usai PDNS 2 diserang ransomware. (Mohammad H. M.2024)

"Kami memang melihat secara umum, mohon maaf pak menteri, permasalahan utama adalah tata kelola, ini hasil pengecekan kita dan tidak adanya *back up*," kata Hinsa. (Andri S. 2024)

Dia mengatakan, bahwa cadangan data itu diperlukan dan sesuai dengan Peraturan BSSN Nomor 4 Tahun 2021 tentang pedoman manajemen keamanan informasi sistem pemerintahan berbasis elektronik. (Andri S. 2024)

Hadi menyebut Kemenko Polhukam akan menggandeng Badan Siber dan Sandi Negara (BSSN) dalam upaya meningkatkan keamanan siber usai serangan ransomware terhadap PDSN 2. (Mohammad H. M.2024)

Audit Keamanan Siber

Komisi I DPR RI menggelar rapat kerja lanjutan dengan Menko Polhukam Hadi Tjahjanto bersama Kementerian Komunikasi dan Informatika dan Badan Siber Sandi Negara (BSSN) terkait pencegahan serangan siber terhadap Pusat Data Nasional Sementara (PDNS) pada masa depan.
"Rapat kita buka dengan sifat terbuka dan nanti jika melihat ada kerahasiaan negara kita lanjutkan dengan sifat tertutup," kata Ketua Komisi I DPR RI Meutya Hafid membuka jalannya rapat di Kompleks Parlemen, Senayan, Jakarta, Senin.(Antara, 2024)

Tahapan-Tahapan Pemulihan

Rita P. S. (2024) Ismail menjelaskan bahwa proses pemulihan dilakukan melalui tiga zona utama. "Proses recovery ini kita lakukan menjadi tiga zona. Kita anggap kejadian kemarin itu ada di zona merah, itu sama sekali proses dikarantina," ucapnya.

Setelah tahap zona merah, data dan layanan akan dipindahkan ke zona biru. Di zona ini, pemerintah memperkuat keamanan dengan melakukan penyisiran terhadap virus, malware, dan ancaman lainnya yang mungkin ada di data tersebut. Selain itu, perbaikan tata kelola dilakukan dengan mereset semua password yang digunakan oleh pengguna di PDNS 2. Rita P. S. (2024)

Rita P. S. (2024) "Zona biru ini kita lakukan perkuatan-perkuatan sebelum nantinya dipindahkan ke zona hijau," kata Ismail.

Menurut Ismail, ketiga zona tersebut merupakan langkah jangka pendek yang dilakukan pemerintah dalam pemulihan layanan. Periode ini berlangsung dari Juli 2024. Untuk jangka menengah, dari Juli hingga Agustus 2024, meliputi proses pemulihan penuh PDNS 2, redeployment layanan tenant, perbaikan *Standard Operating Procedure* (SOP), dan evaluasi tata kelola PDNS. Rita P. S. (2024)

Upaya Peningkatan Kesadaran Dan Edukasi Keamanan Siber

Selain itu, pemerintah juga berupaya untuk meningkatkan kesadaran dan edukasi mengenai keamanan siber kepada seluruh instansi pemerintah dan masyarakat. Langkah ini diambil untuk mengurangi risiko serangan siber di masa mendatang dan memastikan bahwa sistem keamanan siber nasional semakin kuat. Rita P. S. (2024)

Peningkatan Infrastruktur IT

Ke depan, Kominfo berencana untuk terus mengembangkan kapasitas dan kapabilitas Pusat Data Nasional, sehingga mampu memberikan layanan yang lebih handal dan aman. Melalui upaya-upaya ini, diharapkan Indonesia dapat menjadi negara yang lebih siap dan resilient dalam menghadapi berbagai ancaman siber. Rita P. S. (2024)

Hasil Analisis SWOT

- Kekuatan

    1) Pengumpulan Backup Server dan Pemulihan Layanan

        Pemulihan Layanan: Pemerintah mereaktivasi layanan melalui backup server dari situs dingin (cold site) BTAM dan mengaktifkannya di fasilitas PDNS 1 dan Data Center Temporary milik penyedia. (CNN, 2024c).

