International Journal of Computer & Information Technologies (IJOCIT)
www.ijocit.ir & www.ijocit.org
ISSN = 2345-3877

An Approach for Services' Integration and Divergence on Computer Networks Security

Mohammad Reza Khajehaghverdi[1] and Nasser Modiri[2]
Msc, Department of Electrical[1], Associate Professor in Department of Electrical[2]
Computer & IT, Zanjan Branch, Islamic Azad University[1,2]
Zanjan, Iran[1,2]
haghverby@yahoo.com[1]

Abstract: - nowadays, networks have undeniable importance. The use of networks in business, providing the electronic services to the clients and the emergence of new technologies has led to the creation of a variety of services in networks. Due to various threats that exist in the networks, security has become a challenge for them. In this article, at first, the information security management system is introduced. Then different views on the implementation of information security are raised. Finally, based on the variety of services in networks and information security standards, a framework and evaluation method for implementing security in computer networks is represented.

Keywords: Access Control, Information Flow, Block View, Service View, Equipment View, Security Standards Framework, Information Security Management, Hierarchical Infrastructure.

1. Introduction

Due to the growing development of computer networks geographically and variety of services in networks, the biggest challenge in security implementation projects is the continuity of information security in networks of organizations that requires some solutions and processes in order to be preserved and protected.

For implementing information security in computer networks several approaches have been presented and for this purpose different check lists and actions have been made out in organizations but regarding breadth and diversity of network services, none of them have presented a suitable solution for the continuity of information security. So in order to implement security in computer networks in organizations and also the continuity of this security based on the breadth of networks and diversity and divergence of existing services, an approach and a systematic method with the following features is necessary:

- have the ability to assess
- reduce maintenance costs

- be integrated
- have the implementation cycle

So for security implementation in computer networks and its continuity some solutions must be presented. They must be systematic and based on the information security management system and its standards and have the above mentioned features.

2. Information security management system

Information security management system includes some controllers applied by organizations to ensure that risks are properly controlled. Information security management is introduced by ISO standards and helps the organizations to define the best methods in the field of information security for their businesses.

The important information security management standards published by ISO are: ISO 27001 that introduces information security management systems requirements and ISO 27002 that represents regulations for the implementation of information security management.

ISO 27002 standard: in mid-2007 ISO 17799 standard was renamed ISO 27002 standard and joined to the family of ISO 27000 series standards. The purpose of information security management system standards codification is to represent a model based on which we can establish, implement, operate, monitor, review, and improve an information security management system. ISO 27002 standards include 11 security conditions, 39 control objectives, and 133 controlled methods. Following table indicates the family of information security management system standards.

Table 1: The family of isms group

An overview and glossary of terms	ISO 27000
The requirements of information security management system	ISO 27001
Regulation for information security management system	ISO 27002
A guidance in the implementation of an information security management system	ISO 27003
Information security management measurement and metrics	ISO 27004
Guidelines for information security risk management	ISO 27005

2.1. Deming cycle

The implementation of security management systems based on continuous planning cycle that keeps the plan up to date, increases the chance of success. For this purpose the organizations use the Deming Cycle. This cycle components and their general concepts are as following:
Plan: at this stage what is going to be improved is analyzed and improvable areas are reviewed.
Do: change or test can be carried. It is related to the changes that have been decided in the plan stage.
Check: after implementing changes in a short period of time, the impact of changes should be evaluated.
Act: saving the changes and restarting the cycle from the beginning

3. Review of existing security models

3.1. Equipment View

In equipment view, network includes a series of levels that are implemented based on their application, scalability, and cost. It has island structure and is used in each level of technologies and security mechanisms according to three kinds of information security controls (physical, logical, management) for establishing security and defense strategies and can be implemented at different depths (defense in depth). In this view, for codification of strategies and security policies in different levels, organizational structures, processes, and the security services are not used. Moreover it doesn't have a hierarchical infrastructure so management controls are in the background and creating a secure network is possible by defining security zones. Each piece of equipment in each area has different necessities. So each area is protected according to the security needs of the installed equipment on it.

