ABSTRACT

Cybersecurity risks in web-based applications are mostly triggered by technical vulnerabilities and the threat of cyber attacks. Therefore, the application of cybersecurity risk management in applications must consider up to the technical level risk. Previous studies related to the implementation of security risk management in applications still have gaps, including not specifically addressing technical level of risks. In addition, the risk assessment stage has also not accommodate the actual vulnerabilities contained in the application which is one of the factors forming security risks. Blitar Regency Government currently has more than 100 active applications that are potentially affected by these risks. The two risk management frameworks or guidelines that currently exist do not accommodate the needs of implementing technical-level cybersecurity risk management in applications.

This research aims to develop a cybersecurity risk management framework that accommodates technical level security risks to be implemented in web-based applications. The combination of ISO 27005 and NIST SP 800-30 Rev.1 is used as a reference that complements each other in developing the framework. The risk model, analysis approach and assessment are determined by considering the existing limitations. In terms of formulating risk mitigation recommendations, this framework uses the main reference from the Technical Standard for Web-Based Application Security from BSSN. To ensure that the framework can be implemented, testing was conducted by applying it to one active application owned by Blitar Regency Government. Validation by cybersecurity experts was also carried out to obtain an assessment and input on the framework.

Based on the test results, the framework is generally easy for users to follow and implement. Vulnerability-based technical risks have been successfully identified, assessed for their level of risk, and formulated recommendations for handling them with systematic guidance. The risk identification process is carried out by using a vulnerability assessment approach in order to identify actual vulnerabilities in the application. The results of validation conducted by cybersecurity experts show that the framework developed has met the principles of risk management and can be a solution for users in government agencies who still have limitations in conducting penetration testing to identify vulnerabilities.

Keywords: *risk management, cybersecurity, frameworks, ISO 27005, NIST SP 800-30 Rev.1*

INTISARI

Risiko keamanan siber pada aplikasi berbasis web banyak dipicu oleh kerentanan teknis dan ancaman serangan siber. Oleh sebab itu, penerapan manajemen risiko keamanan siber pada aplikasi harus mempertimbangkan sampai pada risiko tingkat teknis. Beberapa penelitian sebelumnya terkait penerapan manajemen risiko keamanan pada aplikasi masih memiliki kesenjangan diantaranya belum membahas lebih spesifik risiko tingkat teknis. Selain itu, pada tahap penilaian risiko juga belum dapat mengakomodir kerentanan aktual yang terdapat pada aplikasi yang merupakan salah satu faktor pembentuk risiko keamanan. Pemkab Blitar saat ini memiliki lebih dari 100 aplikasi aktif yang berpotensi terdampak risiko tersebut. Dua kerangka kerja atau pedoman manajemen risiko yang saat ini ada, belum mengakomodir kebutuhan penerapan manajemen risiko keamanan siber tingkat teknis pada aplikasi.

Penelitian ini bertujuan untuk mengembangkan kerangka kerja manajemen risiko keamanan siber yang mengakomodir risiko keamanan tingkat teknis untuk dapat diimplementasikan pada aplikasi berbasis web. Pemaduan antara ISO 27005 dan NIST SP 800-30 Rev.1 digunakan sebagai referensi yang saling melengkapi dalam menyusun kerangka kerja. Model risiko, pendekatan analisis dan penilaian ditentukan dengan mempertimbangkan keterbatasan yang ada. Dalam hal merumuskan rekomendasi mitigasi risiko, kerangka kerja ini menggunakan acuan utama dari Standar Teknis Keamanan Aplikasi Berbasis Web dari BSSN. Untuk memastikan bahwa kerangka kerja tersebut dapat diimplementasikan maka dilakukan pengujian dengan cara menerapkannya pada satu aplikasi aktif milik Pemkab Blitar. Validasi oleh pakar keamanan siber juga dilakukan untuk mendapatkan penilaian dan masukan terhadap kerangka kerja yang dibuat.

Berdasarkan hasil pengujian, secara umum kerangka kerja ini mudah untuk diikuti dan diimplementasikan oleh pengguna. Risiko-risiko teknis berbasis kerentanan telah berhasil diidentifikasi, dinilai tingkat risikonya, dan dirumuskan rekomendasi penanganannya dengan panduan yang sistematis. Proses identifikasi risiko dilakukan dengan menggunakan pendekatan *vulnerability assessment* sehingga dapat mengidentifikasi kerentanan aktual pada aplikasi. Hasil validasi yang dilakukan oleh pakar keamanan siber menunjukkan bahwa kerangka kerja yang dikembangkan telah memenuhi kaidah manajemen risiko dan dapat menjadi solusi bagi pengguna di instansi pemerintahan yang masih memiliki keterbatasan dalam melakukan *penetration testing* untuk mengidentifikasi kerentanan.

Kata kunci: *manajemen risiko, keamanan siber, kerangka kerja, ISO 27005, NIST SP 800-30 Rev.1*