

ABSTRAK

Perkembangan teknologi informasi mendorong pemanfaatan website dan infrastruktur jaringan sebagai media pengelolaan informasi akademik dan administrasi di SMK Ma'arif NU 1 Ajibarang. Meskipun memberikan kemudahan dalam pengelolaan data, penerapan sistem tersebut berpotensi menimbulkan risiko keamanan yang dapat memengaruhi aspek *Confidentiality*, *Integrity*, dan *Availability* (CIA). Penelitian ini bertujuan untuk menganalisis risiko keamanan website dan infrastruktur jaringan serta menentukan prioritas penanganan risiko menggunakan metode *Failure Mode and Effects Analysis* (FMEA) dan *Analytic Hierarchy Process* (AHP). Pengumpulan data dilakukan melalui observasi, wawancara, studi literatur, dokumentasi, monitoring jaringan menggunakan Wireshark, serta pengujian keamanan menggunakan Nmap. Metode FMEA digunakan untuk mengidentifikasi potensi kegagalan (*failure mode*) dan menghitung nilai *Risk Priority Number* (RPN) berdasarkan parameter *Severity*, *Occurrence*, dan *Detection*, sedangkan metode AHP digunakan untuk menentukan bobot kriteria dan prioritas risiko melalui *pairwise comparison*. Hasil penelitian menunjukkan bahwa risiko dengan prioritas tertinggi terdapat pada Port dan Database Server dengan nilai RPN sebesar 324 dan skor AHP sebesar 7,899, diikuti oleh Manajemen Domain dengan skor AHP 6,273 serta Jaringan Wi-Fi dengan skor AHP 6,154. Hasil pembobotan AHP menunjukkan bahwa kriteria *Severity* memiliki bobot tertinggi sebesar 63,33%, diikuti *Occurrence* sebesar 26,05%, dan *Detection* sebesar 10,62%. Dengan demikian, integrasi metode FMEA dan AHP mampu menghasilkan prioritas risiko yang lebih objektif serta mendukung penyusunan rekomendasi mitigasi untuk meningkatkan keamanan website dan infrastruktur jaringan di SMK Ma'arif NU 1 Ajibarang.

Kata kunci: Analisis Risiko, Keamanan Website, Infrastruktur Jaringan, FMEA, AHP.

ABSTRACT

Advancements in information technology have driven the use of websites and network infrastructure to manage academic and administrative information at SMK Ma'arif NU 1 Ajibarang. While these systems facilitate data management, their implementation introduces potential security risks affecting Confidentiality, Integrity, and Availability (CIA). This study aims to analyze security risks associated with the website and network infrastructure and to prioritize risk management using the Failure Mode and Effects Analysis (FMEA) and Analytic Hierarchy Process (AHP) methods. Data collection involved observation, interviews, literature reviews, documentation, network monitoring via Wireshark, and security testing using Nmap. FMEA was employed to identify potential failure modes and calculate Risk Priority Numbers (RPN) based on Severity, Occurrence, and Detection parameters, while AHP was used to determine criterion weights and risk priorities through pairwise comparison. The results indicate that the highest-priority risk involves the Port and Database Server, with an RPN of 324 and an AHP score of 7.899, followed by Domain Management (AHP score: 6.273) and the Wi-Fi network (AHP score: 6.154). AHP weighting results show that Severity holds the highest weight at 63.33%, followed by Occurrence at 26.05% and Detection at 10.62%. Consequently, integrating FMEA and AHP enables a more objective determination of risk priorities and supports the formulation of mitigation recommendations to enhance the security of the website and network infrastructure at SMK Ma'arif NU 1 Ajibarang.

Keywords: Risk Analysis, Website Security, Network Infrastructure, FMEA, AHP.