3.1.1. Implementation Results

In terms of equipment, however the security implementation in organizations computer networks is easier, faster, and cheaper; it has some disadvantages which are mentioned bellow:[7]

- In this viewpoint, as long as the network is small, the security mechanisms are sufficient.
- In equipment view, security policies are limited.
- Security policies are not flexible and extendable
- For formulating strategies and network security policies in different levels, regulations and organizational structures are not used.
- In this view, there is little relationship between the concept of network security and business
- In this view, terms such as policies, standards, tactics, guidelines, best practices and processes necessary for implementing network security, are not considered.
- Management is possible only at hardware level and network process management is not practical in this perspective.

3.2. Hierarchical View

In designing the network of a large or international organization, in order to achieve a sustainable business and technical objectives in this area, we definitely need a network with various and interrelated components. This is only possible if we can design a network in different layers divide and develop its activities and performances within these layers. Network design experts have suggested a Hierarchical network design model in order to develop a typology of discrete layers. In this model, each layer can focus on specific tasks and activities. So based on each layers characteristics we can choose suitable equipment and systems.

Hierarchical structure has three general parts which include:[8]

- Core layer: this layer is the backbone layer of network running with high speed that transfer and communicate layers. The duty of this layer is switching the traffic and routing to the high speed packages.
- Distribution layer: this layer is the isolation point between core layer and the network's access layer in next level and consists of switches and routers that implement policies on network.
- Access layer: this layer consists of switches and wireless equipment with lower power than the two previous layers and is considered as the final connection

station to the local network users can access to the network services via this layer's switches. Some of the applet security policies are applied in this layer.

3.2.1. Implementation Results

Implementation of security policies in enterprise wide networks based on a hierarchical approach has some advantages and disadvantages which are mentioned below:

Advantages:

- Implementing security policies in wide networks based on a hierarchical approach is both flexible and scalable.
- Security policies are varied.
- Modification and updates are easy and inexpensive
- Security policies are separable
- In this viewpoint, the security policies can be implemented in large and international networks
- One of the defining features of hierarchical networks is its efficiency in processing and no failure in communications

Disadvantages:

- For formulating strategies and security policies in different layers organizational structures are not used.
- In this viewpoint, there is little relationship between the concept of security and business.
- Estimation and evaluation of security is only possible in equipment level of different layers of network.
- In this perspective, designing and implementing security policies are complex and expensive.

3.3. Service View

Based on this view, information security policies are divided into four groups. These policies are defined as four security services presented in the following:

Computer security policies services: includes all items that are defined in relation to computer.

Network security policies services: issues are related to the creation of communication and network platform

Information security policies services: related to the existing information in the network

Access control security policies services: they are discussed in relation to all licenses.

In this view in order to implement security in enterprise networks based on information security management system (organizational structure, manpower, processes, data flow, and so on), first of all, a series of preparatory activities must be done to create sustainable business in the organization. Thus maintaining the order of all these steps and the way they are planned is very important. These steps are strategies, short term and long term goals, polices codification, standards, tactics tips, and best practices. After these steps three other steps need to be taken a higher level so that the organization can implement security based on information security management system in network from the viewpoint of service.

First step: the most important thing is to draw a business process modeling for each unit of organization.

Second step: the number of functional areas must be defined in each process.

Third step: in this step, the details of the communication data are important and data flow in each unit is drawn.

After these steps for implementing security in network, presented services in each unit can be defined in other words, security needs of each unit can be defined as a service. At this point, we should have IT vision toward the organization we already know.

In this view, security policies are introduced in the form of a set of security services in which ITIL model is suitable framework for IT service management. After this step, the organization achieves its initial integration and is prepared to implement security based on information security management system[7].

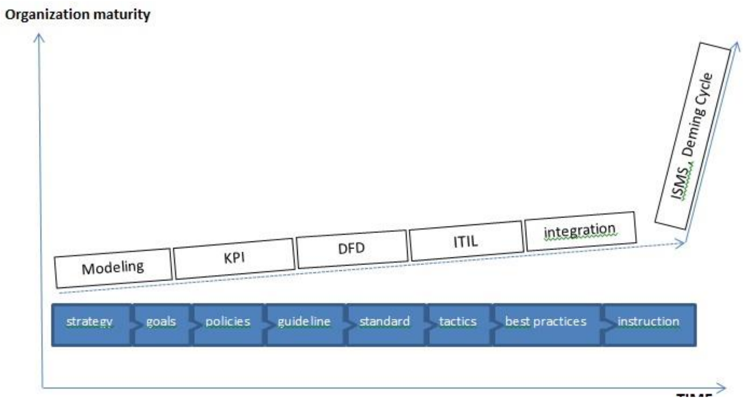

Figure 1: Deming Cycle and ISMS Implementation Steps in Service View

3.3.1. Implementation Results

Advantages:

- Security Policies Are Developed Based On Each Unit's Security Needs
- Structure, Organizational Structure And Management Standards Are Considered In Security Policies Codification
- It Has High Management Capabilities
- The Processes Are Integrated
- With Regard To The Integrity, The Organization Is Ready To Implement An Information Security Management System

Disadvantages:

- The maintenance process and updating is difficult.
- The codification of information security policies is a complex process.
- Scalability is poor.
- Flexibility is poor.
- Its implementation in large networks is difficult.

