International Journal of Engineering Research and Development
e-ISSN: 2278-067X, **p**-ISSN: 2278-800X, www.ijerd.com
Volume 6, Issue 12 (May 2013), PP. 60-63

Analysis of Automation Studies in the Field of Information Security Management

Punit Dwivedi[1], S. Christobel Diana[2]
[1,2]Dept. of Information Technology, SRM University, Chennai, India

Abstract: - Now a days, information security is critical issue, for any organization, to take care of. There are several standardization researches that provide a framework to organization for information security management. ISO 27001 is of the standards, which provides a stable framework for information security management. Information security management, as defined in ISO 27001, deals with establishing, implementing, operating, reviewing, monitoring, maintaining and improving an information security management system. This paper gives an overview about automation possibilities in information security management. The study is focused on the possibility of applying (i) hard- and software systems for automatic operation of certain security controls, and (ii) the Security Control Automation Protocol (SCAP) for automation of compliance and security configuration checking. The results of the study can be a great help for organizations and their information security managers. They can use these results for identifying systems they can use to achieve greater efficiency in information security management process.

Keywords:- Automation, ISO 27001, Security Controls, Information Security Management, Security Content Automation Protocol.

I. INTRODUCTION

Information security managers are responsible for managing information systems' security. The information security management is an expensive and challenging task for ISMs. Many different and complex software components - including firmware, operating systems, and applications - must be configured securely, patched when needed, and continuously monitored for security. Most organizations have an extensive set of security requirements. For commercial firms, such requirements are established through complex interactions of business goals, governmental regulations, and insurance requirements; for government organizations, security requirements are mandated [1].

Chasing these requirements is human-error prone and time consuming, because organizations depends upon the ISMs for these tasks and the have lack of automated ways of performing security management tasks. This paper provides a study of automation possibilities in processes and controls related to information security. In section II, overview of information security management is provided, as defined in ISO 27001. In section III, analysis of security controls, that can be automated using existing hard- and software tools, is provided. Section IV analyses the Security Control Automation Protocol (SCAP) and its possibilities to automate vulnerability checking and security measurement.

II. INFORMATION SECURITY MANAGEMENT

The ISO 27001 defines the process of information security management. ISO 27001 provides a model for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System (ISMS) [2]. It follows the "Plan-Do-Check-Act" (PDCA) process model, which is applied to structure all ISMS processes. The actions to be carried out in each phase are:

a) Plan: Establish ISMS policy, objectives, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.

b) Do: Implement and operate the ISMS policy, controls, processes and procedures.

c) Check: Assess and measure process performance against ISMS policy, objectives and practical experience and report the results to management for review.

d) Act: Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

In following sections discussion will go through automation possibilities of security control operations and compliance and security configuration checking.

III. AUTOMATION OPERATION OF SECURITY CONTROL

In ISO 27001, there are 133 security controls specified, and these security controls have to be implemented and operated in order to mitigate the risk. These security controls are mostly related to human resource issues and some of them are related to technologies.

In [3] an analysis has been provided of how many of these controls can be automated by existing security application that support automation in the operations of security controls. In following subsections, the automatable controls and the hard- and software tools that support the automation are briefly described.

A. Automatable Controls

A security control can be automated if the operation of the control can be done without the intervention of human in the process. In some cases, controls can be partially automated. The identification of controls that can be automated is based on following criteria [3]:

- The operation and monitoring of the control requires only machine-readable and - process able resources.
- The control can be partially or completely implemented by at least one security application mentioned in the following sub section.

Based on these criteria, table I shows how many criteria can be automated for each domain. The analysis results show that only 30% of the security controls can be automated.

Table I: ISO 27001 Automatable Controls

Domain	Information security controls	
	Automatable controls	***Total Controls***
Security Policy	0	2
Organization of information security	0	11
Asset Management	1	5
Human resources security	1	9
Physical and environmental security	2	13
Communication and operations management	15	32
Access control	13	25
Information systems acquisition, development and maintenance	4	16
Information security incident management	0	5
Business continuity management	0	5
Compliance	1	10

B. Soft- and hardware tools

In order to identify automatable controls, several enterprise level security soft- hardware solutions were reviewed, especially those that allow to automate the operations of controls in a centralized way. The following soft- and hardware has been studied with regard to their potential of automating security controls [3]:

1) *Microsoft:* Systems Management Server (SMS) and Active Directory (AD)
2) *Symantec*: Protection Suite Enterprise Edition (ED), Net Backup and Veritas Cluster Server (VCS).
3) *Alien Vault*: Open Source Security Information Management (OSSIM).
4) *nCircle*: IP360 and Configuration Compliance Manager (CCM)
5) *Honeywell:* NOTIFIER fire alarm systems.

