ENTERPRISE CYBERSECURITY RISK ASSESSMENT WITH THREAT MODELING: CASE STUDY XYZ INSURANCE COMPANY

By

BINTANG RAMDHANI
2-1851-011

MASTER'S DEGREE
in

MASTER OF INFORMATION TECHNOLOGY
ENGINEERING AND INFORMATION TECHNOLOGY FACULTY

SWISS GERMAN UNIVERSITY
The Prominence Tower
Jalan Jalur Sutera Barat No. 15, Alam Sutera
Tangerang, Banten 15143 - Indonesia

August 2021

Revision after Thesis Defense on 30 July 2021

STATEMENT BY THE AUTHOR

I hereby declare that this submission is my work and to the best of my knowledge, it contains no material previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any other degree or diploma at any educational institution, except where due acknowledgement is made in the thesis.

Bintang Ramdhani

Student Date

Approved by:

Dr. Ir. Mohammad Achmad Amin Soetomo. M.Sc.

Thesis Advisor Date

Dr. Charles Lim B.Sc. M.Sc.

Thesis Co-Advisor Date

Dr. Maulahikmah Galinium, S.Kom, M.Sc.

Dean Date

ABSTRACT

ENTERPRISE CYBERSECURITY RISK ASSESSMENT WITH THREAT MODELING: CASE STUDY XYZ INSURANCE COMPANY

By

Bintang Ramdhani
Dr. Ir. Mohammad Achmad Amin Soetomo. M.Sc.
Dr. Charles Lim B.Sc. M.Sc.

SWISS GERMAN UNIVERSITY

XYZ Insurance is a company that always try to meet the needs of its customers, one of the customer's needs during this pandemic is health services, therefore, XYZ insurance develops a telemedicine application. In order to ensure the reliable operation of the application, it is necessary to pay attention to the security issues for the application. To overcome security problems. In this research, a risk assessment is carried out using threat modeling with STRIDE, where Data Flow Diagrams (DFD) is the main input, its help identifies and differentiate existing threats, researcher found 40 threats on telemedicine application, where these threats are in process as many as 28 threats, data flow as many as 8 threats, and data store as 4 threats.

Meanwhile, to measure the identified threat, researcher used DREAD to get threat score and CVSS to get vulnerability score. From the results of that threats and vulnerabilities, a risk value is obtained, where in this telemedicine application there are 2 very high risks, there are on the webserver process - SQL Injection and Directory traversal. By knowing the risks that exist, the appropriate controls to mitigate these risks are recommended.

Keywords: Threat Modeling, Risk Assessment, DFD, STRIDE, DREAD, CVSS.

DEDICATION

I dedicate this works for the future of the country I loved: Indonesia

and

my beloved family

ACKNOWLEDGEMENTS

I wish to thank Dr. Ir. Moh. A. Amin Soetomo, M.Sc, as my Thesis Advisor for his time and advice, and suggestions, and Dr. Charles Lim, BSc., MSc., CTIA, CHFI, EDRP, ECSA, ECSP, ECIH, CEH, CEI my Thesis Co-Advisor or his time, advice, guidance, insights, and ideas.

I also thank to MIT Batch-23 fellow students in Swiss German University MIT that were tirelessly available for discussion, sharing thoughts, experiences, and even spent time together.

Finally, I would like to thank my beloved wife and son for their support, patience and understanding during my master's education.

Table of Contents

LIST OF FIGURES

Figures Page

LIST OF TABLES

Table Page