Perancangan Kerangka Kerja Keamanan Siber pada Smart Airport Berdasarkan Integrasi ENISA Securing Smart Airport, NIST Cyber Security Framework dan ISO/IEC 27002:2022 (Studi Kasus Bandara Internasional XYZ) = Designing Cybersecurity Framework at Smart Airport Based on the Integration of ENISA Securing Smart Airport, NIST Cybersecurity Framework and ISO/IEC 27002:2022 (Case Study at XYZ International Airport)

Irma Nurfitri Handayani, author

Abstrak

Penelitian ini bertujuan untuk merancang kerangka kerja keamanan siber pada smart airport untuk meningkatkan keamanan siber dan mencegah serangan siber pada smart airport. Smart airport menimbulkan risiko baru akan adanya serangan siber, pengelolaan smart airport dengan menggunakan teknologi IT dan IoT harus dikelola dengan baik yaitu melalui tata kelola teknologi informasi yang sesuai dengan kerangka kerja yang sudah terimplementasi dengan baik dan berstandar Internasional. Selain kerangka kerja tata kelola teknologi informasi, perlu diperhatikan lebih dalam lagi mengenai keamanan siber dan perlindungan data pribadi agar smart airport memiliki tingkat keamanan yang tinggi untuk menjaga keberlangsungan bisnisnya. Untuk mewujudkan smart airport yang aman dengan mempertimbangkan risiko serangan siber perlunya dibuat kerangka kerja keamanan siber sebagai evaluasi untuk pengelola smart airport. Penelitian ini mengintegrasikan kerangka kerja Enisa Securing Smart Airport, NIST Cyber Security Framework dan ISO/IEC 27002:2022. Dari hasil penelitian diperoleh aktivitas yang berasal dari NIST CSF adalah 39%, aktivitas yang berasal dari ENISA Securing Smart Airport adalah 6%, dan aktivitas yang berasal dari ISO/IEC 27002:2022 adalah 17%. Diharapkan kerangka kerja smart airport ini dapat melindungi keamanan siber dengan menggunakan NIST CSF, melindungi keamanan informasi dengan menggunakan ISO 27002:20022 dan mengikuti standar keamanan airport berdasarkan ENISA Securing Smart Airport. Hasil dari penelitian ini adalah kerangka kerja keamanan siber untuk smart airport, yang diujicobakan di Bandara Internasional XYZ dengan hasil nilai kematangan 3,9 berada pada level implementasi terdefinisi.
.....This research aims to design a cyber security framework at smart. Airport to improve cyber security and prevent cyber attacks at smart airports. Airports are transforming into smart airports as airport user services continue to increase, creating an efficient, effective and comfortable travel experience for travelers. Smart airports pose new risks of cyber attacks, management of smart airports using IT and IoT technology must be managed well, namely through information technology governance that is in accordance with a framework that has been well implemented and has international standards. Apart from the information technology governance framework, futher attention needs to be paid to cyber security and personal data protection so that smart airports have a high. Level of security to maintain business continuity. To create a safe smart airport by considering the risk of cyber attacks, it is necessary to have a cyber security framework as an evaluation for smart airport managers. This research integrates the Enisa Securing Smart Airport Framework, NIST Cybersecurity Framework and ISO/IEC 27002:2022. From the research result, the activity originating from NIST CSF was 39%, from ENISA Securing Airport was 6% and from ISO/IEC 27002:2022 was 17%. The goal is a smart airport framework that can protect cyber security by using NIST

CSF, protect information security by using ISO/IEC 27002:2022 and based on airport security standards by using ENISA Securing Smart Airport. The result of this research is a cybersecurity framework for smart airports, which was tested at XYZ Internasional Airport with a maturity value of 3,9 at the defined implementation level.