Informatics Institute of Technology

In collaboration with

University of Westminster, UK.

Framework for Vulnerability and Patch Management Process in a Corporate Infrastructure

A Dissertation By

Dayan Kalanajith Gajanayake

Supervised by

Mr. Sithira Hewaarachchi

Submitted in partial fulfillment of the requirements for the

MSc Cyber Security and Forensics

Department of Computing

August 2022

Abstract

A vulnerability in cyber security refers to any defect in an organization's information system, system operations, or internal controls. These weaknesses are attractive targets for lurking cybercriminals and can be exploited through the points of vulnerability. These hackers are capable of gaining unauthorized access to networks and causing significant harm to data privacy. As a result, cybersecurity vulnerabilities are critical to monitor for overall security posture, as holes in a network can result in a full-scale penetration of an organization's systems.

Vulnerability management is the process of discovering, identifying, classifying, remediating, and mitigating vulnerabilities found in software or hardware, whereas patch management is the process of identifying, testing, deploying, and verifying patches for devices' operating systems and applications. Vulnerability and patch management processes are often confused, although they are two distinct, but required, phases for good cyber hygiene, endpoint hardening, and attack surface reduction. Organizations may take a proactive approach to vulnerability repair and mitigation by implementing best practices in vulnerability and patch management. Patching vulnerabilities is an essential step in endpoint security and a major component of cyber hygiene best practices.

As the digital world advances, many businesses discover that the "old way" of doing things is too time-consuming and adds to significant delays in their vulnerability and patch management operations. Modern cyber hygiene solutions are multifaceted in their approach to system security and can assist bridge the gap between these two critical functions.

However, People and organizations have become more exposed to outside attacks as a result of their usage of the internet. Indeed, cyber concerns primarily impact information systems through various sorts of hostile assaults such as malware, viruses, social engineering, etc. This work is motivated by the need for a more intuitive and automated network-level framework for the vulnerability and patch management process in corporate infrastructure.

Keywords

Vulnerability Management, Patch Management, Corporate Infrastructure