Coordinated Vulnerability Disclosure Process Key Dimensions Set

Mārtiņš Vecstaudžs, Kaspars Osis

Vidzeme University of Applied Sciences, Valmiera, Latvia

Introduction

Since the enforcement of Directive (EU) 2022/2555 mandating the implementation of Coordinated Vulnerability Disclosure (CVD) processes, each EU Member State has adopted its own national approach. While some countries still rely on email-based systems to receive and process CVD reports, Latvia has taken a significant step forward by developing a dedicated digital platform for CVD management. However, a common issue across all implementations is the lack of a structured approach to the development of CVD programs when viewed through multiple dimensions. As a result, the failure to examine and address various dimensions, such as legal, technical, organizational, societal aspects and others limit the overall effectiveness and maturity of the CVD process.

Materials and Methods

This study examines the revised and enhanced stages in the life cycle of a CVD report and compares them against various relevant and influencing dimensions, such as legal, technical, organizational, societal aspects and others, based on expert input.

Results

The outcome of this study is the development of a theoretical six-dimensions tool outlining the key dimensions that influence the life cycle of a CVD report, which should be taken into account by those implementing and developing CVD programs. This tool can be applied to improve various workflows within the life cycle of a CVD report and beyond. Furthermore, the insights from the six-dimensions model will be used to enhance the Latvian CVD platform.

Discussion

Given that there is currently no formal obligation for European Union Member States to optimize CVD process workflows, despite their complexity and the diverse approaches taken, the proposed model provides significant added value by introducing six dimensions aimed at improving CVD process efficiency. It can serve as a strategic tool for enhancing national cybersecurity capabilities by leveraging CVD data for future phases, such as predicting and mitigating emerging vulnerabilities before they evolve into in actual security incidents. Nevertheless, the model has certain limitations, as its dimensions are derived mainly from theoretical considerations and expert input, and therefore require validation through empirical studies and practical application, which will form part of the author's broader research work.

Keywords

CVD, vulnerability reporting, cybersecurity, CVD process key dimensions