ABSTRACT

The use of technology to improve operations processes and service delivery has drastically changed the business environment, bringing with it new threats, cybersecurity threats. This study presents a threat modeling architecture for cybersecurity for a digital merchant point of sale (POS) platform developed by an Indonesian government bank. Such critical systems require adequate security against data leakage, financial loss and system outages as the platform enables critical financial services.

The research is done by looking first at the possible security threats and vulnerabilities present in the Digital Merchant POS Platform and its components by application of two of the most popular threat modeling frameworks STRIDE and MITRE ATT&CK. STRIDE is an acronym for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service & Elevate Privilege and is a threat taxonomy developed by Microsoft. MITRE ATT&CK, on the other hand, is a behavior-based matrix of adversary tactics and techniques used during real-world attacks. This paper attempts to fill this research gap by combining these two methodologies and providing a comprehensive understanding of the context and other relevant aspects of the proposed cybersecurity measures with this study.

This study applies the Design Science Research Methodology (DSRM) with particular attention to the problem definition, development and solution and evaluation. Two types of data sources were used, primary and secondary. Interviews and necessary observations with the representatives of the bank have revealed weaknesses in the security of the current system. Also, scholarly articles, reputable practices, and other sources from the bank were used.

The digital Merchant pos platform's current architecture has serious security flaws according to the report's review. Lack of multi-channel authentication for users increases the risk of the system being compromised in the event that a user has their login details stolen. Financial data confidentiality is also compromised because data storage devices are not encrypted during transmission and while

idle to avert unauthorized access to data. Exploitable weaknesses in the API gateway were also uncovered, these included token spoofing and DoS attacks.

In order to enhance security of the MIPS system, the multi zone model involving the DMZ, Trusted Zone, Restricted zone and the Public Zone has been recommended. This design ensures that the MIPS system is secure as each zone has been outfitted with its own security measure. For instance, the Public Zone that deals with users outside the organization utilizes WAF and secure session protocol to eliminate hacking and forgery attack whereas the Restrict Zone that comprises sensitive information uses strong encryption and control access protocols to ensure that risk of breach is eliminated.

The evaluation phase of the study involved utilizing STRIDE and MITRE ATT&CK frameworks. The combined use of both the empirical methodologies led to mitigation planning as attack vectors were linked to their corresponding counter measures.The pattern that was evident was a tapering of the system's vulnerability as robust defense mechanisms were deployed.Also utilization of automated threat systems and comprehensive logging monitors in the designed system ensures that the system is always on guard and prepared for incidents.

This research adds value to the discipline of cybersecurity by illustrating shrewd use of threat modeling frameworks in the process of designing secure system architectures. The proposed design not only improves the security of the Digital Merchant POS Platform but also provides a model that other companies in the finance industry can follow in order to go through comparable cyber security situations. Also in this study, the role of being proactive in planning cybersecurity measures and the process of managing such measures are evaluated and strategies appropriate.

For such segments as financial institutions, IT professionals and cybersecurity practitioners, this research proffers valuable recommendations. The use of security policies will help save valuable assets, preserve faith among customers and meet formal requirements. Efforts and resources invested into integration of STRIDE and MITRE ATT&CK frameworks guarantees a well-rounded approach