UNIVERSITAS PERTAHANAN REPUBLIK INDONESIA

ANALISIS DAMPAK SERANGAN *RANSOMWARE* PADA INFRASTRUKTUR INFORMASI VITAL

(STUDI KASUS SERANGAN *LOCKBIT* 3.0 PADA PUSAT DATA NASIONAL SEMENTARA)

DEVI TIANA OCTAVIANI SUPRIYADI
120230405001

Tesis yang Ditulis untuk Memenuhi Sebagian Persyaratan
dalam Mendapatkan Gelar Magister Terapan Pertahanan

FAKULTAS SAINS DAN TEKNOLOGI PERTAHANAN
PROGRAM STUDI REKAYASA PERTAHANAN SIBER

BOGOR
2025

LEMBAR PERSETUJUAN TESIS

Nama	:	Devi Tiana Octaviani Supriyadi
NIM	:	120230405001
Program Studi	:	Rekayasa Pertahanan Siber
Fakultas	:	Sains dan Teknologi Pertahanan
Judul Tesis	:	Analisis Dampak Serangan *Ransomware* pada Infrastruktur Informasi Vital (Studi Kasus Serangan *Lockbit* 3.0 pada Pusat Data Nasional Sementara)

Pembimbing I,	Pembimbing II,
Dr. Bisyron Wahyudi, S.Si., M.T	Dr. Ir. H. A. Danang R, S.Si., M.T., M.Tr.Opsla., CEH., CSBA., IPM., ASEAN Eng.
Tanggal: 7 Februari 2025	Kolonel Laut (E)/NRP.10829/P Tanggal: 7 Februari 2025

Mengetahui,
Dekan Fakultas Sains dan Teknologi Pertahanan

Prof. Dr. Ir. Muhamad Asvial, M.Eng.
Pembina Utama Muda (IV/c)
Tanggal: 10 Februari 2025

LEMBAR PENGESAHAN TESIS

Nama	:	Devi Tiana Octaviani Supriyadi
NIM	:	120230405001
Program Studi	:	Rekayasa Pertahanan Siber
Fakultas	:	Sains dan Teknologi Pertahanan
Judul Tesis	:	Analisis Dampak Serangan *Ransomware* pada Infrastruktur Informasi Vital (Studi Kasus Serangan *Lockbit* 3.0 pada Pusat Data Nasional Sementara)

No.	Nama	Tanda Tangan	Tanggal
1.	Pembimbing I: Dr. Bisyron Wahyudi, S.Si., M.T		7/2/25
2.	Pembimbing II: Dr. Ir. H. A. Danang R, S.Si., M.T., M.Tr.Opsla., CEH., CSBA., IPM., ASEAN Eng. Kolonel Laut (E)/NRP.10829/P		7/2/25
3.	Penguji I: Dr. Ir. H. Achmad Farid Wadjdi, M.M		7/2/25
4.	Penguji II: Prof. Ir. J.W. Saputro, M.Sc., MBA., Ph.D		7/2/25
5.	Penguji III: Dr. Sunarta, S.T., M.T Kolonel Laut (E)/NRP.12898/P		10/2/25

PERNYATAAN ORISINALITAS

Dengan ini saya menyatakan bahwa dalam tesis ini tidak terdapat karya atau bagian karya yang pernah diajukan untuk memperoleh gelar kesarjanaan jenjang apapun di suatu Perguruan Tinggi; dan sepanjang sepengetahuan saya juga tidak terdapat istilah, frasa, kalimat, paragraf, subbab atau bab dari karya yang pernah ditulis atau diterbitkan; kecuali yang secara tertulis diajukan dalam naskah ini dan disebutkan dalam Daftar Referensi.

Apabila dikemudian hari terbukti bahwa terdapat plagiat dalam tesis ini, saya bersedia menerima sanksi sesuai ketentuan peraturan/undang-undang yang berlaku.

Bogor, Januari 2025

Devi Tiana Octaviani Supriyadi

KATA PENGANTAR

Segala puji dan syukur penulis panjatkan ke hadirat Allah *Subhanahu wa Ta'ala* atas limpahan rahmat dan karunia-Nya sehingga penulisan tesis yang berjudul: "Analisis Dampak *Ransomware* pada Infrastruktur Informasi Vital (Studi Kasus Serangan *Lockbit* 3.0 pada Pusat Data Nasional Sementara)" dapat diselesaikan dengan baik.

Penyusunan tesis ini ditujukan sebagai salah satu syarat dalam memperoleh gelar Magister Terapan Pertahanan pada Program Studi Rekayasa Pertahanan Siber, Fakultas Sains dan Teknologi Pertahanan, Universitas Pertahanan Republik Indonesia.

Penyusunan tesis ini dapat diselesaikan berkat bantuan dan dukungan dari berbagai pihak, baik secara langsung maupun tidak langsung. Untuk itu, pada kesempatan ini peneliti mengucapkan terima kasih kepada:

1. Dr. Bisyron Wahyudi, S.Si., M.T. selaku pembimbing I dan Kolonel Laut (E) Dr. Ir. H. A. Danang Rimbawa, S.Si., M.T., M.Tr.Opsla., CEH., CSBA., IPM., ASEAN Eng. selaku Kaprodi dan pembimbing II atas bimbingan, arahan, serta dukungan yang telah diberikan sehingga tesis ini dapat terselesaikan dengan baik.
2. Dr. Ir. H. Achmad Farid Wadjdi, M.M, Prof. Ir. J. W. Saputro, M.Sc., MBA., Ph.D, Kolonel Laut (KH) Dr. Hondor Saragih, S.T., M.Si.(Han)., M.M.S.I, Kolonel Laut (E) Dr. Sunarta, S.T., M.T, selaku penguji I, II, dan III yang telah memberikan saran dan masukan berharga dalam upaya penyempurnaan tesis ini.
3. Semua dosen, staf, dan rekan-rekan Mahasiswa Cohort 2 Rekayasa Pertahanan Siber, serta seluruh civitas akademika Universitas Pertahanan atas dukungan dan bantuan yang telah diberikan selama masa studi.
4. Orang Tua kami tercinta Bapak Yuddi Supriyadi, Ibu M.L. Dian Purwandari, atas doa dan dukungannya selama ini.