    2) Peningkatan Keamanan Siber oleh BSSN

        Badan Siber dan Sandi Negara (BSSN): Pemerintah melalui BSSN akan terus meningkatkan keamanan siber dengan cara menyambungkan komando kendali BSSN untuk memastikan sistem lebih kuat. (CNN, 2024 ; Dwi R. , 2024).

    3) Aktivasi CSIRT untuk Pemantauan Berkelanjutan

        Monitoring Continues: Mengaktifkan Computer Security Incident Response Team (CSIRT) untuk memantau upaya pengelolaan PDNs dan backup data secara terus-menerus. (CNN, 2024).

    4) Implementasi Strategi Backup 3-2-1

        Validasi Sistem: Validasi terhadap PDNS sedang dilakukan oleh BSSN untuk memastikan bahwa sistem tersebut mematuhi aturan backup 3-2-1, yaitu memiliki tiga salinan data, disimpan di dua media berbeda, dengan satu salinan di luar lokasi utama (offsite). (Rita P. S., 2024).

Pengelolaan pemulihan layanan dan keamanan siber di Indonesia menunjukkan kekuatan yang signifikan melalui beberapa langkah strategis.

Pertama, pemulihan layanan dengan memanfaatkan backup server dari cold site BTAM menunjukkan komitmen pemerintah dalam memastikan kontinuitas operasional. Kedua, upaya peningkatan keamanan siber oleh Badan Siber dan Sandi Negara (BSSN) melalui penguatan sistem kendali menandakan keseriusan dalam melindungi infrastruktur digital.

Selain itu, aktivasi Computer Security Incident Response Team (CSIRT) untuk pemantauan berkelanjutan mencerminkan pendekatan proaktif dalam mengelola insiden keamanan siber. Terakhir, implementasi strategi backup 3-2-1 oleh BSSN memastikan bahwa data terlindungi dengan baik, sehingga mengurangi risiko kehilangan informasi penting. Secara keseluruhan, langkah-langkah ini menunjukkan kesiapan dan ketahanan sistem dalam menghadapi tantangan di era digital.

- Kelemahan

    1) Pengaturan Backup Data dengan Fokus pada Jaminan Kontinuitas

        Jaminan Kontinu: Pengaturan backup data dan layanan kementerian/lembaga/pemerintah daerah untuk menjaga kontinuitas layanan publik. (CNN, 2024c).

    2) Evaluasi Forensik Digital

        Identifikasi Pelaku: Tim BSSN melakukan forensik digital untuk identifikasi pelaku serangan ransomware, termasuk analisis detail tentang serangan tersebut. (Dwi R. 2024).

    3) Isolasi Infrastruktur PDNS 2

        Data Terproteksi: Isolasi infrastruktur PDNS 2 untuk mencegah akses ilegal dan memastikan data tidak bisa disalahgunakan, meskipun data tersebut terenkripsi. (Herlan W. 2024).

Meskipun ada langkah-langkah signifikan yang diambil untuk memperkuat pemulihan layanan dan keamanan siber, terdapat beberapa kelemahan yang perlu diperhatikan. Pertama, pengaturan backup data yang lebih berfokus pada jaminan kontinuitas layanan publik menunjukkan bahwa mungkin ada kekurangan dalam pengelolaan data secara menyeluruh, yang dapat berpotensi mengabaikan aspek-aspek penting lainnya dari keamanan data.

Kedua, meskipun evaluasi forensik digital dilakukan untuk mengidentifikasi pelaku serangan ransomware, ketergantungan pada analisis pasca-serangan menunjukkan bahwa respons terhadap insiden keamanan mungkin belum sepenuhnya proaktif. Hal ini dapat mengakibatkan lambatnya penanganan serangan yang akan datang.

