IMPROVING DISTRIBUTED VULNERABILITY ASSESSMENT MODEL OF CYBERSECURITY

Kálmán Hadarics[1] and Ferenc Leitold[2]

DOI: 10.24989/ocg.v331.32

Abstract
In the digital age more and more services and data are available over the Internet. Companies and public organizations becoming increasingly vulnerable related to hacks and cyberattacks. In order to provide successful online services, effective security initiatives and targeted protections are necessary to mitigate security risks. Effective cybersecurity more than deploying firewalls and other security software (e.g. antivirus, intrusion detection/prevention systems.). Through risk assessment and risk management practices we can identify critical parts of information systems and can transform them into security tactics. Furthermore in the Distributed Vulnerability Assessment (DVA) model three factors are identified: (1) characteristics and prevalence of cyber-threats, (2) vulnerabilities of IT infrastructure and its components and processes, (3) vulnerabilities deriving from users' behavior.

In this paper, we examine and improve our mathematical model of Distributed Vulnerability Assessment. This model can be extended for using additional information and considerations. This paper also presents a practical method which can be applied to eGovernment infrastructure and services also to reduce the impact of malware attacks of the information system.

Keywords: *distributed vulnerability analysis, malware, threat, cybersecurity*

1. Introduction

The recent evolution of information technology caused significant increase in productivity and everyday life. These days using online services is self-evident. Our personal and other specific data are accessible from different devices like computers, tablets, smartphones and other IoT devices. However if our data are available online they are exposed to theft or unwanted manipulation. There are different cyber-threats. With the help of that cyber criminals can steal unauthorized data or other credential information. In the digital age the information security became a crucial point of an information system. If you want to launch a new digital service you have to ensure data security. An unwanted security incident can disrupt our business success, and partners will abandon our service.

If we want to observe the protection level of our IT system and infrastructure we have to consider our data flows and processes. But all systems, networks, applications or other infrastructure element may contain vulnerabilities or just misconfiguration. Newer and newer threats are appearing everyday therefore continuous review of security rules are expected. In order to achieve digital enterprise success, effective security initiatives and targeted protections are necessary to reduce or mitigate security risks.

[1] University of Dunaújváros, H-2400 Dunaújváros, Táncsics M. u. 1/A., hadarics@uniduna.hu
[2] Secudit Ltd., H-8200 Veszprém, Kupa utca 16., fleitold@secudit.com