5. Adik tercinta dan tersayang, Dania Ayu JS dan Dhimas Kurnia PS serta keluarga lain yang senantiasa memberikan doa dan semangat untuk mendukung penulis dalam menyelesaikan tesis ini dengan baik.
6. Sugi Wiranto selaku *support systems* selalu memberikan semangat serta motivasi kepada penulis sehingga dapat menyelesaikan tesis ini dengan baik.
7. Para Narasumber yang telah berkenan meluangkan waktu dan memberikan informasi yang sangat berharga dalam penyusunan tesis ini.
8. Seluruh pihak yang tidak bisa disebutkan satu per satu yang telah membantu dan memberikan dukungan dalam bentuk apapun, baik secara langsung maupun tidak langsung, dalam penyelesaian tesis ini.

Semoga Tuhan Yang Maha Esa membalas kebaikan-kebaikan berbagai pihak atas bantuannya.

Penulis menyadari bahwa tesis ini masih jauh dari sempurna. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun demi perbaikan di masa mendatang.

Akhir kata, semoga tesis ini dapat memberikan kontribusi positif dalam pengembangan ilmu pertahanan dan bermanfaat bagi para pemangku kepentingan dalam meningkatkan keamanan serta pertahanan negara di bidang siber.

Bogor, Februari 2025

Devi Tiana Octaviani Supriyadi

ABSTRAK

ANALISIS DAMPAK SERANGAN *RANSOMWARE* PADA INFRASTRUKTUR INFORMASI VITAL (STUDI KASUS SERANGAN *LOCKBIT* 3.0 PADA PUSAT DATA NASIONAL SEMENTARA)

DEVI TIANA OCTAVIANI SUPRIYADI

Penelitian ini menganalisis dampak serangan ransomware LockBit 3.0 pada Pusat Data Nasional Sementara (PDNS) dan Infrastruktur Informasi Vital (IIV) di Indonesia. Tujuan penelitian ini adalah mengidentifikasi kerentanan sistem, mengevaluasi dampak operasional, finansial, dan keamanan data, serta menilai efektivitas strategi mitigasi yang diterapkan. Pendekatan penelitian menggunakan metode kualitatif deskriptif dengan studi kasus, melibatkan wawancara, kuesioner dengan 10 responden, serta analisis dokumentasi. Sebanyak 8 dari 10 responden menyatakan bahwa kerugian akibat serangan ransomware tidak dapat dihitung secara pasti karena melibatkan kerugian operasional, finansial, serta dampak jangka panjang terhadap reputasi. Hasil penelitian menunjukkan bahwa serangan ransomware menyebabkan gangguan besar pada layanan publik, kerugian finansial yang signifikan, dan penurunan kepercayaan masyarakat terhadap layanan PDNS. Kelemahan utama ditemukan pada sistem deteksi dini, SOP yang kurang terstruktur, serta kesiapan staf yang rendah dalam menghadapi serangan. Kesimpulan penelitian menekankan perlunya pembaruan SOP, penguatan teknologi deteksi, dan pelatihan berkala untuk meningkatkan kesiapan. Saran diberikan untuk penelitian lebih lanjut, termasuk eksplorasi penggunaan kecerdasan buatan (AI) dalam deteksi ransomware, analisis dampak jangka panjang, serta perbandingan strategi mitigasi antara sektor publik dan swasta.
Kata kunci: *ransomware, LockBit 3.0, Pusat Data Nasional Sementara, Infrastruktur Informasi Vital, Strategi Mitigasi.*

ABSTRACT

ANALYSIS OF THE IMPACT OF *RANSOMWARE* ATTACKS ON VITAL INFORMATION INFRASTRUCTURE (CASE STUDY OF *LOCKBIT* 3.0 ATTACK ON TEMPORARY NATIONAL DATA CENTER)

DEVI TIANA OCTAVIANI SUPRIYADI

This research analyzes the impact of the LockBit 3.0 ransomware attack on the Temporary National Data Center (PDNS) and the Infrastructure for Vital Information (IIV) in Indonesia. The objectives of this research were to identify system vulnerabilities, evaluate operational, financial and data security impacts, and assess the effectiveness of the mitigation strategies implemented. The research approach used a descriptive qualitative method with a case study, involving interviews, questionnaires with 10 respondents, and documentation analysis. A total of 8 out of 10 respondents stated that losses due to ransomware attacks cannot be calculated precisely because it involves operational and financial losses, as well as long-term impacts on reputation. The results showed that the ransomware attack caused major disruption to public services, significant financial losses, and decreased public trust in PDNS services. Major weaknesses were found in the early detection system, poorly structured SOPs, and low staff preparedness for the attack. The research conclusions emphasized the need for SOP updates, strengthening of detection technologies, and periodic training to improve preparedness. Suggestions are provided for further research, including exploration of the use of artificial intelligence (AI) in ransomware detection, long-term impact analysis, and comparison of mitigation strategies between the public and private sectors.

Keywords: *ransomware*, LockBit 3.0, Temporary National Data Center, Vital Information Infrastructure, Mitigation Strategy.

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL