DATA CYBER INDONESIA

Ruang Riset Siber Indonesia

Tantangan Kedaulatan Digital: Evaluasi Ketahanan Siber pada Sistem Pemerintahan Berbasis Elektronik (SPBE) di Indonesia

Penulis:

Sigit Waluyo

Peneliti Profesional, Data Cyber Indonesia

Email: sigitwaluyo@datacyber.or.id

Website: https://datacyber.or.id

Tanggal Terbit: 08 November 2026

DOI: 10.5281/zenodo.24048956

Lisensi: CC BY 4.0 (Creative Commons Attribution)

Kode Verifikasi: DCY-RISET-2026-091

Tantangan Kedaulatan Digital: Evaluasi Ketahanan Siber pada Sistem Pemerintahan Berbasis Elektronik (SPBE) di Indonesia

Abstrak

Sistem Pemerintahan Berbasis Elektronik (SPBE) merupakan tulang punggung transformasi digital Indonesia. Namun, di balik narasi kemajuan indeks kematangan SPBE yang meningkat dari 2,34 (2022) menjadi 3,12 (2024), terdapat realitas yang mengkhawatirkan: paparan data pribadi di darknet melonjak 33,5 kali lipat, serangan siber mencapai 5,5 miliar anomali pada 2025, dan insiden kebocoran data pada Pusat Data Nasional Sementara (PDNS) mengungkap bahwa hanya 2% data yang dicadangkan. Lebih parah, dari 8 insiden siber yang dilaporkan, 5 di antaranya tidak dikonfirmasi secara resmi. Riset ini bertujuan mengevaluasi secara kritis ketahanan siber SPBE dengan membedah jurang antara kepatuhan administratif (skor indeks) dan ketahanan operasional riil. Metode yang digunakan adalah analisis kualitatif-deskriptif terhadap data sekunder dari BSSN, jurnal akademik, dan studi kasus insiden. Temuan utama riset ini: (1) Indeks kematangan SPBE mengukur kepatuhan proses, bukan ketahanan aktual; (2) Terdapat jurang antara skor tinggi dan kesiapan operasional yang rendah, seperti terlihat pada kasus PDNS; (3) Lemahnya transparansi dan pengungkapan insiden menciptakan risiko kedaulatan data yang serius; (4) Pemerintah daerah menghadapi tantangan lebih besar, dengan 103 notifikasi insiden (23%) masih berstatus need action. Riset ini menyimpulkan bahwa kedaulatan digital Indonesia tidak bisa hanya diukur dari skor indeks. Diperlukan pergeseran paradigma dari kepatuhan administratif menuju kesiapan operasional nyata, transparansi insiden, dan penguatan kapasitas SDM keamanan siber di seluruh lini pemerintahan.

1. Latar Belakang

Transformasi digital pemerintahan melalui Sistem Pemerintahan Berbasis Elektronik (SPBE) adalah keniscayaan. Sejak Peraturan Presiden No. 95 Tahun 2018 tentang SPBE diteken, pemerintah berkomitmen membangun tata kelola pemerintahan yang efisien, transparan, dan terintegrasi. Indeks SPBE pun menjadi tolok ukur keberhasilan yang bergengsi. Namun, di balik gemerlapnya skor indeks, terdapat realitas gelap yang jarang terungkap: kebocoran data pribadi, serangan siber yang masif, dan lemahnya transparansi insiden. Jurnal akademik dari Universitas Negeri Makassar (2026) membongkar paradoks ini secara tajam. Indeks SPBE nasional naik dari 2,34 (2022) menjadi 3,12 (2024), tetapi paparan data di darknet melonjak 33,5 kali lipat. Serangan siber mencapai 5,5 miliar pada 2025. Insiden PDNS menimpa instansi dengan skor SPBE tertinggi, tetapi hanya 2% data yang dicadangkan. Dari 8 insiden, 5

tidak dikonfirmasi resmi. Ini adalah pukulan telak bagi narasi kemajuan. Riset ini hadir untuk membedah lebih dalam: Apakah kedaulatan digital Indonesia sedang dipertaruhkan?

2. Rumusan Masalah

1. Bagaimana ketahanan siber SPBE di Indonesia dievaluasi berdasarkan data insiden dan kerentanan aktual?
2. Mengapa terjadi jurang antara skor kematangan SPBE dan ketahanan operasional riil di lapangan?
3. Apa implikasi dari lemahnya transparansi dan pengungkapan insiden siber terhadap kedaulatan data Indonesia?
4. Apa strategi yang diperlukan untuk menutup jurang antara kepatuhan administratif dan kesiapan operasional?

