PENERAPAN METODE TOPSIS DALAM PENENTUAN PRIORITAS KERENTANAN KEAMANAN PADA DATA KASPERSKY PT PLN NUSA DAYA

Dzahwa Fadillia, 202231030

Di bawah bimbingan Dr. Ir. Luqman, S.T., M.Kom., IPM., ASEAN, Eng.

ABSTRAK

Penanganan kerentanan keamanan pada perangkat komputer memerlukan mekanisme prioritisasi yang tepat agar risiko operasional dapat diminimalkan secara efektif. Penelitian ini bertujuan untuk merancang model prioritisasi kerentanan menggunakan metode *Technique for Order Preference by Similarity to Ideal Solution* (TOPSIS) dengan mempertimbangkan empat kriteria, yaitu *Severity Score, Update Availability, Age in Days, dan Device Count*. Data penelitian berupa 821 kerentanan yang diperoleh dari *Kaspersky Security Center* PT PLN Nusa Daya, kemudian diolah melalui tahapan TOPSIS untuk menghasilkan nilai preferensi (Ci) sebagai dasar pemeringkatan risiko. Hasil penelitian menunjukkan bahwa kerentanan dengan nilai Ci tinggi termasuk dalam kategori *High Risk* dan memerlukan penanganan segera, sedangkan kerentanan dengan nilai Ci rendah diklasifikasikan sebagai *Low Risk*. Validasi hasil perhitungan melalui perbandingan antara perhitungan program dan perhitungan manual menunjukkan tingkat konsistensi yang tinggi. Dengan demikian, model prioritisasi yang diusulkan dapat digunakan sebagai dasar pengambilan keputusan dalam menentukan prioritas penanganan kerentanan keamanan di lingkungan perusahaan.

Kata kunci: Kerentanan, TOPSIS, Prioritas Risiko, Keamanan Siber.

APPLICATION OF THE TOPSIS METHOD FOR DETERMINING SECURITY VULNERABILITY PRIORITIES BASED ON KASPERSKY DATA AT PT PLN NUSA DAYA

Dzahwa Fadillia, 202231030

Under the Guidance Dr. Ir. Luqman, S.T., M.Kom., IPM., ASEAN, Eng.

ABSTRACT

The management of security vulnerabilities in computer systems requires an effective prioritization mechanism to minimize operational risks. This study aims to develop a vulnerability prioritization model using the Technique for Order Preference by Similarity to Ideal Solution (TOPSIS) method by considering four criteria: Severity Score, Update Availability, Age in Days, and Device Count. The dataset consists of 821 vulnerability records obtained from Kaspersky Security Center at PT PLN Nusa Daya, which were processed through the TOPSIS procedure to generate preference values (Ci) as the basis for risk ranking. The results indicate that vulnerabilities with higher Ci values are classified as High Risk and require immediate mitigation, while those with lower Ci values fall into the Low Risk category. Validation through a comparison between system-based and manual calculations demonstrates consistent results. Therefore, the proposed model can serve as a decision-support tool for determining vulnerability remediation priorities within the organization.

Keywords: Vulnerability, TOPSIS, Risk Prioritization, Cybersecurity.