KATA PENGANTAR

Puji syukur kehadirat Tuhan Yang Maha Esa atas segala rahmat-Nya sehingga makalah ini dapat tersusun hingga selesai. Makalah ini disusun untuk memenuhi tugas mata kuliah Etika Profesi dan Hukum TIK. Penulis berharap makalah ini dapat menambah pengetahuan dan pengalaman bagi para pembaca terkait pentingnya keamanan data di era digital.

Jember, 29 November 2025

Penulis

DAFTAR ISI



Di era revolusi industri 4.0, data telah menjadi aset baru yang lebih berharga daripada minyak. Pemerintah Indonesia melalui inisiatif Sistem Pemerintahan Berbasis Elektronik (SPBE) berupaya mengintegrasikan data nasional melalui Pusat Data Nasional (PDN). Namun, tantangan keamanan siber menjadi ancaman nyata. Insiden serangan Ransomware pada PDN Sementara di bulan Juni 2024 menjadi bukti kerentanan infrastruktur digital negara. Kasus ini tidak hanya melumpuhkan layanan publik tetapi juga memicu perdebatan mengenai tata kelola dan kedaulatan data negara.



Berdasarkan latar belakang di atas, maka rumusan masalah dalam makalah ini adalah: Bagaimana kronologi dan penyebab teknis terjadinya serangan pada PDN Sementara? Bagaimana dampak serangan tersebut ditinjau dari aspek kerugian publik dan keamanan negara? Bagaimana tinjauan kasus ini berdasarkan UU ITE dan UU Perlindungan Data Pribadi?



Tujuan dari penulisan makalah ini adalah untuk menganalisis kegagalan sistem keamanan pada insiden PDN serta memberikan rekomendasi perbaikan tata kelola siber di Indonesia.



Insiden bermula ketika layanan keimigrasian di berbagai bandara internasional mengalami gangguan total. Berdasarkan investigasi forensik digital, ditemukan bahwa gangguan disebabkan oleh serangan siber berjenis Ransomware varian Brain Cipher, sebuah pengembangan dari LockBit 3.0. Penyerang berhasil mengenkripsi data pada server virtual dan meminta tebusan sebesar 8 juta Dolar Amerika Serikat. Pemerintah menolak membayar tebusan, namun mengakui kesulitan dalam melakukan pemulihan (recovery) karena mayoritas data tidak memiliki cadangan (backup) yang terpisah.

Secara teknis dan manajerial, terdapat beberapa faktor fatal yang menyebabkan insiden ini. Pertama, lemahnya implementasi Defense in Depth. Fitur keamanan dasar seperti Windows Defender ditemukan dalam kondisi non-aktif pada server yang terinfeksi. Kedua, ketiadaan Disaster Recovery Plan (DRP) yang memadai. Fakta bahwa backup data bersifat opsional bagi instansi pengguna menunjukkan ketidakpahaman pengelola terhadap prinsip redundansi data. Seharusnya, backup menerapkan prinsip 3-2-1 (3 salinan, 2 media, 1 offsite).

2.3 Tinjauan Etika dan Hukum

Dalam perspektif UU No. 27 Tahun 2022 tentang Pelindungan Data Pribadi (PDP), kegagalan pengendali data (dalam hal ini instansi terkait) untuk melindungi data pribadi masyarakat merupakan bentuk pelanggaran administratif yang serius. Pasal 39 UU PDP mewajibkan pengendali data untuk mencegah akses data pribadi secara tidak sah. Selain itu, dari sisi etika profesi IT, kelalaian administrator dalam membiarkan celah keamanan terbuka melanggar prinsip profesionalisme dan kehati-hatian (due diligence).

BAB 3 PENUTUP

3.1 Kesimpulan

Serangan Ransomware pada PDN Sementara merupakan "wake-up call" bagi keamanan siber Indonesia. Insiden ini disebabkan oleh kombinasi kelalaian manusia, lemahnya prosedur backup, dan kurangnya proteksi pada endpoint. Dampaknya sangat luas, mulai dari terganggunya layanan publik hingga menurunnya kepercayaan internasional.

3.2 Saran

Pemerintah perlu segera mewajibkan standar keamanan ISO 27001 bagi seluruh infrastruktur kritis negara. Backup data harus menjadi kewajiban mutlak, bukan opsi. Selain itu, audit keamanan berkala harus dilakukan oleh pihak independen untuk memastikan integritas sistem tetap terjaga.

DAFTAR PUSTAKA