Applying NSTISSC Security Model on Using Web Content Management Systems

Ahmed Hussein
Arabic Academy for Financial and Banking Sciences / Jordan

Abstract

The goal of this paper is to introduce a method for how to guarantee secure usage for the WCMS, by ensuring main security characteristics such as confidentiality, integrity and availability for the usage of WCMS via applying customized NSTISSC security model.

Keywords: Web Content Management System (WCMS), Security, NSTISSC model, Security Characteristics and Security Solutions.

Introduction

Website is the mirror that reflects the shape of any business or organization. That’s why the website is important and this importance became clearer when the website is considered the primary method for the business to post information to customer, supplier and/or internal staff (Winett 2001, ChameleonNet 2003, Patel, 2004).

But regarding to the rapid changes that recurrently took place in the business environment; the website content must be modified and updated to comply with these changes and these modifications must be performed in a secure manner. These processes are performed using special type applications known as Web Content Management Systems (WCMS) (Proctor et.al. 2003, Thomas et.al. 2003, Winett 2001, ChameleonNet 2003, Patel 2004).

The processes of maintain and manage organizational websites by different authorized and responsible persons to add or modify the web content in secure and organized manner is Web Content Management (WCM) (Claero Systems 2002, Winett 2001, Patel 2004).

There are two main types of websites, static and dynamic, static websites is the type of websites where text, graphics, multimedia and information are resides in a file, rather than database, so changes can be made on the website only by changing the contents of that file, such as HTML pages. On the other hand, dynamic websites stores some of its text, graphic, multimedia and information in a database, so for example each time user accesses the website, a different picture or even a different view of it is displayed (Winett 2001).
Nowadays managing web content to increase its effectiveness can be considered as a competitive advantage, because of the wide spread of e-commerce and internet technologies, adding to that marketing based techniques. Organizations can perform the modifications and update to its websites to improve these sites content, to be simple, up-to-date and at the same time reflects the real picture of the company products or services, specially when these contents are distributed and want to be integrated together (Villamor-Lugo et.al. 2004, Proctor et.al. 2003, Winett 2001).

These contents must be acceptable by the person who navigates that web site, to attract him and avoiding him going after other competitor's websites (Winett 2001, Claero Systems 2002, Patel 2004).

WCMS started to take place and be a backbone system in the organizational infrastructure. Many vendors are only founded to provide customers with this type of solutions, which are in general web based application, which allows external and remote users access ability to modify and update websites contents (Winett 2001, Claero Systems 2002, ChameleonNet 2003, Patel 2004).

Many organizational roles can be involved in the process of web content management, starting from operational level up to top management level, including middle, executive personnel and technical (Winett 2001, Claero Systems 2002, ChameleonNet 2003, Patel 2004).

But all that must be performed in secure manner that guarantee the three pillars of security which are confidentiality or privacy, integrity and availability. These security pillars are mentioned in the document number 4011 for the National Security Telecommunications and Information Systems Security (NSTISS), this document presents a standard model for information security (NSTISS 1994, Whitman et.al. 2003).

Information states that the NSTISSC model includes are transmission, storage and processing, and security measures or security solutions this model proposes are technology, policy and SETA (Security Education, Training and Awareness), adding to that the previously mentioned security characteristics confidentiality, integrity and availability. (NSTISS 1994, Whitman et.al. 2003)

The problem in this field is how to guarantee a secure WCMS by securing its main characteristics and way of use.

The security assignment process sophistication will be reduced once the organization knows and understands its environment and how it attends to use this system.

The next parts of the paper present the literature reviews, followed by detailed description of the basic characteristics for using WCMS, then there relations to the security factors and components based on the NSTISS model, and finally conclusion and set of references parts.
Literature Reviews

Winett in his white paper, Effective web content management: empowering the business user while IT maintains control, presented in details what is a web content management system role in any operational level in any organization, and the revenue expected from a web content management system for suppliers, customers and organizational staff by presenting each party and benefits that they can gain from using such systems proved by three real success stories from real life.

Claero Systems in its white paper about its own WCMS described in general the content management and its importance for small and mid-size organizations by making it easy to change the web content so less time, effort and money spent on updating website contents and at the same time stay online with the customers which are the main benefits, that each organization looking for.

Another WCMS vendor ChameleonNet described in details the characteristics of the WCMS and how it affects on improving the organizational income by reducing the costs of outsourcing the process of designing and updating websites, where this process can be done in-house in a professional manner regardless the technical expertise available in such field of technology (web design).

