AKAMPUS AKADEMIK PUBLISING
Jurnal Ilmiah Ekonomi Dan Manajemen
Vol.3, No.6 Juni 2025
e-ISSN: 3025-7859; p-ISSN: 3025-7972, Hal 330-346
DOI: https://doi.org/10.61722/jiem.v3i6.5266

Evaluasi Manajemen Risiko Keamanan Siber pada Infrastruktur Digital Pemerintah: Studi Kasus Pusat Data Nasional (PDN)

Syarifa Tommy[1], Muhammad Irwan Padli Nasution[2]
Prodi Manajemen, Fakultas Ekonomi dan Bisnis Islam
Universitas Islam Negeri Sumatera Utara, Medan, Indonesia
Email: syarifatommy12@gmail.com[1], irwannst@gmail.com[2]

Abstract. *The data leak incident that hit the National Data Center (NDC) in June 2024 became one of the biggest cyber crises in the history of the Indonesian government's digital transformation. The attack, which used LockBit 3.0 ransomware, paralyzed hundreds of public services, showing the weakness of the national cybersecurity system and decreasing public trust in the government. This research aims to analyze the chronology, impact, and mitigation strategies that can be applied in overcoming the digital security crisis in the government sector. Using a case study-based qualitative-descriptive study approach, data was collected from documentation, official government reports, scientific journals, and media coverage. The results show that the main causes of data leakage lie in weak security management, absence of data backup, and poor implementation of digital system governance. The study recommends the need for national policy updates, human resource capacity building, and the adoption of cutting-edge security technologies to strengthen government cyber resilience.*

Keywords: *Cybersecurity, data breach, National Data Center, SPBE, ransomware.*

Abstract. *Insiden kebocoran data yang menimpa Pusat Data Nasional (PDN) pada Juni 2024 menjadi salah satu krisis siber terbesar dalam sejarah transformasi digital pemerintahan Indonesia. Serangan yang menggunakan ransomware LockBit 3.0 ini mengakibatkan lumpuhnya ratusan layanan publik, menunjukkan lemahnya sistem keamanan siber nasional dan menurunnya kepercayaan masyarakat terhadap pemerintah. Penelitian ini bertujuan untuk menganalisis kronologi, dampak, serta strategi mitigasi yang dapat diterapkan dalam menanggulangi krisis keamanan digital di sektor pemerintahan. Dengan pendekatan studi kualitatif-deskriptif berbasis studi kasus, data dikumpulkan dari dokumentasi, laporan resmi pemerintah, jurnal ilmiah, serta pemberitaan media. Hasil kajian menunjukkan bahwa penyebab utama kebocoran data terletak pada lemahnya manajemen keamanan, tidak adanya backup data, serta buruknya penerapan tata kelola sistem digital. Studi ini merekomendasikan perlunya pembaruan kebijakan nasional, peningkatan kapasitas SDM, dan adopsi teknologi pengamanan mutakhir untuk memperkuat ketahanan siber pemerintahan.*

Kata kunci*: Keamanan siber, kebocoran data, Pusat Data Nasional, SPBE, ransomware.*

PENDAHULUAN

Dalam era transformasi digital yang semakin pesat, data telah menjadi aset strategis dan fundamental bagi organisasi, baik di sektor publik maupun swasta. Pemerintah

Received April 28, 2025; Revised Mei 31, 2025; Juni 04, 2025
* Ana Marcal, ana.marcha1406@gmail.com

Indonesia melalui kebijakan Sistem Pemerintahan Berbasis Elektronik (SPBE) mendorong digitalisasi layanan publik untuk menciptakan birokrasi yang efisien, transparan, dan akuntabel. Dalam kerangka ini, keberadaan Pusat Data Nasional (PDN) memegang peran krusial sebagai infrastruktur utama yang menghimpun, menyimpan, dan mengelola data dari ratusan instansi pemerintahan secara terpusat. Namun, seiring meningkatnya digitalisasi, kompleksitas risiko yang dihadapi juga bertambah, terutama dalam bentuk ancaman keamanan siber yang semakin canggih dan terorganisir.

Salah satu peristiwa yang menandai krisis keamanan digital nasional adalah insiden kebocoran data PDN pada Juni 2024, yang disebabkan oleh serangan ransomware LockBit 3.0. Serangan ini tidak hanya menyebabkan lumpuhnya layanan publik di berbagai sektor, tetapi juga mengungkapkan kelemahan struktural dalam manajemen keamanan informasi pemerintah, seperti lemahnya kontrol akses, ketiadaan sistem pencadangan (backup), dan minimnya kesiapan dalam menangani insiden siber secara terkoordinasi. Padahal, keberhasilan sistem digital pemerintahan tidak hanya ditentukan oleh ketersediaan infrastruktur teknologi, tetapi juga oleh kualitas manajerial dalam mengelola risiko dan menjamin kontinuitas layanan publik di tengah krisis.

Penelitian ini bertujuan untuk mengisi kekosongan studi mengenai strategi manajemen mitigasi krisis siber di sektor pemerintahan, dengan menyoroti pentingnya penguatan tata kelola, kesiapsiagaan organisasi, dan respons manajerial dalam menghadapi serangan digital yang kompleks.

Meningkatnya ketergantungan terhadap sistem digital dalam pemerintahan dan pelayanan publik membuat isu keamanan siber menjadi semakin krusial. Data Badan Siber dan Sandi Negara (BSSN) mencatat lebih dari 700 juta anomali trafik siber di Indonesia sepanjang tahun 2023, didominasi oleh *malware* dan *ransomware.* Dalam forum nasional Lemhannas RI, keamanan siber bahkan diposisikan sebagai isu strategis dalam dinamika geopolitik global. Tantangan ini tidak hanya membutuhkan inovasi teknologi, tetapi juga kepemimpinan manajerial yang mampu membangun sistem pengamanan yang terstruktur, terstandar, dan siap menghadapi eskalasi serangan digital yang kian kompleks.