3. Tujuan

1. Mengevaluasi ketahanan siber SPBE secara kritis berbasis data insiden.
2. Membedah penyebab jurang antara skor indeks dan ketahanan aktual.
3. Menganalisis implikasi lemahnya transparansi insiden terhadap kedaulatan data.
4. Merumuskan strategi perbaikan yang komprehensif.

4. Batasan Masalah

Objek kajian adalah ketahanan siber SPBE di Indonesia pada periode 2023–2026. Data bersumber dari laporan resmi BSSN, jurnal akademik, regulasi terkait, dan pemberitaan media massa. Penelitian tidak melakukan audit teknis langsung terhadap sistem pemerintah, melainkan analisis sekunder terhadap data yang dipublikasikan.

5. Tinjauan Pustaka

Kajian ini merujuk pada Peraturan Presiden No. 95 Tahun 2018 tentang SPBE sebagai landasan hukum utama. Jurnal akademik dari Pinisi Journal of Public Policy (Universitas Negeri Makassar, 2026) yang berjudul "Kontradiksi Kematangan SPBE dan Kerentanan Data Pribadi pada Instansi Publik Indonesia 2023–2026" menjadi tulang punggung analisis kritis. Data resmi dari BSSN tentang lanskap ancaman siber 2026 (5,5 miliar anomali trafik, rata-rata 180 anomali per detik) dan laporan insiden di pemerintah daerah (500 notifikasi, 103 need action) melengkapi data empiris. Kerangka kerja NIST Cybersecurity Framework 2.0 (Govern, Identify, Protect, Detect, Respond, Recover) digunakan sebagai pisau analisis untuk mengevaluasi kesiapan operasional.

6. Metodologi

Penelitian menggunakan pendekatan kualitatif-deskriptif dengan metode studi dokumentasi dan analisis isi (content analysis). Data dikumpulkan dari literatur akademik, laporan resmi pemerintah, dan pemberitaan media massa. Analisis dilakukan secara tematik untuk mengidentifikasi pola, paradoks, dan implikasi dari data yang tersedia.

7. Teknik Analisis

Analisis tematik dan kritis terhadap data insiden, skor indeks, dan literatur. Data disajikan secara deskriptif-analitis untuk membedah jurang antara kepatuhan administratif dan ketahanan operasional.

8. Hasil

1. Indeks kematangan SPBE nasional naik dari 2,34 (2022) menjadi 3,12 (2024), tetapi paparan data pribadi di darknet melonjak 33,5 kali lipat pada periode yang sama.
2. Serangan siber mencapai 5,5 miliar anomali pada 2025, dengan rata-rata 180 anomali per detik.
3. Insiden PDNS menimpa instansi dengan skor SPBE tertinggi, tetapi hanya 2% data yang dicadangkan.
4. Dari 8 insiden siber yang dilaporkan, 5 di antaranya tidak dikonfirmasi secara resmi.
5. Di pemerintah daerah, terdapat 500 notifikasi indikasi insiden pada 2026, dengan 103 notifikasi (23%) masih berstatus need action.
6. Pendaftaran TTIS (Tim Tanggap Insiden Siber) tidak menjamin kesiapan operasional riil.

9. Pembahasan

Temuan riset ini membongkar tiga paradoks besar dalam ketahanan siber SPBE. Paradoks pertama adalah paradoks metrik: Indeks kematangan SPBE mengukur kepatuhan proses (apakah dokumen ada, apakah SOP dijalankan), bukan ketahanan aktual (apakah sistem benar-benar aman dari serangan). Naiknya skor indeks tidak berkorelasi dengan menurunnya insiden kebocoran data. Paradoks kedua adalah paradoks prioritas: Kasus PDNS adalah contoh paling telanjang. Instansi dengan skor SPBE tertinggi justru menjadi korban, dan yang lebih memilukan, hanya 2% data yang dicadangkan. Ini menunjukkan bahwa investasi pada kepatuhan administratif tidak diimbangi dengan investasi pada infrastruktur ketahanan. Paradoks ketiga adalah paradoks transparansi: Dari 8 insiden, 5 tidak dikonfirmasi resmi. Ketertutupan ini menciptakan ruang gelap yang menyuburkan spekulasi, merusak kepercayaan publik, dan membahayakan kedaulatan data. Jika insiden tidak diungkap secara transparan, bagaimana mungkin evaluasi dan perbaikan bisa dilakukan? Di tingkat pemerintah

daerah, tantangannya lebih berat. 103 notifikasi need action berarti hampir seperempat insiden belum tertangani. Pendaftaran TTIS tanpa kesiapan operasional adalah ilusi. Kedaulatan digital bukan hanya soal memiliki sistem sendiri, tetapi soal mampu melindungi sistem itu dari ancaman. Saat ini, Indonesia masih terjebak pada retorika kemajuan indeks, sementara kerentanan riil terus menganga.