Ketiga, isolasi infrastruktur PDNS 2 untuk mencegah akses ilegal adalah langkah penting, tetapi juga menciptakan tantangan dalam memastikan akses yang

diperlukan untuk pemeliharaan dan pembaruan sistem. Meskipun data terenkripsi, isolasi dapat membatasi kemampuan untuk mengelola dan memanfaatkan data secara efektif.

Secara keseluruhan, meskipun langkah-langkah yang diambil penting, masih ada area yang perlu diperbaiki untuk memastikan perlindungan yang lebih holistik dan respons yang lebih cepat terhadap ancaman siber.

- Peluang

    1) Penyajian Data Secara Berlapis Berdasarkan Tingkat Klasifikasi

        Tingkat Klasifikasi Data: Penyiapan pengaturan penempatan data dan cadangan secara berlapis sesuai dengan tingkat klasifikasi data, yaitu mulai dari data strategis, data terbatas, hingga data terbuka. (CNN, 2024c).

    2) Kerjasama Investigasi dengan Polri

        Kerjasama Polri: Investigasi digital forensik dilakukan bersama dengan tim Cyber Crime Kepolisian RI (Polri) untuk mendapatkan penanganan yang lebih tepat dan efektif. (Herlan W. 2024).

    3) Pengaturan Backup Data untuk Semua Kementerian dan Lembaga

        Jaminan Kontinu: Pengaturan backup data dan layanan kementerian/lembaga/pemerintah daerah untuk menjaga kontinuitas layanan publik. (CNN, 2024c).

Terdapat beberapa peluang signifikan yang dapat dimanfaatkan untuk meningkatkan pengelolaan data dan keamanan siber. Pertama, penyajian data secara berlapis berdasarkan tingkat klasifikasi memungkinkan pengaturan penempatan data dan cadangan yang lebih sistematis. Dengan mengklasifikasikan data mulai dari data strategis hingga data terbuka, organisasi dapat meningkatkan keamanan dan efisiensi dalam mengelola informasi.

Kedua, kerjasama investigasi dengan Kepolisian RI (Polri) untuk digital forensik membuka peluang untuk penanganan insiden keamanan yang lebih efektif. Kolaborasi ini dapat memperkuat kemampuan dalam mengidentifikasi dan menangkap pelaku kejahatan siber, serta memberikan wawasan yang lebih dalam tentang pola serangan yang ada.

Ketiga, pengaturan backup data yang komprehensif untuk semua kementerian dan lembaga memberikan jaminan kontinuitas layanan publik. Dengan memastikan bahwa setiap entitas pemerintah memiliki kebijakan backup yang jelas dan terintegrasi, risiko kehilangan data dapat diminimalkan, dan respons terhadap insiden dapat dilakukan dengan lebih cepat.

Secara keseluruhan, memanfaatkan peluang ini akan meningkatkan ketahanan sistem, memperkuat keamanan data, dan memastikan kontinuitas layanan publik dalam menghadapi tantangan yang ada di era digital.

- Ancaman

    1) Pemulihan dari Backup Server Cold Site

        Pemulihan ini bergantung pada kesiapan server cadangan, yang jika tidak memadai, dapat memperlambat proses pemulihan dan memengaruhi layanan publik.(CNN, 2024c).

    2) Kemungkinan Ancaman pada Infrastruktur PDNS yang Belum Diisolasi

        Isolasi PDNS 2 efektif untuk perlindungan, namun infrastruktur yang belum diisolasi mungkin masih rentan terhadap potensi ancaman siber. (Herlan W. 2024).

    3) Aktivasi CSIRT untuk Monitoring yang Berkelanjutan

        Monitoring membutuhkan sumber daya yang besar. Jika tidak didukung oleh dana dan tenaga kerja yang cukup, ini bisa menghambat upaya mitigasi risiko yang optimal. (Dwi R. 2024).

Dalam konteks pengelolaan data dan keamanan siber, beberapa ancaman signifikan harus diwaspadai. Pertama, pemulihan dari backup server cold site sangat bergantung pada kesiapan dan keandalan server cadangan tersebut. Jika server cadangan tidak memadai atau tidak siap, proses pemulihan dapat terhambat, yang pada gilirannya dapat memengaruhi layanan publik dan mengganggu operasional penting.