Kondisi tersebut mencapai puncaknya dalam insiden kebocoran data PDN pada 20 Juni 2024, ketika ransomware LockBit 3.0 menyerang sistem digital nasional. Ransomware ini bekerja dengan model *Ransomware-as-a-Service* dan dikenal dengan

kecepatannya dalam mengenkripsi data serta sistem pemerasan ganda. Serangan ini menyebabkan lumpuhnya layanan ratusan instansi pemerintah, menandakan kegagalan bukan hanya pada sisi teknis, tetapi juga pada aspek manajemen keamanan data. Ketiadaan mekanisme deteksi dini, lemahnya kebijakan otorisasi akses, serta tidak adanya sistem respons insiden yang terintegrasi menunjukkan perlunya pendekatan manajerial yang lebih komprehensif dalam menjaga integritas dan ketersediaan data strategis negara.

Kasus peretasan PDN yang terjadi di Indonesia saat ini menjadi isu yang mengkhawatirkan publik. PDN merupakan infrastruktur penting yang seharusnya memiliki perlindungan maksimal sebagai wujud tanggung jawab negara dalam menjaga kerahasiaan data pribadi masyarakat. Serangan ini berdampak luas dengan menonaktifkan sebagian layanan pemerintahan yang tergabung dalam SPBE dan memunculkan risiko kebocoran data yang sangat sensitif. Data yang terdampak berpotensi disalahgunakan, baik oleh aktor kriminal siber maupun untuk kepentingan lain yang dapat merugikan negara dan masyarakat. Kasus ini mengungkapkan lemahnya pertahanan keamanan siber nasional pada infrastruktur digital vital dan menjadi cermin bahwa strategi mitigasi yang telah diterapkan masih belum memadai.

Dalam maraknya upaya digitalisasi, isu keamanan data menjadi perhatian utama di berbagai kalangan. Salah satu ancaman paling signifikan dalam era digital saat ini adalah ransomware. Istilah ini berasal dari kata *ransom* (tebusan) dan *malware* (perangkat lunak berbahaya), yang merujuk pada jenis serangan siber yang mengunci data korban dan menuntut tebusan untuk memulihkannya (Hartono, 2023).

Ransomware telah menjadi ancaman global yang serius, menyerang tidak hanya individu dan organisasi, tetapi juga infrastruktur siber-fisik yang vital (Ezekiel, 2024). Malware ini secara aktif mencari file tertentu (misalnya .htm/.html), mengekstrak data seperti alamat email, dan mengirimkannya secara tersembunyi ke server peretas. Beberapa varian bahkan memiliki kemampuan mengunduh file dari internet dan mengeksekusinya secara otomatis pada sistem target.

Jenis serangan ini dapat menyebabkan gangguan besar, termasuk kondisi *Denial-of-Service* (DoS) yang membuat sistem tidak bisa diakses. Ransomware membatasi akses pengguna terhadap data atau perangkat, lalu meminta uang tebusan sebagai syarat pemulihan data. Fenomena ini menunjukkan bahwa tantangan keamanan digital tidak

cukup ditangani secara teknis saja, tetapi juga perlu dikelola melalui pendekatan manajemen keamanan data yang sistematis dan preventif (Rimbarawa dkk., 2021).

Peretasan terhadap Pusat Data Nasional (PDN) merupakan bentuk pelanggaran serius terhadap infrastruktur yang bertanggung jawab dalam penyimpanan dan pengelolaan data berskala nasional (Hafsyah & Darmawan, 2022). Sejak pertama kali digagas pada 1960-an, PDN dirancang untuk meningkatkan efisiensi dan keamanan pengelolaan data strategis dari berbagai sektor, menjadikannya sasaran potensial bagi serangan siber (Chintal, 2014). Dalam perkembangannya, praktik peretasan tidak selalu bersifat destruktif, tetapi juga menunjukkan aspek kreativitas dan inovasi, seperti yang tercermin dalam konferensi komunitas peretas dan pengembangan teknologi berbasis pemrograman terbuka. Peran peretas pun beragam, mulai dari ancaman keamanan hingga kontribusi pada pengembangan teknologi informasi global (Firdaus, 2022).

Berdasarkan evaluasi dari *National Cyber Security Index* (NCSI), tingkat keamanan siber di Indonesia masih tergolong rendah. Indonesia memperoleh skor sebesar 38,96, yang berada di bawah rata-rata global. Temuan ini mengindikasikan bahwa sistem keamanan digital nasional belum sepenuhnya mampu menjamin perlindungan terhadap data dan informasi strategis dari berbagai potensi ancaman siber. Data yang dirilis oleh Badan Siber dan Sandi Negara (BSSN) pada bulan Agustus 2023 mencatat adanya 78.464.385 anomali trafik yang terdeteksi dalam sistem jaringan nasional. Dari jumlah tersebut, jenis ancaman yang paling dominan adalah Trojan, dengan total kasus mencapai 42.857.779. Trojan merupakan salah satu jenis *malware* yang secara umum digunakan untuk memberikan akses tidak sah kepada pihak eksternal terhadap suatu sistem, sehingga berpotensi besar menimbulkan kebocoran atau pencurian data.

