DATA CYBER INDONESIA

Ruang Riset Siber Indonesia

Analisis Kerentanan Ransomware pada Infrastruktur Kritis Perbankan Indonesia Tahun 2026: Vektor Serangan dan Strategi Mitigasi

Penulis:

Muhammad Rizky Alatas

Peneliti Profesional, Data Cyber Indonesia

Email: muhammadrizkyalatas@datacyber.or.id

Website: https://datacyber.or.id

Tanggal Terbit: 08 November 2026

DOI: 10.5281/zenodo.24048626

Lisensi: CC BY 4.0 (Creative Commons Attribution)

Kode Verifikasi: DCY-RISET-2026-088

Analisis Kerentanan Ransomware pada Infrastruktur Kritis Perbankan Indonesia Tahun 2026: Vektor Serangan dan Strategi Mitigasi

Abstrak

Sektor perbankan Indonesia menghadapi ancaman serangan siber yang semakin canggih, khususnya ransomware. Riset ini menyusun analisis deskriptif terhadap data insiden siber sepanjang tahun 2026. Metode yang digunakan adalah studi literatur dan analisis data sekunder dari laporan BSSN, OJK, serta lembaga keamanan global. Hasil kajian menunjukkan bahwa ransomware varian hybrid fileless dengan teknik double extortion menjadi ancaman utama. Adopsi AI oleh aktor ancaman mempercepat dan memperluas skala serangan. Diperlukan implementasi zero trust architecture, backup offline, dan peningkatan kapasitas SDM keamanan siber untuk mengurangi risiko.

1. Latar Belakang

Perkembangan digitalisasi perbankan di Indonesia membawa risiko keamanan siber yang signifikan. Sepanjang 2026, BSSN mencatat peningkatan serangan ransomware yang menyasar sektor keuangan. Serangan ini tidak hanya merugikan secara finansial, tetapi juga merusak reputasi dan kepercayaan nasabah. Laporan global menunjukkan bahwa sektor Finance & Insurance menjadi salah satu target utama dengan teknik double extortion yang semakin masif.

2. Rumusan Masalah

1. Apa saja vektor serangan ransomware yang dominan pada sektor perbankan Indonesia pada 2026?
2. Bagaimana dampak finansial dan operasional dari serangan tersebut?
3. Apa strategi mitigasi yang paling efektif untuk diterapkan?

3. Tujuan

1. Mengidentifikasi vektor serangan ransomware yang dominan.
2. Menganalisis dampak finansial dan operasional.
3. Merumuskan strategi mitigasi yang aplikatif.

4. Batasan Masalah

Objek kajian adalah laporan insiden siber pada sektor perbankan Indonesia sepanjang 2026. Data bersumber dari laporan BSSN, OJK, dan publikasi media massa. Penelitian

tidak melakukan pengujian langsung terhadap sistem perbankan.

5. Tinjauan Pustaka

Kajian merujuk pada laporan BSSN tentang tren serangan siber 2026, laporan OJK tentang ketahanan siber perbankan, serta publikasi dari Help Net Security yang merangkum Black Kite 2026 Ransomware Report. Panduan teknis dari CareersInfoSecurity juga menjadi rujukan dalam merumuskan strategi mitigasi.

6. Metodologi

Penelitian menggunakan pendekatan kualitatif-deskriptif dengan metode studi dokumentasi. Data dianalisis secara tematik untuk mengidentifikasi pola serangan dan efektivitas mitigasi.

7. Teknik Analisis

Analisis deskriptif-komparatif terhadap data insiden dan literatur terkait.

8. Hasil

1. Ransomware varian hybrid fileless dengan teknik double extortion menjadi ancaman dominan.
2. Adopsi AI oleh aktor ancaman mempercepat dan memperluas skala serangan.
3. Kerugian finansial mencapai miliaran rupiah.
4. Zero trust architecture, backup offline, dan MFA menjadi mitigasi paling efektif.

9. Pembahasan

Serangan ransomware terhadap perbankan Indonesia menunjukkan tren yang mengkhawatirkan. Varian hybrid fileless yang mampu mematikan backup dan menggunakan double extortion menjadi ancaman utama. Diperlukan pendekatan keamanan yang berlapis dan proaktif, bukan hanya reaktif. Kolaborasi lintas lembaga dan adopsi kerangka kerja keamanan global menjadi kunci.

10. Kesimpulan

Ransomware merupakan ancaman serius bagi sektor perbankan Indonesia. Diperlukan implementasi zero trust architecture, backup offline, dan peningkatan kapasitas SDM untuk mengurangi risiko.

11. Rekomendasi

1. Implementasi zero trust architecture secara menyeluruh.
2. Backup data secara offline dan terisolasi (air-gapped).
3. Penerapan Multi-Factor Authentication (MFA) di semua akun.
4. Pelatihan rutin bagi karyawan tentang kesadaran keamanan.
5. Kerja sama lintas lembaga untuk berbagi informasi ancaman.

12. Keterbatasan Riset

Penelitian hanya menggunakan data sekunder. Tidak semua insiden dilaporkan ke publik.

Daftar Pustaka

Infobanknews. (2026). Ransomware dan Phishing Masih Hantui Perbankan, AI Bikin Serangan Makin Masif.
Help Net Security. (2026). Ransomware in 2026: More groups, more victims, no slowdown.
CareersInfoSecurity. (2025). Stopping Ransomware: Tools, Tactics and Frameworks.

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-2026-088

Kode Verifikasi: DCY-RISET-2026-088

DOI: 10.5281/zenodo.24048626

Lisensi: CC BY 4.0

Diterbitkan oleh Data Cyber Indonesia

Tanggal: 08 November 2026