It is important to clarify that the list of security applications mentioned in this paper is not exhaustive. The analysis was performed only to identify automatable controls. Paper [3] provides a complete analysis of which controls can be automated by which software.

IV. SECURITY CONTENT AUTOMATION PROTOCOL

The most recent work related to information security automation has focused on standardizing the format and nomenclature by which security software products communicate information about software

identification, software flaws and security configurations. These efforts resulted in the definition of the Security Content Automation Protocol (SCAP). SCAP has been specified by the National Institute of Standards and Technology (US) in NIST SP800-126 [4].

SCAP can be used in the checking phase of the information security management process in order to provide an automated way of (i) performing continuous monitoring of system security configuration settings, (ii) examining systems for signs of compromise, and (iii) having situational awareness; i.e. being able to determine the security posture of systems and the organization at any given time.

SCAP has two major elements. First, it is a protocol: a suite of open specifications that standardize the format and nomenclature by which software communicates information about software flaws and security configurations. Each specification is also known as an *SCAP component*. Second, SCAP includes software flaw and security configuration standardized reference data, also known as *SCAP content*. SCAP has several fields of application, including (i) automated checks for known vulnerabilities, (ii) automating the verification of security configuration settings, and (iii) generating reports that link low-level settings to high-level requirements [5].

The current components of the SCAP protocol are:

- Common Platform Enumeration (CPE): nomenclature and dictionary of product names and versions.
- Common Configuration Enumeration (CCE): Nomenclature and dictionary of system configuration issues.
- Common Vulnerabilities and Exposures (CVE): Nomenclature and dictionary of security-related software flaws.
- Common Vulnerability Scoring System (CVSS): Specification for measuring the relative severity of software flaw vulnerabilities.
- Extensible Configuration Checklist Description Format (XCCDF): Language for specifying checklists and reporting checklist results.

A) Practical use of SCAP

Organizations should use security configuration checklists that are expressed using SCAP to improve and monitor their systems' security, and to demonstrate compliance with high level security requirements that originate from mandates, standards, and guidelines.

SCAP content is available from multiple sources. For example, the National Vulnerability Database (US) [6] hosts a dictionary of CPE entries and information on CVE entries, while the MITRE Corporation hosts an OVAL database and maintains a list of CCE entries [7]. The National Checklist Program (US) web site [8] and the Centre for Internet Security (CIS) [9] are repositories for SCAP-expressed checklists. There you can find best-practice security configurations accepted for several operating systems and applications.

Organizations should also acquire and use SCAP-validated products. This protocol is gradually being adopted by security applications. At the moment of writing this paper 30 security software development companies offer SCAP validated products. A complete list of these systems can be found in [10].

V. CONCLUSIONS

Information security management is a complex and therefore time-consuming and expensive task. Organizations face changing threat landscapes and have to address them on multiple levels. Some efforts in research and industry already concentrate on increasing the automation of some aspects in information security. To structure and consolidate these efforts we checked which phases of the ISO 27001 process model (Plan-Do-Check-Act) can be automated.

In this paper, existing methods for increasing automation possibilities in plan, do, check phases are shown. (i) Existing security applications can be used to automate about 30% of the 133 ISO 27001 controls in the Do phase, (ii) SCAP suite and its significant industry support can be used to support Check phase automation. This mapping of existing automation efforts with the different ISMS phases as defined in ISO 27001 gives an exact idea of automation possibilities in information security management and serves as a reference for security managers in order to increase the effectiveness of their ISMS. The analysis has shown that several isolated automation approaches exist. However, only by integrating these approaches organizations will be able to maximize their utility. In further research we will propose an automation framework for information security management, by studying the integration of existing approaches in this field.

REFERENCES

[1]. S. Radack and R. Kuhn, "Managing Security: The Security Content Automation Protocol," *IT Professional*, 2011, p. 9-11.

[2]. "ISO/IEC 27001: Information technology - Security techniques Information security management systems – Requirements," 2005.

[3]. R. Montesino and S. Fenz, "Information security automation: how far can we go?," *Sixth International Conference on Availability, Reliability and Security (ARES)*, Vienna, Austria: 2011.
[4]. S. Quinn, K. Scarfone, M. Barrett, and C. Johnson, "NIST SP 800-117: Guide to Adopting and Using the Security Content Automation Protocol (SCAP)," Jul. 2010.
[5]. National Vulnerability Database (NVD)" Available: http://nvd.nist.gov/.
[6]. OVAL - Open Vulnerability and Assessment Language" Available: http://oval.mitre.org/.
[7]. National Checklist Program Repository" Available: http://web.nvd.nist.gov/view/ncp/repository.
[8]. Center for Internet Security (CIS)" Available: http://cisecurity.org.
[9]. Security Content Automation Protocol Validated Products" Available: http://nvd.nist.gov/scapproducts.cfm.