Melihat kondisi tersebut, analisis terhadap insiden kebocoran data yang menimpa Pusat Data Nasional (PDN) menjadi sangat penting untuk dilakukan. Penelitian ini bertujuan untuk mengidentifikasi penyebab utama terjadinya insiden, serta merumuskan strategi mitigasi yang relevan dan aplikatif guna mencegah terulangnya kejadian serupa di masa mendatang. Dengan demikian, transformasi digital yang tengah digencarkan oleh pemerintah melalui sistem pemerintahan berbasis elektronik (SPBE) dapat berjalan secara aman, berkelanjutan, dan terpercaya di mata publik.

METODE

Penelitian ini menggunakan pendekatan kualitatif deskriptif dengan metode studi kasus. Fokus utama penelitian adalah insiden serangan *ransomware* LockBit 3.0 yang terjadi pada Pusat Data Nasional (PDN) Sementara 2 di Surabaya pada Juni 2024. Data dikumpulkan melalui studi literatur, laporan resmi pemerintah, dokumentasi akademik, serta artikel berita dari media nasional yang kredibel. Analisis dilakukan dengan cara mengevaluasi kronologi kejadian, menganalisis sistem keamanan yang diterapkan sebelum dan sesudah insiden, serta menelaah respons pemerintah dan dampaknya terhadap masyarakat dan layanan publik. Pendekatan ini bertujuan untuk memberikan gambaran menyeluruh tentang akar permasalahan, serta menyusun strategi mitigasi berbasis data dan kajian empiris.

HASIL DAN PEMBAHASAN

1. Digitalisasi Pemerintah dan Peran Pusat Data Nasional (PDN)

Di tengah pesatnya perkembangan era digital, Pusat Data Nasional (PDN) memiliki peran yang sangat vital bagi pemerintahan. PDN merupakan infrastruktur teknologi yang berfungsi untuk mengelola, menyimpan, serta melindungi data dari berbagai instansi pemerintah secara terpusat. Seiring dengan meningkatnya kebutuhan digitalisasi dan pengintegrasian layanan publik melalui konsep *e-government*, keberadaan PDN menjadi fondasi utama dalam mendorong pemerintahan yang lebih efisien, aman, dan transparan di era transformasi digital. Pusat Data Nasional (PDN) memiliki peran strategis dalam mendukung implementasi Sistem Pemerintahan Berbasis Elektronik (SPBE) di Indonesia. Sebagai infrastruktur utama, PDN berfungsi sebagai pusat penyimpanan, pengelolaan, dan pemulihan data yang digunakan secara bersama oleh instansi pusat dan pemerintah daerah. Hal ini memungkinkan integrasi layanan publik yang lebih efisien dan efektif, serta mendukung interoperabilitas antar sistem pemerintahan.

Menurut Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang SPBE, PDN dirancang untuk meningkatkan kualitas penyelenggaraan layanan SPBE dengan menyediakan infrastruktur yang andal dan terstandarisasi. PDN juga berperan dalam memastikan keamanan dan ketersediaan data pemerintah, yang merupakan aspek krusial dalam penyelenggaraan pemerintahan digital. Dengan adanya PDN, diharapkan terjadi peningkatan efisiensi operasional dan pengurangan duplikasi data antar instansi, sehingga mendukung terciptanya tata kelola pemerintahan yang bersih, transparan, dan

akuntabel. Lebih lanjut, PDN mendukung transformasi digital nasional dengan menyediakan infrastruktur yang memungkinkan integrasi data dan layanan secara menyeluruh. Hal ini sejalan dengan upaya pemerintah dalam mewujudkan pelayanan publik yang berkualitas dan terpercaya melalui pemanfaatan teknologi informasi dan komunikasi. Dengan demikian, PDN menjadi fondasi penting dalam pembangunan sistem pemerintahan yang modern dan responsif terhadap kebutuhan masyarakat.(Hadi & Ayu Putu Sri Widnyani, 2024)

Ketergantungan layanan publik terhadap infrastruktur digital pemerintah semakin meningkat seiring dengan masifnya transformasi digital dalam sektor administrasi dan pelayanan. Pemerintah saat ini banyak mengandalkan sistem digital untuk mendukung berbagai fungsi, mulai dari pengelolaan data kependudukan, layanan kesehatan, pendidikan, hingga perpajakan. Infrastruktur digital seperti Pusat Data Nasional (PDN), jaringan intra-pemerintah, dan sistem aplikasi layanan publik menjadi tulang punggung bagi penyelenggaraan layanan yang cepat, efisien, dan terintegrasi.

Ketika infrastruktur ini terganggu, misalnya karena serangan siber seperti *ransomware* atau kegagalan sistem, dampaknya sangat luas dan langsung dirasakan oleh masyarakat. Misalnya, terhentinya layanan administrasi kependudukan, gangguan dalam sistem informasi rumah sakit, atau lambatnya proses pengajuan perizinan. Hal ini menunjukkan betapa vitalnya keberadaan dan ketahanan infrastruktur digital bagi stabilitas dan keberlanjutan layanan publik.

Menurut Raharjo dan Rahayu (2023) dalam jurnal “Tantangan Keamanan Siber dalam Implementasi SPBE di Indonesia”, disebutkan bahwa ketergantungan ini mengharuskan pemerintah untuk tidak hanya membangun infrastruktur digital yang andal, tetapi juga sistem keamanan siber yang kuat dan responsif. Sebab, potensi risiko yang muncul dari kegagalan sistem atau serangan digital dapat memengaruhi kepercayaan publik terhadap pemerintah secara keseluruhan. Dengan kata lain, keberhasilan digitalisasi layanan publik sangat ditentukan oleh kualitas, keamanan, dan keandalan infrastruktur digital yang menopang sistem pemerintahan. Oleh karena itu, penguatan infrastruktur digital dan mitigasi risiko siber menjadi keharusan dalam menyongsong pemerintahan berbasis elektronik yang berkelanjutan dan terpercaya.