4. Suggested Model

In this study, inspired by existing models, and in order to improve security measures, we have proposed a new approach known as 2+20HSEC model that will be discussed in details in the following. In this model, the implementation of information security polices and communications in large and extensive networks is possible with minimum complexity and also according to the network extension it has high flexibility, scalability, management updating and processing and provides necessary conditions for continuity of organizations business and security assessment.

4.1. 2 +20HSEC Model

In this model, the network in addition to structures and facilities in the area of environmental security that also are considered as security implementation measures in other views, has 20 more separate parts with specific features. These parts are separated based on the needs of the organization, diversity of services, function and technologies. They are called blocks. Each block includes a series of equipment, process, and procedures so in each block equipment requirements, data flows, and process are identified and evaluated and analyzed as well as the relationship between them. So the blocks and the relationship between them can be integrated. In this model, Hierarchical networks infrastructure is used to link the equipment used in various parts.[1]

4.2. Network's Blocks in 2+20HSEC Model

In this model, in addition to the hierarchical infrastructure, the network is logically divided into some blocks. In the field of IT each block fulfills a part of the organization's requirements independently. This feature is very beneficial in the implementation of information security management system and raises network's performance.

Due to effects of some parameters like budget, time, and manpower on security implementation and confidentiality maintenance, availability and integrity of information assets and equipment, this division can be efficient. Also the assessment and evaluation of security in the network would be easier, faster, and cheaper.

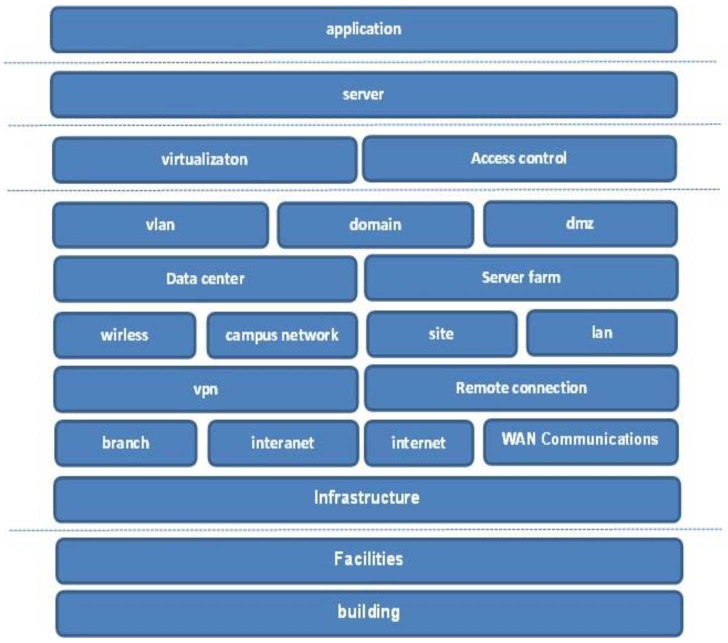

Figure 2: Network's Blocks in 2+20 HSEC Model View

4.3. Security Status in Block View

Since the network is divided into block, security implementation area is clearly divided into some parts. Each part consists of a set of strategies and information security policies that are developed according to security requirements, equipment processes and activities in these blocks and based on information security standards. In general it provides the conditions for protecting organization's assets and information.

4.4. The Architecture of the Suggested Model

The architecture of the presented model has got some steps and is based on Deming Cycle and information security management system. Each step consists of a number of processes. Finally the implementation existing activities in the above mentioned processes, provides necessary conditions for implementing security in each block. The steps and stages of the architecture of suggested model has been represented in the Figure 3.

