Abstract

In recent years, our society has become more dependent on the Internet and ICT in almost every domain (finance, health, education, etc.) making it a major driver of economy growth. However, with the wide adoption of ICT and the Internet, new threats have emerged in the cyberspace called cybercrimes which figure among the key risks factors of companies and governments.

However, due to the complexity of the components of those risks, it is very difficult for top management to get an effective assessment of the risk induced by IT. This in turn jeopardizes the allocation of budget to IT and cybersecurity as well as the prioritization of their related initiatives.

In this light, a system for the automation of risk assessment and monitoring is then highly needed.
In an effort to provide governments and private companies especially those of developing countries with an affordable solution for real time monitoring of the risk level incurred by their information system and to get a nationwide insight of cyber risks, an architecture of a system aimed at automating the collection and centralization of cyber-risk factors nationwide is proposed in this paper.

The novelty of this architecture is that it doesn’t only capture the risks related to individual asset vulnerabilities as other frameworks such as CVSS but in addition proposes an XML schema that captures the risks related to asset vulnerabilities and their attack surface as well as the risks related to attack scenario requiring the combination of breaches of several assets.

This article is structured as follows: section 1 introduces the article, section 2 presents some concepts and works related to the topic covered by the article, section 3 states the problem, section 4 specifies the articles contribution to research, section 5 presents the solution and section 6 presents a case study.

References


Index Terms

Computer Science      Security
Keywords

Risk, vulnerability, attack surface.