2. Analisis Krisis Kebocoran Pusat Data Nasional (PDN)

Pada pertengahan Juni 2024, Indonesia mengalami sebuah insiden serius terkait keamanan digital yang menyerang sistem Pusat Data Nasional Sementara (PDNS) 2 di Surabaya. Kementerian Komunikasi dan Informatika (Kemenkominfo) sebagai pengelola Pusat Data Nasional (PDN) mengungkapkan bahwa insiden kebocoran data bermula pada malam hari tanggal 17 Juni 2024 pukul 23.15 WIB, ketika fitur keamanan *windows defender* dinonaktifkan. Peretas menonaktifkan antivirus dan mulai menjalankan aksinya dengan menghapus file sistem penting dan mematikan layanan-layanan utama. Dampak dari serangan ini mulai benar-benar dirasakan beberapa hari kemudian, tepatnya pada 20 Juni 2024 pukul 00.54 WIB, ketika layanan publik seperti sistem keimigrasian di bandara terganggu. Banyak masyarakat yang mengalami keterlambatan atau bahkan gagal melakukan perjalanan karena sistem data paspor dan izin keimigrasian tidak bisa diakses.

Layanan proses penerimaan peserta didik baru (PPDB), serta keamanan data pribadi juga menjadi terganggu. Bahkan, data masyarakat yang dicuri berisiko diperjualbelikan secara ilegal, yang bisa mengarah pada penyalahgunaan identitas. Penyalahgunaan ini dapat mencakup pengajuan pinjaman online tanpa izin, pembobolan rekening bank, hingga digunakan dalam tindakan kriminal lainnya. Data-data yang berada di dalam server PDN merupakan data penting negara, seperti Nomor Induk Kependudukan (NIK), Kartu Tanda Penduduk (KTP), nomor ponsel, hingga data-data diri yang bersifat rahasia lainnya. Gangguan ini meluas dan berdampak pada lebih dari 210 instansi pemerintah. Salah satu hal yang cukup mengejutkan dari serangan ini adalah bagaimana peretas bisa masuk ke dalam sistem. Dugaan awal menunjukkan bahwa akses ke sistem diperoleh melalui penggunaan password yang sangat lemah, seperti “Admin#1234”, yang seharusnya mudah ditebak dan tidak layak digunakan dalam sistem penting negara. Setelah masuk, peretas dengan mudah menyebarkan virus ke seluruh jaringan dan mengunci data-data penting milik pemerintah.

Setelah ditelusuri, serangan ini dilakukan oleh kelompok peretas bernama *Brain Cipher*, yang merupakan bagian dari varian *ransomware* terkenal LockBit 3.0. Mereka meminta tebusan sebesar 8 juta dolar AS (sekitar Rp131 miliar) agar data bisa dipulihkan.

Namun, pemerintah Indonesia menolak untuk membayar tebusan tersebut dan memilih melakukan pemulihan secara mandiri. Insiden kebocoran data pada Pusat Data Nasional Sementara (PDNS) 2 di Surabaya pada Juni 2024 menjadi salah satu krisis siber terbesar dalam sejarah digitalisasi pemerintahan Indonesia. Serangan ini tidak hanya melumpuhkan layanan publik, tetapi juga mengungkap kelemahan mendasar dalam sistem keamanan siber nasional. Insiden ini bukan sekadar gangguan biasa, tetapi merupakan serangan siber yang dilakukan dengan menggunakan *ransomware* bernama LockBit 3.0. *Ransomware* ini adalah sejenis virus komputer yang bekerja dengan cara mengunci atau mengenkripsi data penting di sistem, lalu meminta tebusan agar data tersebut bisa dibuka kembali. Jadi, setelah diserang, data-data penting pemerintah menjadi tidak bisa diakses, kecuali jika pemerintah membayar uang tebusan kepada peretas.

Dampak dari insiden tersebut sangat besar, selain layanan publik yang lumpuh, insiden ini juga mengguncang kepercayaan masyarakat terhadap keamanan data di tangan pemerintah. Masyarakat mulai meragukan apakah data pribadi mereka benar-benar aman di sistem pemerintahan, terutama di tengah upaya digitalisasi yang semakin luas. Sistem Pemerintahan Berbasis Elektronik (SPBE), yang seharusnya mendukung efisiensi dan transparansi layanan publik, justru tampak memiliki celah besar dalam hal perlindungan data. Insiden ini telah menjadi perhatian luas, baik di media nasional maupun internasional, dan menjadi momen penting untuk mengevaluasi ulang sistem digital pemerintahan.

Berdasarkan kajian dari jurnal yang ditulis oleh Ramdhan dkk. (2024), insiden ini menunjukkan bahwa proyek strategis seperti PDN harus didukung oleh manajemen keamanan siber yang terstruktur dan profesional, karena data nasional merupakan aset penting yang harus dijaga dengan ketat.

3. Kerentanan dalam Sistem Pusat Data Nasional

Kerentanan dalam sistem Pusat Data Nasional (PDN) menjadi sorotan besar pasca insiden serangan *ransomware* LockBit 3.0 yang terjadi pada pertengahan Juni 2024. Serangan ini mengungkap berbagai kelemahan mendasar dalam pengelolaan infrastruktur digital pemerintah, yang semestinya menjadi tulang punggung sistem pemerintahan berbasis elektronik (SPBE). Salah satu kerentanan utama adalah lemahnya sistem

keamanan siber yang diterapkan oleh pengelola PDN. Berdasarkan laporan dari berbagai sumber, sistem pertahanan seperti antivirus *Windows Defender* secara sengaja dimatikan oleh pelaku pada malam hari menjelang serangan. Ini menunjukkan kurangnya pengawasan dan deteksi dini terhadap aktivitas mencurigakan di dalam sistem. Yang lebih mengkhawatirkan, akses awal ke server PDN ternyata diperoleh hanya dengan menggunakan kata sandi yang sangat lemah dan mudah ditebak, yaitu "Admin#1234". Penggunaan sandi semacam ini menunjukkan bahwa tata kelola keamanan digital belum mengikuti standar dasar keamanan siber yang baik.