Kedua, meskipun ada upaya untuk mengisolasi infrastruktur PDNS 2, bagian dari infrastruktur yang belum diisolasi tetap rentan terhadap potensi ancaman siber. Ketidaklengkapan dalam isolasi dapat menjadi celah bagi serangan, yang dapat mengekspos data sensitif dan mengganggu keamanan sistem secara keseluruhan.

Ketiga, aktivasi Computer Security Incident Response Team (CSIRT) untuk pemantauan berkelanjutan adalah langkah penting, namun ini juga memerlukan sumber daya yang besar. Jika upaya pemantauan tidak didukung oleh dana dan tenaga kerja yang memadai, efektivitas dalam mitigasi risiko dapat terhambat, sehingga meningkatkan kemungkinan terjadinya insiden keamanan.

Secara keseluruhan, ancaman-ancaman ini menekankan pentingnya persiapan yang baik, isolasi yang menyeluruh, dan dukungan sumber daya yang memadai untuk menjaga keamanan dan ketahanan sistem dalam menghadapi tantangan di era digital.

KETERBATASAN PENELITIAN

Keterbatasan penelitian ini terletak pada sumber data yang hanya berasal dari berita *online*. Agar dapat menggali informasi lebih mendalam dan menghasilkan analisis yang lebih komprehensif, diperlukan data hasil wawancara dengan para aktor dan *stakeholders* yang terlibat dalam peristiwa kebocoran data PDNS 2 Surabaya ini.

PENUTUP

KESIMPULAN

Serangan siber pada Pusat Data Nasional (PDNS) 2 Surabaya yang terjadi pada Juni 2024, menunjukkan kerentanan serius dalam sistem keamanan siber pemerintah Indonesia. Insiden yang disebabkan oleh ransomware Braincipher ini berhasil mengenkripsi data penting dan mengganggu berbagai layanan publik, termasuk layanan imigrasi. Tindakan peretas ini mengakibatkan gangguan operasional yang luas serta tuntutan tebusan bernilai jutaan dolar.

Menanggapi insiden ini, pemerintah melalui BSSN, Kemenko Polhukam, dan Kominfo mengambil langkah-langkah untuk memperkuat infrastruktur keamanan siber dan meningkatkan regulasi terkait manajemen data. Implementasi zona pemulihan berlapis, peningkatan backup data, serta pengawasan berkelanjutan oleh Computer Security Incident Response Team (CSIRT) menunjukkan upaya pemulihan yang terstruktur. Analisis SWOT dalam laporan ini juga mengidentifikasi kekuatan, kelemahan, peluang, dan ancaman yang dihadapi, di mana penguatan backup, kerjasama lintas lembaga, serta pendidikan dan peningkatan kesadaran menjadi poin krusial.

Keterbatasan penelitian ini adalah kurangnya data primer yang dapat melengkapi analisis, sehingga ke depan, wawancara dengan aktor dan stakeholders yang terlibat diperlukan untuk memberikan pandangan lebih komprehensif tentang tantangan dan kebutuhan dalam sistem keamanan siber nasional.

DAFTAR PUSTAKA

Ahlan, A.R., Lubis, M. dan Lubis, A.R. (2015) “Information Security Awareness at the Knowledge-Based Institution: Its Antecedents and Measures,” in *Procedia Computer Science*. Amsterdam: Elsevier B.V., hal. 361–373. Tersedia pada: https://doi.org/10.1016/j.procs.2015.12.151.

Alvarez-Dionisi, L.E. dan Urrego-Baquero, N. (2019) “Implementing a Cybersecurity Culture,” *ISACA JOURNAL*, 2, hal. 1–6. Tersedia pada:

https://www.isaca.org/resources/isaca-journal/issues/2019/volume-2/implementing-a-cybersecurity-culture.