10. Kesimpulan

Kedaulatan digital Indonesia sedang diuji. Skor kematangan SPBE yang meningkat tidak serta-merta mencerminkan ketahanan siber yang tangguh. Terdapat jurang yang lebar antara kepatuhan administratif dan kesiapan operasional riil. Lemahnya transparansi insiden, rendahnya kesiapan backup, dan belum tuntasnya penanganan insiden di daerah adalah alarm merah yang tidak bisa diabaikan. Diperlukan pergeseran paradigma: dari sekadar mengejar skor indeks menuju pembangunan ketahanan siber yang nyata, terukur, dan transparan.

11. Rekomendasi

1. Reformasi indeks SPBE: Tambahkan komponen penilaian ketahanan siber riil (frekuensi insiden, waktu deteksi, waktu pemulihan, persentase data yang dicadangkan) ke dalam indikator SPBE.
2. Kewajiban transparansi insiden: Buat regulasi yang mewajibkan instansi pemerintah mengungkapkan insiden siber yang dialami kepada publik dalam waktu tertentu, dengan tetap melindungi informasi sensitif.
3. Audit backup dan pemulihan: Lakukan audit menyeluruh terhadap kesiapan backup dan rencana pemulihan bencana (disaster recovery plan) di semua instansi pemerintah, dengan target minimal 80% data kritis dicadangkan secara terpisah.
4. Penguatan kapasitas SDM: Tingkatkan jumlah dan kompetensi analis keamanan siber di instansi pemerintah, terutama di daerah.
5. Integrasi NIST CSF 2.0: Adopsi kerangka kerja NIST Cybersecurity Framework 2.0 secara sistematis, bukan hanya sebagai dokumen, tetapi sebagai panduan operasional.
6. Kerja sama lintas lembaga: Perkuat sinergi antara BSSN, Kominfo/Komdigi, BPK, dan instansi daerah untuk berbagi informasi ancaman dan praktik terbaik.

12. Keterbatasan Riset

Penelitian ini hanya menggunakan data sekunder dari literatur, laporan resmi, dan pemberitaan media. Tidak ada audit teknis langsung atau wawancara dengan pengelola SPBE. Temuan bergantung pada akurasi dan kelengkapan sumber yang tersedia untuk publik. Beberapa data insiden mungkin tidak terungkap sepenuhnya

karena keterbatasan transparansi.

Daftar Pustaka

Peraturan Presiden Republik Indonesia Nomor 95 Tahun 2018 tentang Sistem Pemerintahan Berbasis Elektronik (SPBE).
Ayuni, N., Gusmayanti, E. S., & Angreini, N. (2026). Kontradiksi Kematangan SPBE dan Kerentanan Data Pribadi pada Instansi Publik Indonesia 2023–2026. Pinisi Journal of Public Policy, Universitas Negeri Makassar.
Badan Siber dan Sandi Negara (BSSN). (2026). BSSN Tekankan Penguatan Ketahanan Siber untuk Menjaga Keberlanjutan Ekonomi Digital dan Industri Nasional.
Badan Siber dan Sandi Negara (BSSN). (2026). BSSN Dorong Pemerintah Daerah Alihkan Fokus TTIS ke Kesiapan Operasional Nyata.

Halaman Verifikasi

Dokumen ini diterbitkan secara resmi oleh Data Cyber Indonesia. Pindai QR code di bawah untuk memverifikasi keaslian dokumen ini melalui website kami.

Pindai atau buka tautan berikut untuk memverifikasi:
https://datacyber.or.id/verifikasi/DCY-RISET-2026-091

Kode Verifikasi: DCY-RISET-2026-091

DOI: 10.5281/zenodo.24048956

Lisensi: CC BY 4.0

Diterbitkan oleh Data Cyber Indonesia

Tanggal: 08 November 2026