Selain itu, tidak adanya sistem pencadangan (*backup*) data yang layak memperburuk situasi. Ketika data dikunci oleh *ransomware*, seharusnya instansi pemerintah bisa segera memulihkan sistem dari salinan cadangan. Namun, kelalaian dalam menyiapkan backup justru membuat proses pemulihan menjadi rumit dan memakan waktu yang lama. Hal ini mengindikasikan bahwa aspek kesiapsiagaan terhadap ancaman siber masih jauh dari kata ideal. Kelemahan lainnya juga terletak pada keterbatasan dalam koordinasi antar-lembaga. Meski PDN dikelola oleh Kementerian Komunikasi dan Informatika (Kominfo), penanganan insiden memerlukan sinergi dengan Badan Siber dan Sandi Negara (BSSN), serta lembaga teknis lainnya.

Dalam praktiknya, koordinasi ini tampak lamban dan tidak efisien, yang berkontribusi terhadap lambatnya proses pemulihan. Dampak dari kerentanan ini sangat luas. Gangguan sistem mempengaruhi lebih dari 200 instansi, termasuk layanan krusial seperti imigrasi, pendidikan, dan catatan sipil. Ketergantungan layanan publik terhadap infrastruktur digital membuat setiap celah keamanan menjadi ancaman serius terhadap pelayanan masyarakat. Oleh karena itu, penguatan sistem keamanan PDN perlu dilakukan secara menyeluruh, tidak hanya melalui teknologi, tetapi juga dari sisi kebijakan, prosedur operasional, dan peningkatan kapasitas sumber daya manusia. (Hendrawan, Kusnadi 2023).

4. Implikasi Kebocoran Data terhadap Pemerintah dan Masyarakat

Insiden peretasan terhadap Pusat Data Nasional (PDN) menjadi sinyal kuat bahwa pemerintah belum sepenuhnya siap dalam menghadapi ancaman keamanan siber. Dari sisi regulasi, memang sudah terdapat sejumlah dasar hukum seperti Undang-Undang Informasi dan Transaksi Elektronik (UU ITE), Undang-Undang Perlindungan Data

Pribadi (UU PDP), serta Peraturan Presiden Nomor 47 Tahun 2023, sehingga kekosongan hukum sebenarnya tidak terjadi. Namun, yang menjadi sorotan utama adalah bagaimana aturan-aturan tersebut dijalankan di lapangan. Kurangnya implementasi yang efektif membuat sistem keamanan siber nasional rentan. Jika ke depannya pemerintah tidak segera melakukan evaluasi dan perbaikan menyeluruh terhadap pelaksanaan aturan tersebut, maka beragam dampak negatif bisa terjadi. Kebocoran data dari Pusat Data Nasional (PDN) bukan sekadar masalah teknis atau serangan siber biasa, ini adalah krisis nasional yang menyentuh berbagai aspek kehidupan masyarakat dan menguji kemampuan pemerintah dalam mengelola keamanan digital di era modern. PDN merupakan infrastruktur vital yang menyimpan data dari ratusan lembaga pemerintah, termasuk data pribadi jutaan warga negara. Maka, ketika PDN diretas, dampaknya bisa meluas dan serius.

Dari sisi pemerintah, kebocoran ini langsung memengaruhi kepercayaan publik terhadap kapabilitas negara dalam menjaga data warganya. Layanan-layanan digital yang seharusnya mempermudah masyarakat, seperti sistem imigrasi, administrasi kependudukan, pendaftaran pendidikan, dan berbagai layanan online lainnya, bisa lumpuh. Contohnya saat insiden ini terjadi, layanan imigrasi di bandara terganggu, menyebabkan banyak penumpang tertahan dan gagal bepergian karena sistem data paspor tidak bisa diakses. Selain itu, lebih dari 210 instansi pemerintahan terkena dampak gangguan sistem akibat serangan ini.

Secara internal, serangan ini menunjukkan adanya kelemahan dalam tata kelola keamanan siber pemerintah, seperti penggunaan kata sandi lemah (“Admin#1234”) dan tidak adanya backup data yang memadai. Padahal, dalam pengelolaan data vital negara, standar keamanan seperti enkripsi kuat, audit sistem berkala, serta redundansi data (*backup*) adalah hal yang seharusnya wajib dilakukan. Karena kelalaian ini, pemerintah tidak hanya mengalami kerugian secara operasional, tetapi juga dari sisi citra dan reputasi nasional, baik di mata masyarakat maupun dunia internasional.

Sementara itu, bagi masyarakat, implikasinya bahkan lebih mengkhawatirkan. Kebocoran data pribadi seperti nama, alamat, nomor identitas, data keuangan, bahkan rekam medis membuka peluang besar untuk terjadinya berbagai bentuk kejahatan digital. Misalnya, data yang bocor dapat digunakan oleh pihak tidak bertanggung jawab untuk melakukan penipuan, mengajukan pinjaman online ilegal, membobol rekening bank,

hingga menyalahgunakan identitas untuk kegiatan kriminal. Ini semua bisa terjadi karena data yang seharusnya hanya dimiliki oleh pemerintah, kini jatuh ke tangan peretas atau bahkan diperjualbelikan di internet gelap (*dark web*).