Andri S. (2024) *Kronologi dan Dampak Serangan Siber Terhadap PDNS Surabaya yang tak Punya Back Up Datanya*. Tersedia pada: https://news.republika.co.id/berita/sfqqoh409/kronologi-dan-dampak-serangan-siber-terhadap-pdns-surabaya-yang-tak-punya-back-up-datanya-part2 (Diakses: 28 Oktober 2024).

Anggraeni, R. (2024a) *DPR Sesali Bertahun-tahun PDNS 2 Tidak Punya Data Cadangan (Backup)*, *Bisnis Tekno*. Diedit oleh Leo Dwi Jatmiko. Tersedia pada: https://teknologi.bisnis.com/read/20240627/101/1777675/dpr-sesali-bertahun-tahun-pdns-2-tidak-punya-data-cadangan-backup (Diakses: 20 Oktober 2024).

Anggraeni, R. (2024b) *Server PDNS Down, BSSN Lakukan Audit Digital Forensik*, *Bisnis Tekno*. Tersedia pada: https://teknologi.bisnis.com/read/20240627/101/1777617/server-pdns-down-bssn-lakukan-audit-digital-forensik (Diakses: 20 Oktober 2024).

Antara (2024) *Komisi I DPR gelar rapat lanjutan soal serangan siber terhadap PDNS*. Tersedia pada: https://www.antaranews.com/berita/4351619/komisi-i-dpr-gelar-rapat-lanjutan-soal-serangan-siber-terhadap-pdns (Diakses: 29 Oktober 2024).

Aranditio, S. (2024) *Terdampak Peretasan PDN, Apa yang Harus Dilakukan Mahasiswa Penerima Beasiswa KIP Kuliah?*, *Kompas.id*. Tersedia pada: https://www.kompas.id/baca/humaniora/2024/07/01/kemendikbudristek-pastikan-data-pokok-pendidikan-aman-dari-peretasan-pdn (Diakses: 20 oktober 2024).

Ashraf, S. (2005) *"Organization Need and Everyone's Responsibility Information Security Awareness."* SANS Institute, hal. 21. Tersedia pada: https://www.giac.org/paper/gsec/4340/organization-everyones-responsibility-information-security-awareness/107113#:~:text=Information Security Awareness is user's,like confidentiality%2C integrity and availability.

CNN Indonesia (2024a) *Imbas Peretasan PDNS, Pemerintah Godok Aturan Kewajiban Backup Data*, *CNN Indonesia*. Tersedia pada: https://www.cnnindonesia.com/teknologi/20240710091916-192-1119505/imbas-peretasan-pdns-pemerintah-godok-aturan-kewajiban-backup-data (Diakses: 20 Oktober 2024).

CNN Indonesia (2024b) *Insiden Peretasan PDNS 2, Pakar Sorot Kualitas SDM Indonesia*, *CNN Indonesia*. Tersedia pada: https://www.cnnindonesia.com/teknologi/20240626110919-192-1114286/insiden-peretasan-pdns-2-pakar-sorot-kualitas-sdm-indonesia (Diakses: 20 Oktober 2024).

CNN Indonesia (2024c) *PDNS Diretas, Upaya Pemerintah untuk Pulihkan Pelayan Publik, CNN Indonesia.* Tersedia pada: https://search.app/m5sxknmdupAyru9x6 (Diakses: 21 Oktober 2024).

Dwi, R. (2024) *BSSN Jelaskan Upaya Pulihkan Layanan Imigrasi Usai PDNS Kena Ransomware.* Tersedia pada: https://search.app/MtTCPYJxpudWkymk7 (Diakses: 21 Oktober 2024).

Herlan,W. (2024) *Perkembangan Pemulihan PDNS 2 di Kementrian Kominfo,* Tersedia pada: https://search.app/Hbe7TCXahdcBsgWYA (Diakses: 21 Oktober 2024).

Fadilah, K. (2024) *Pemerintah Bakal Siapkan 4 Lapis Backup Data Usai PDNS Diretas*, *detikNews*. Tersedia pada: https://news.detik.com/berita/d-7417288/pemerintah-bakal-siapkan-4-lapis-backup-data-usai-pdns-diretas (Diakses: 20 Oketober2024).

