ABSTRAK

ANALISIS STRATEGI KEAMANAN SIBER INDONESIA DALAM MENGHADAPI ANCAMAN RANSOMWARE: STUDI KASUS SEKTOR LAYANAN PUBLIK DAN PERBANKAN, 2020—2024

Oleh

ELNAYA PRICILIA

Keamanan siber merupakan salah satu sektor penting bagi Indonesia. Namun, seiring perubahan lanskap ancaman global, Indonesia kini mengembangkan segmen mitigasi yang lebih spesifik, seperti *financial-sector cybersecurity* dan *public-service cloud security* guna menegakkan kedaulatan digital nasional secara menyeluruh.

Penelitian ini menganalisis strategi keamanan siber Indonesia terhadap eskalasi ancaman ransomware transnasional periode 2020–2024 dengan studi kasus serangan LockBit 3.0 pada Bank Syariah Indonesia (2023) dan Brain Cipher pada Pusat Data Nasional Sementara 2 (2024). Menggunakan pendekatan kualitatif deskriptif, penelitian ini mengevaluasi upaya keamanan Indonesia melalui lensa Teori Strategi Keamanan Siber Nasional dan Konsep Tata Kelola Keamanan Siber Nasional. Data sekunder bersumber dari laporan resmi BSSN dan dokumen kebijakan dianalisis menggunakan teknik kondensasi, penyajian, dan triangulasi sumber.

Hasil penelitian menunjukkan bahwa implementasi 5 Pilar ITU di Indonesia masih menemui kendala pada aspek teknis dan organisasi, terutama terkait *compliance gap* instansi pemerintah serta fragmentasi otoritas antarlembaga yang menghambat respons cepat terhadap serangan siber. Akibatnya, aktor eksternal masih dapat mengeksploitasi celah keamanan pada sektor publik dan perbankan karena belum terwujudnya integrasi yang utuh di kelima pilar tersebut. Penelitian menyimpulkan bahwa penguatan kedaulatan digital memerlukan sinkronisasi komando kelembagaan yang tersentralisasi, ketegasan sanksi hukum atas kelalaian risiko, serta kedisiplinan operasional yang ketat guna mewujudkan ekosistem data publik yang resiliens.

Kata kunci: Keamanan Siber, *Ransomware*, 5 Pilar ITU, BSI, PDNS 2.

ABSTRACT

ANALYSIS OF INDONESIA'S CYBER SECURITY STRATEGY AGAINST RANSOMWARE ATTACKS: A CASE STUDY OF THE PUBLIC SERVICE AND BANKING SECTORS, 2020—2024

By

ELNAYA PRICILIA

Cybersecurity is one of the crucial sectors for Indonesia. However, along with the shifting global threat landscape, Indonesia is now developing more specific mitigation segments, such as financial-sector cybersecurity and public-service cloud security, in order to enforce national digital sovereignty comprehensively.

This research analyzes Indonesia's cybersecurity strategy against the escalation of transnational ransomware threats during the 2020–2024 period, focusing on the case studies of the LockBit 3.0 attack on Bank Syariah Indonesia (2023) and the Brain Cipher attack on the Temporary National Data Center 2 (2024). Utilizing a descriptive qualitative approach, this study evaluates Indonesia's cybersecurity efforts through the lens of National Cybersecurity Strategy Theory and National Cybersecurity Governance Concepts. Secondary data derived from official BSSN reports and policy documents were analyzed using data condensation, data display, and source triangulation techniques.

The results indicate that the implementation of the 5 ITU Pillars in Indonesia still encounters obstacles in technical and organizational aspects, particularly regarding the compliance gap within government agencies and the fragmentation of authority among institutions, which hinders rapid responses to cyberattacks. Consequently, external actors are still able to exploit security vulnerabilities in the public and banking sectors due to the absence of full integration across these five pillars. The study concludes that strengthening digital sovereignty requires centralized institutional command synchronization, strict legal sanctions for risk negligence, and rigorous operational discipline to realize a resilient public data ecosystem.

Keywords: *Cybersecurity*, *Ransomware*, ITU 5 Pillars, BSI, PDNS 2.