Ketika masyarakat merasa data pribadinya tidak aman, kepercayaan terhadap sistem digital pemerintah menurun drastis. Mereka akan ragu untuk menggunakan layanan e-government atau menyerahkan data pribadinya kepada instansi pemerintah. Dalam jangka panjang, hal ini bisa menghambat proses transformasi digital nasional, yang selama ini digencarkan untuk meningkatkan efisiensi, transparansi, dan keterbukaan layanan publik. Krisis ini juga mengungkapkan adanya kesenjangan besar antara ambisi digital pemerintah dan kesiapan teknis yang sebenarnya. Pemerintah Indonesia telah mencanangkan visi SPBE (Sistem Pemerintahan Berbasis Elektronik), namun kasus kebocoran PDN membuktikan bahwa landasan keamanannya belum kuat. Oleh karena itu, perlu ada langkah serius dan menyeluruh untuk membenahi kebijakan, infrastruktur, dan sumber daya manusia di bidang keamanan siber.

Salah satu dampak yang paling mungkin muncul adalah menurunnya kepercayaan publik terhadap pemerintah. Masyarakat bisa mempertanyakan keseriusan dan profesionalisme pemerintah dalam menjaga data pribadi mereka, terutama bila sampai terjadi kehilangan data akibat tidak adanya sistem cadangan atau backup yang memadai. Jika kepercayaan ini hilang, maka implikasinya tidak hanya terbatas pada persepsi negatif, tetapi juga bisa meluas ke gangguan dalam aktivitas sosial dan ekonomi. Ketika masyarakat merasa tidak aman secara digital, maka roda pemerintahan dan ekonomi pun bisa terganggu. Kebocoran data dari Pusat Data Nasional (PDN) bukan sekadar masalah teknis atau serangan siber biasa, ini adalah krisis nasional yang menyentuh berbagai aspek kehidupan masyarakat dan menguji kemampuan pemerintah dalam mengelola keamanan digital di era modern. PDN merupakan infrastruktur vital yang menyimpan data dari ratusan lembaga pemerintah, termasuk data pribadi jutaan warga negara. Maka, ketika PDN diretas, dampaknya bisa meluas dan serius.

5. Evaluasi Respons dan Penanganan Insiden oleh Pemerintah

Penanganan insiden kebocoran data di Pusat Data Nasional (PDN) menunjukkan bahwa Indonesia masih memiliki banyak pekerjaan rumah dalam hal keamanan siber. Agar kejadian serupa tidak terulang, pemerintah perlu belajar dari negara lain yang sudah

terbukti sukses membangun sistem keamanan digital yang kuat, salah satunya adalah Belanda. Belanda merupakan contoh negara yang sangat siap dalam menangani ancaman siber. Mereka telah memiliki regulasi khusus seperti *Network* and Information *Systems Security Act* (NISSA) yang secara hukum mengatur keamanan sistem digital. Selain itu, Belanda memiliki pedoman yang sangat terstruktur, seperti *national manual on decision-making in crisis situation* dan *national digital crisis plan*. Kedua panduan ini tidak hanya mengatur cara penanganan ketika krisis siber terjadi, tapi juga mencakup langkah-langkah persiapan dan pencegahan. Menariknya, panduan ini berlaku tidak hanya untuk pemerintah, tapi juga untuk organisasi swasta, manajer, direktur, bahkan hingga karyawan biasa, sehingga semua pihak paham bagaimana merespons serangan siber.

Sebaliknya, di Indonesia saat ini, sistem penanganan krisis siber masih terbatas pada tingkat nasional saja, belum menjangkau perusahaan swasta atau organisasi lain secara menyeluruh. Selain itu, Indonesia belum memiliki undang-undang khusus yang benar-benar mengatur keamanan siber secara komprehensif. Selama ini, penanganan ancaman digital masih bertumpu pada beberapa regulasi yang tersebar, seperti UU ITE, UU Perlindungan Data Pribadi (PDP), dan Perpres tentang SPBE, namun belum cukup kuat untuk menangani kasus seperti serangan ransomware. Menariknya, pada Oktober 2023, Indonesia dan Belanda telah menjalin kerja sama di bidang keamanan siber. Ini seharusnya menjadi momentum penting bagi Indonesia untuk belajar langsung dari Belanda, baik dari sisi teknologi, kebijakan, hingga pelatihan keahlian teknis.

Untuk memperbaiki sistem yang ada, ada beberapa hal penting yang harus dilakukan pemerintah Indonesia. Pertama, pemerintah harus segera mengesahkan RUU Keamanan Siber sebagai payung hukum utama. Regulasi ini akan menjadi dasar yang kuat dan jelas untuk semua langkah keamanan digital yang diterapkan, baik di institusi publik maupun swasta. Kedua, sistem keamanan yang digunakan oleh institusi penting seperti PDN harus ditingkatkan secara serius. Tidak cukup hanya mengandalkan sistem lama yang mungkin sudah tidak relevan dengan jenis ancaman terbaru. Pemerintah juga harus rutin melakukan pengujian sistem keamanan melalui *cyber security testing*, yang mencakup audit keamanan, tes penetrasi, pemindaian kerentanan, serta penilaian risiko. Tujuannya adalah untuk mengetahui celah-celah yang bisa dimanfaatkan peretas dan segera memperbaikinya sebelum diserang. Ketiga, sumber daya manusia yang mengelola sistem digital pemerintahan juga harus dibekali pelatihan intensif. Para teknisi dan tim IT di

instansi pemerintah perlu mendapatkan pembelajaran rutin tentang perkembangan serangan siber dan cara-cara pencegahannya. Mereka juga harus diajarkan untuk berpikir seperti hacker agar bisa memprediksi celah mana yang mungkin diserang.