Hadyan, R. (2024) *Password Disebar Karyawan Picu Serangan Siber ke PDNS 2, Bagaimana Mitigasinya?*, *Investor Trust*. Diedit oleh F.F.S. Putra. Tersedia pada: https://investortrust.id/news/password-disebar-karyawan-picu-serangan-siber-ke-pdns-2-bagaimana-mitigasinya (Diakses: 24 Juli 2024).

Ibnu N. (2024) *Mengenal Braincipher, Ransomware Canggih yang Mampu Jebol Server Pusat Data Nasional.Inilah.com.* Tersedia pada: https://www.inilah.com/Mengenal Braincipher, Ransomware Canggih yang Mampu Jebol Server Pusat Data Nasional (Diakses: 20 oktober 2024).

Kure, E. (2024) *Peretasan PDNS 2 Diduga Ulah Oknum Karyawan Lintasarta, Berhenti Kerja Agustus 2021 dan Mulai Bocorkan Data 11 Oktober 2022*, *Berita Satu*. Diedit oleh AD. Tersedia pada: https://www.beritasatu.com/ekonomi/2827333/peretasan-pdns-2-diduga-ulah-oknum-karyawan-lintasarta-berhenti-kerja-agustus-2021-dan-mulai-bocorkan-data-11-oktober-2022 (Diakses: 24 Juli 2024).

Luthfiani, D. (2024) *Peretas Pusat Data Nasional Minta Tebusan Rp 131 Miliar, Tempo*. Diedit oleh R. Paraqbueq. Tersedia pada: https://nasional.tempo.co/read/1883534/peretas-pusat-data-nasional-minta-tebusan-rp-131-miliar (Diakses: 20 oktober 2024).

Mohammad H. M.(2024) *Deretan Perkembangan Pasca PDNS Diretas*. Diedit oleh Dwi A. Tersedia pada: Deretan Perkembangan Pasca PDNS Diretas - Tekno Tempo.co (Diakses: 29 oktober 2024).

Oltsik, J. (2024) *Improving cybersecurity culture: A priority in the year of the CISO*, *CSO*. Tersedia pada: https://www.csoonline.com/article/1298541/improving-cybersecurity-culture-a-priority-in-the-year-of-the-ciso.html#:~:text=“The concept of cybersecurity culture,people’s behavior with information technologies. (Diakses: 20 Oktober 2024).

Rahmawati, D. (2024) *BSSN Jelaskan Upaya Pulihkan Layanan Imigrasi Usai PDNS Kena Ransomware*, *detikNews*. Tersedia pada: https://news.detik.com/berita/d-7412027/bssn-jelaskan-upaya-pulihkan-layanan-imigrasi-usai-pdns-kena-ransomware (Diakses: 24 Juli 2024).

Rita P. S. (2024) *Kominfo Ungkap Strategi Pemulihan PDNS Pasca Serangan Ransomware.* Tersedia pada:Kominfo Ungkap Strategi Pemulihan PDNS Pasca Serangan Ransomware (Diakses: 29 Juli 2024).

Safitri, E. (2024) *Jokowi Perintahkan BPKP Audit Pusat Data Nasional Buntut Peretasan*, *detikNews*. Tersedia pada: https://news.detik.com/berita/d-7414588/jokowi-perintahkan-bpkp-audit-pusat-data-nasional-buntut-peretasan (Diakses: 24 Juli 2024).

Wakang, A.A. (2024) *Beranda Nasional PDNS Diretas, PPI Dunia Sarankan Buat Simulasi Rutin Kesiapan Hadapi Serangan Siber*, *Tempo*. Diedit oleh I. Hamdi. Tersedia pada: https://nasional.tempo.co/read/1886811/pdns-diretas-ppi-dunia-sarankan-buat-simulasi-rutin-kesiapan-hadapi-serangan-siber