Informatics Institute of Technology
In collaboration with
University of Westminster, UK

Multi-Layered Defense in Depth Framework to Defend and Respond Against Advanced Persistent Threat Attacks Targeting the Sri Lankan Financial Sector

A dissertation by
Jehan M De Zilva

Supervised by
Mr. Austen Mascranghe

Submitted in partial fulfilment of the requirements for the
Master of Science degree in Cyber Security and Forensics
Department of Computing

July 2021

Abstract

Businesses face a constantly evolving threat landscape. One of the most significant challenges is presented by advanced persistent threats (APTs), which are sophisticated, multi-faceted attacks targeting a particular organization. Mitigating the risk of APTs requires advances beyond traditional layered security to include real-time threat management. The threat landscape continues to become more challenging. The motivation and means for carrying out attacks on information systems are changing. Determined, committed attackers are employing multiple means to breach security controls. Businesses need to respond in kind with various security controls, including real-time monitoring and rapid containment measures. It is essential to understand that APTs are not a new means of conducting an attack and are not something that can be blocked or disrupted once and the problem goes away. APTs are better understood to be more like a cyber-attack campaign than a single type of threat. These types of attacks cannot be stopped by using a single defensive measure. The traditional tools in use have failed to stop these advanced attacks as they rely on signatures in their databases. Instead, a defense in depth approach needs to be used which used multiple layers of defenses to safeguard against such attacks. The global frameworks available do not consider the local context in terms of a country and therefore some organizations will find it difficult to fully implement such frameworks as they are not customized to fit their business models. This study aims to put forward a new framework which will take into account the Sri Lankan Banks' readiness and awareness levels and propose a new and effective framework which is customized according to the local business operating processes.

Keywords: Advanced Persistent Threat, Cyber Threats, Cyber Framework