Secara keseluruhan, untuk menghadapi era digital yang semakin kompleks, Indonesia harus membangun sistem keamanan yang tidak hanya berbasis teknologi, tetapi juga kebijakan, prosedur, dan kesiapan sumber daya manusia. Dengan persiapan yang matang dan evaluasi yang berkelanjutan, Indonesia bisa lebih siap menghadapi ancaman digital dan membangun kepercayaan publik yang lebih kuat terhadap sistem pemerintahannya.

6. Strategi Mitigasi Kebocoran Data di Era Digitalisasi Pemerintah

Strategi mitigasi kebocoran data di era digitalisasi pemerintah mencakup sejumlah langkah sistematis yang dirancang untuk memperkuat perlindungan terhadap data masyarakat dan memastikan keberlanjutan layanan publik. Pemerintah perlu membangun sistem keamanan siber yang tidak hanya bersifat reaktif, tetapi juga proaktif dan preventif (Soleh & Tjenreng, 2024).

Pertama, penguatan infrastruktur keamanan menjadi langkah paling mendasar. Pemerintah harus memastikan bahwa seluruh sistem penyimpanan dan pengolahan data dilindungi dengan teknologi enkripsi yang kuat, *firewall*, serta sistem deteksi dan pencegahan intrusi (IDS/IPS). Selain itu, penting untuk melakukan segmentasi jaringan dan pembatasan akses agar data sensitif tidak mudah diakses oleh pihak yang tidak berwenang. Kedua, strategi mitigasi harus mencakup penerapan kebijakan pengelolaan kata sandi yang ketat. Kasus seperti penggunaan password lemah "Admin#1234" dalam insiden PDN menunjukkan lemahnya kesadaran keamanan digital. Oleh karena itu, penerapan otentikasi multi-faktor (*multi-factor authentication*/MFA) menjadi krusial dalam memperkuat lapisan keamanan akses. Ketiga, pentingnya membangun budaya keamanan siber di seluruh elemen pemerintahan. Edukasi dan pelatihan rutin kepada aparatur sipil negara (ASN) mengenai praktik keamanan informasi harus dilakukan secara berkelanjutan. ASN sebagai operator sistem harus memahami cara kerja sistem serta risiko-risiko siber yang mungkin timbul. Keempat, pemerintah wajib memiliki sistem backup data secara berkala di lokasi yang berbeda (*offsite*), sehingga ketika terjadi

serangan atau kegagalan sistem, data masih dapat dipulihkan dan layanan publik tetap berjalan.

Ketidaksiapan backup data seperti yang terjadi dalam insiden PDN menjadi pelajaran penting bagi tata kelola digital yang lebih profesional. Kelima, perlu dibentuk tim tanggap insiden (*incident response team*) yang siaga 24/7 dan memiliki kewenangan penuh untuk menangani serangan siber secara cepat dan terkoordinasi. Tim ini bertugas melakukan investigasi forensik digital, pemulihan sistem, dan analisis kerentanan agar kejadian serupa tidak terulang. Terakhir, penguatan regulasi dan penegakan hukum terkait keamanan data juga menjadi aspek vital. Pemerintah harus mempercepat harmonisasi dan implementasi Undang-Undang Perlindungan Data Pribadi (UU PDP), serta menyusun Peraturan Pemerintah (PP) pelaksanaannya secara menyeluruh agar setiap pelanggaran dapat direspons secara tegas dan berkeadilan (Adristi, 2024).

Menurut Handayani et al. (2022) dalam jurnal Jurnal Keamanan Siber Indonesia, pendekatan mitigasi kebocoran data yang efektif harus mencakup aspek teknologi, sumber daya manusia, dan regulasi secara sinergis. Mereka menekankan pentingnya audit keamanan berkala dan pengujian penetrasi untuk mengukur ketahanan sistem terhadap ancaman yang terus berkembang. Dengan menerapkan strategi-strategi tersebut secara konsisten dan menyeluruh, pemerintah dapat membangun sistem digital yang tidak hanya efisien, tetapi juga aman dan terpercaya dalam melayani masyarakat di era transformasi digital.

KESIMPULAN

Dalam perspektif peneliti, data tidak semata-mata dipahami sebagai himpunan informasi digital, melainkan merupakan aset strategis negara yang merepresentasikan kepercayaan publik terhadap institusi pemerintahan. Di era transformasi digital, data mencerminkan dimensi identitas, hak, dan kepentingan warga negara yang menuntut pengelolaan secara profesional, transparan, serta aman. Oleh karena itu, pengelolaan data tidak cukup dilakukan melalui solusi teknis sesaat, melainkan harus dilandasi oleh kerangka manajemen risiko yang terstruktur, sistematis, dan berbasis prinsip-prinsip tata kelola yang baik (*good governance*).

Melalui kajian terhadap insiden kebocoran data pada Pusat Data Nasional (PDN) tahun 2024, penelitian ini mengungkap bahwa peristiwa tersebut tidak semata disebabkan oleh serangan siber eksternal, tetapi merupakan manifestasi dari kegagalan struktural

dalam manajemen keamanan informasi di lingkungan pemerintahan. Berbagai kelemahan seperti lemahnya pengendalian akses, ketiadaan sistem pencadangan data yang memadai, serta buruknya koordinasi antarinstansi, memperlihatkan bahwa infrastruktur digital nasional belum memiliki kapasitas manajerial yang cukup untuk menghadapi dinamika ancaman siber yang semakin kompleks.