Thomas et.al., in there paper Simple Web Content Management Tool as the Solution to a Web Site Redesign, presented a real life situation for redesigning the Buffalo University web site by creating a tool that enhance web content management, defining their needs in the tool to be developed depending on the requirements.

NSTISS in its document No. 4011 that represents a standard model for security called the NSTISSC model represents the relation between the three parties of proposed security pillars (Confidentiality, Integrity, Availability), security solutions (Policy, Technology, SETA) and information states (Storage, Processing, Transmission) and how to assign the pillars for any information state and by which solution.

Patel in his paper Driving Revenue with Web Content Management, described the content lifecycle, and how in each phase of this lifecycle the organization can improve security of the contents in each level, by describing the main phases on WCM process and sub-phases in each.
Characteristics of Using WCMS

In this section I will present the main characteristics of using WCMS that are predictable in any WCMS system and they are:

1- Affordability: which means that many users can use this system regardless to there technical background, like marketing and financials managers (Winett 2001, Thomas et.al. 2003).

2- Organized usage: which means here to allow each authorized user to access predefined parts of website not all of it depending on his position and responsibilities. This facility prevents the un-consistency of data and information that can occur when more than one person changes the data in the same part of the website (Winett 2001, Claero Systems 2002, ChameleonNet 2003, Patel 2004, Thomas et.al. 2003).

3- Authoring Websites: flexible editing and creating websites is an urgent need and the overall need is to perform these actions anywhere any time (Winett 2001, Claero Systems 2002, ChameleonNet 2003, Patel 2004, Thomas et.al. 2003).

4- Systems Integration: here I discuss the ability to integrate the WCMS with other organizational systems, for example the EDI (Electronic Data Interchange) systems to improve organizational productivity with external stakeholders like suppliers, mediators and partners. Another good example is to integrate the WCMS with web services to get instantly changes in news, stock markets prices and weather (ChameleonNet 2003, Thomas et.al. 2003).

Characteristics of NSTISSC Model

Figure 1 presents the NSTISSC model
(Figure 1) NSTISSC model  (NSTISS 1994, Whitman et.al. 2003).
"This model responds to the need for a theoretical foundation for modeling the information systems security sciences" (NSTISS 1994).

"The model has several significant applications. Initially, the two-dimensional matrix is used to identify information states and system vulnerabilities. Then, the three layers of security measures can be employed to minimize these vulnerabilities based on knowledge of the threat to the information asset" (NSTISS 1994).

In this model we can determine for example how to guarantee the availability for information in storage state by technology, or confidentiality of information in transmission by applying a policy. These are examples for how to guarantee each security pillar by which measure or solution to each data state.

The Proposed Model

In the new proposed WCMS security model I suggest removing the proposed information states and substitute them with the characteristics of using WCMS, to produce the following model:

(Figure 2) Proposed model
By using this model we can guarantee the WCMS usage security by assigning which is the best solution or measure to be used to guarantee which security characteristics to which WCMS characteristics. For example we can guarantee organized usage confidentiality throw policy and technology, or we can guarantee affordability availability throw SETA.

This proposed model doesn't only provide a model for information system security solutions, but also considered as an evaluation tool for the current organizational WCMS security status that could affect positively in the process of risk management and improving the security environment for WCMS usage.

Another advantage for this model that its can be applied on any other information system, by understanding the right characteristics for using it, and substituting the WCMS proposed characteristics with those for the new system, its become easy to create a secure environment for using it.

Conclusion

Any organization uses websites and looking forward updating it, must think about implementing or purchasing a WCSM regardless the website type or how it was developed (which programming language used?) but again all companies seeks for security, so such system must be secure enough or organization must provides the security outline for using this or any information systems.

The better understanding for the needs of WCMS and business environment embowers the right selection of the security structure for using the WCMS, which also empowers and improves all levels in the organization to change the web content in professional and secure manner so all stakeholders can gain benefits.

So in this paper I introduced an enhanced security model for WCMS by creating a three dimensions structure consists of security characteristics (confidentiality, integrity and privacy), security solutions and measures (policy, technology and SETA) and WCMS characteristics (affordability, organized usage, authoring websites and systems integration) and how we can assign the right solution to guarantee the security characteristics for the WCMS characteristics to ensure a secure usage for that system.
References