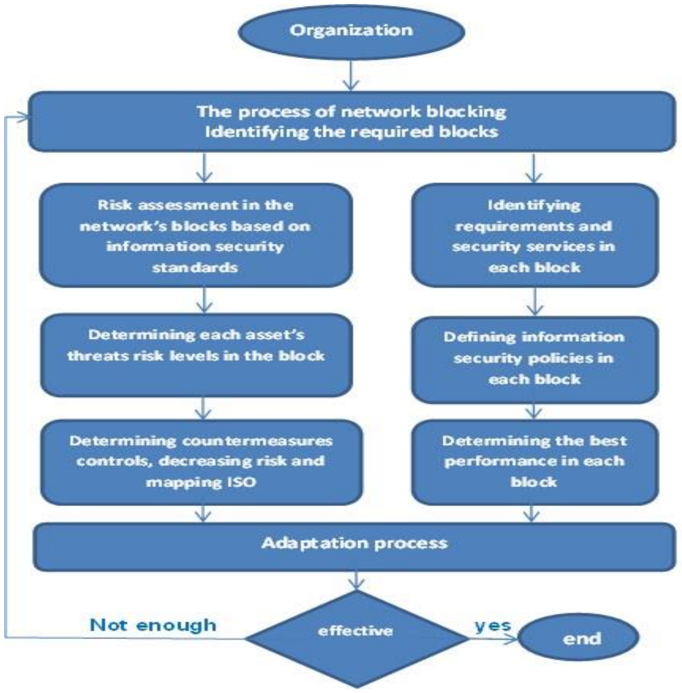
Organization
The process of network blocking
Identifying the required blocks
Risk assessment in the network's blocks based on information security standards
Identifying requirements and security services in each block
Determining each asset's threats risk levels in the block
Defining information security policies in each block
Determining countermeasures controls, decreasing risk and mapping ISO
Determining the best performance in each block
Adaptation process
Not enough
effective
yes
end

Figure 3: The Architecture of the Suggested Approach

5. Conclusions

In this study, inspired by existing model, we represented model to improve the indicators of security implementation in computer networks regarding the breadth and diversity of network services, the implementation of communication and information security policies in extensive networks with minimum complexity would be possible. Also, this model provides the necessary conditions for business continuity and security assessment.

In summary, the main advantages of the proposed model are as follows:

- The proposed model has the modular property
- The suggested model can be implemented in different areas of the organization totally or partially
- In this model the use of different assessment methods is provided
- In case of any changes and threats in network, security evaluation is done in related blocks
- In this model, assessment and evaluation are more powerful

The suggested model has been implemented in the area of access control in municipal services network and after making necessary assessments and evaluations, improvement in security components were visible. The following table shows the impact of network implementation parameters on access control security components quantitively in different views

table 2: Measuring the Impact of Parameters On security components

Security components in different views				Network implementation parameters
block	service	hierarchical	Equipment	
150	83.5	112	56	Extension
103.5	83	34.5	34.5	Continuity

6. References

[1] Haghverdi. M, 2014," Master Thesis: Framework for Access Control Implementation in Metropolitan Wide Networks Based on ISMS, Islamic Azad University, Zanjan Branch

[2] Sheikhpour, R,modiri. N, "An Approach to Map COBIT Processes to ISO/IEC 27001 Information Security Management Controls", International Journal of Security and Its Applications,april 2012, Vol. 6, No.2

[3] S. Toosarvandani. M, Modiri. N, Afzali.M. "The Risk Assessment And Treatment Approach In Order To Provide LAN Security Based On Isms Standard", International Journal In Foundations Of Computer Science & Technology (IJFCST), November 2012, Vol.2,No.6

[4] Stackpole, B, Oksendahl, E, 2011, "Security Strategy : From Requirements to Reality" , CRC Press Taylor & Francis Group an inform business

[5] L.Norman,T,2010,"Risk Analysis and Security Countermeasure Selection" , CRC Press Taylor & Francis Group an inform business , ISBN 978-1-4200-7870-1

[6] D. Frangopoulos, E,March 2007, "Social Engineering and The ISO/IEC 17799:2005 Security Standard : A Study on Effectiveness", University of South Africa School of computing

[7] Modiri. N, Fesharaki. B, Grivani.M, 2012, "Principles of Information and Communication Security Management Policy Planning", Mehregan Ghalam.

[8] Welcher, p, "Hierarchical network design model", Available Online at: <http://www.edrawsoft.com/Hierarchical-

Network-Design.php>, [Accessed on 2014/05/10]