Dengan demikian, temuan ini menggarisbawahi urgensi penerapan pendekatan manajerial dalam mitigasi krisis keamanan siber, khususnya dalam kerangka tata kelola sektor publik. Keamanan data seharusnya tidak hanya dipandang sebagai isu teknis, tetapi juga sebagai cerminan kapasitas institusional dan kredibilitas negara dalam menjalankan agenda digitalisasi pemerintahan. Oleh karena itu, diperlukan strategi yang bersifat holistik, meliputi pembaruan regulasi, peningkatan kapasitas sumber daya manusia, serta internalisasi budaya keamanan informasi di seluruh jenjang birokrasi untuk mewujudkan sistem pemerintahan digital yang berkelanjutan dan mendapatkan legitimasi dari masyarakat.

Hasil penelitian ini menyoroti pentingnya perubahan paradigma dalam pendekatan pemerintah terhadap isu keamanan data, dari yang semula bersifat reaktif dan teknis menjadi lebih strategis dan berbasis manajerial. Kelemahan dalam tata kelola Pusat Data Nasional (PDN) menunjukkan bahwa keberadaan regulasi yang bersifat normatif tidak akan efektif apabila tidak didukung oleh implementasi yang konsisten serta mekanisme pengawasan yang berkelanjutan. Dalam konteks ini, diperlukan kebijakan yang tidak hanya menetapkan standar minimum keamanan informasi, tetapi juga mewajibkan penerapan protokol manajemen risiko siber secara sistematis oleh setiap instansi publik. Protokol tersebut mencakup pelaksanaan audit keamanan secara berkala, peningkatan kapasitas sumber daya manusia melalui pelatihan teknis, serta pengembangan sistem kesiapsiagaan dalam menghadapi potensi krisis siber.

Selain itu, penguatan kebijakan mitigasi serangan siber menuntut adanya perumusan kerangka kerja nasional yang bersifat lintas sektor dan berbasis sinergi antarinstansi. Kolaborasi fungsional antara Kementerian Komunikasi dan Informatika (Kominfo), Badan Siber dan Sandi Negara (BSSN), serta berbagai lembaga yang memiliki otoritas dalam pengelolaan data, perlu diwujudkan dalam bentuk sistem koordinasi yang terintegrasi dan saling mendukung. Pendekatan kerja yang bersifat sektoral dan terfragmentasi (silo) justru akan memperlemah efektivitas pengawasan serta respons

terhadap ancaman siber yang semakin kompleks. Tanpa adanya integrasi kebijakan dan mekanisme pelaksanaan yang menyeluruh, kerentanan infrastruktur informasi nasional berpotensi terus menjadi hambatan krusial dalam mewujudkan agenda transformasi digital yang aman, efisien, dan berkelanjutan.

BILIOGRAFI

Adristi, FI, & Ramadhani, E. (2024). Analisis Dampak Kebocoran Data Pusat Data Nasional Sementara 2 (PDNS 2) Surabaya: Pendekatan Matriks Budaya Keamanan Siber dan Dimensi Budaya Nasional Hofstede. Selekta Manajemen: Jurnal Mahasiswa Bisnis & Manajemen , 2 (6), 196–212.

Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia. (2023). *Jurnal Kajian Stratejik Ketahanan Nasional*, *6* (2). https://doi.org/10.7454/jkskn.v6i2.10082

BSSN. (2023). *Laporan Tahunan Keamanan Siber Indonesia*. Jakarta: Badan Siber dan Sandi Negara. Kementerian Komunikasi dan Informatika. (2023). *Pedoman Umum SPBE*.

Budi, E., Wira, D., & Infantono, A. (2021). Strategi Penguatan Cyber Security Guna Mewujudkan Keamanan Nasional di Era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi Dan Inovasi Indonesia (SENASTINDO)*, *3*, 223–234. https://doi.org/10.54706/senastindo.v3.2021.141

Firdaus, I. (2022). Upaya Perlindungan Hukum Hak Privasi Terhadap Data Pribadi dari Kejahatan Peretasan. Jurnal Rechten : Riset Hukum dan Hak Asasi Manusia, 4(2), 23–31. https://doi.org/10.52005/rechten.v4i2.98

Hartono, B. (2023). Ransomware: Memahami Ancaman Keamanan Digital. Bincang Sains dan Teknologi, 2(02), 55–62. https://doi.org/10.56741/bst.v2i02.353

Hafsyah, A., & Darmawan, A. (2022). Analisis Isi Berita Kebocoran Data Pribadi Jokowi ke Publik (Studi Pada Media Online Tempo. co Edisi 3-5 September 2021). Nasional Hasil Skripsi, september. https://conference.untag-sby.ac.id/index.php/snhs/article/view/939%0Ahttps://conference.untag,sby.ac.id/index.php/snhs/article/download/939/414

Hadi, I., &Ayu Putu Sri Widnyani, I. (2024). Modernisasi dan Digitalisasi Public Servis: Mewujudkan Indonesia Emas Melalui Harmonisasi Sistem Pemerintahan

Berbasis Elektronik (SPBE).Hendrawan, K. (2023). Analisis Strategi Keamanan Siber Pada Infrastuktur Pemerintah Indonesia: Studi Kasus Pusat Data Nasional. Jurnal Teknologi Informasi Dan Keamanan Siber, 01, 45–60.

Soleh, M., & Tjenreng, Z. (2024). Strategi Pencegahan Kebocoran Data Pelayanan Publik Di Era Digital. Jurnal Kajian Pemerintah (JKP): Journal Of Government, Social and Politics, 11(1), 1–10. https://doi.org/10.31219/osf.io/placeholderhttps://journal.uii.ac.id/selma/article/view/35529

Tempo. (2024). *Serangan Siber Ganggu Layanan Publik, PDN Diserang Ransomware*. Diakses dari tempo.co