ICIBA 2014, the Third International Conference on
Information Technology and Business Applications
Palembang-Indonesia, 20-21 February 2014

Data Security Model Design on the Intranet Using Ethernet Network Virtual Desktop in STIE Mulia Darma Pratama Palembang

Sabar Masdilam, Firdaus, Yesi Novaria Kunang

Master of Information Technology Program
Bina Darma University
e-mail: utiscipto@gmail.com

Abstract

The purpose of this study is to investigate and analyze the security issues of data and security models to design the intranet network using Ethernet virtual desktop , In this network all the resources contained on a computer server accessible by the client . Therefore, the data for the system and gated , it would require a different security with security when using network technology that does not use ethernet virtul desktop. For system security and data on the network using the Ethernet virtual desktop to do security refers to the standards of ISO 27001 . In the ISO 27001 standard twelve data security , but that according to this study is the issue of physical safety and environment (clause number 6) which includes physical security of computer servers and security networks that are connected to the server , communications and operations management (clause number 7) security through a network architecture that separates the remote server with a web server and a database server , the access control (clause number 8) security settings through a user the privileges to the server by right , time and name of the client computer , acquisition, development and maintenance of information systems (clause number 9)security through user must be fill user name and password in order to access xampp, phpMyAdmin and to be able to access the system through the 3 stages of the application must be the user name and password , compliance (clause number 12)security through the creation of security policies, procedures and Security policy conformance with regulations.

Keywords : *Data Security , Network Intranet which uses ethernet Virtual Desktop , ISO 27001*

1 INTRODUCTION

Development of an intranet network aims to support education so that college can provide better information to the community. In STIE Mulia Darma Pratama Palembang currently use the intranet as a tool to access the application program akedemik administrative information system for academic administration , faculty and students .The development of technology has now found a tool that serves as a client computer that does not use central processing, ie unit virtual ethernet desktop.Oleh therefore the use of personal computers that still use central processing, the unit that serves as the client computer is not favorable when compared with the use of virtual ethernet as desktop computers clientnya . Some things that hurt when using a client computer that still uses the central unit processing, when compared with the use of Ethernet virtual desktop is the cost of electrical energy consumption and greater software costs and also in terms of the control of the employees work hard to be monitored.Consider the advantages of the use of Ethernet virtual desktop , then STIE now using ethernet virtual desktops to client computers in a network intranetnya.In network intranet that uses virtual ethernet desktop all users can access the remote server resources , this results in all users can open the database and the very dangerous utuk data security of people who are not responsible.

Designing security model to maintain data security in intranet network using Ethernet virtual desktop is something that must be done because there are a lot of vulnerabilities that compromise the security of the data data.Dalam designing security models , information systems security standard used is ISO 27001 . International Standard Organization (ISO) has set the standard for security services that enable an open system interconnection between systems . Until now STIE Mulia Dharma Pratama security model does not yet have data on the intranet network using Ethernet virtual desktop. Based on the background that has been described here the authors tried to design a model of network security data on an intranet that uses the ethernet virtual desktop and make the research title is ”Designing Data Security Model in the Intranet Network Using Ethernet Virtual Desktop in TIE Mulia Dharma Pratama Palembang ”

2 RESEARCH METHODOLOGY

2.1 Research Methods

The method used in this study is action research methods (action research) . This method is a method of research that aims to develop new skills or new approaches and ways to solve problems with direct application to the object . In this study, researchers did a comparison between the data security standards applied are based on the ISO 27001 information security system consisting of 12 klause.Dalam this study not all clauses of ISO 27001 is used as a reference for comparison , as adjusted by the title of the study , then the 12 clauses of clause 5 are taken only as follows :

1. Physical and environmental security (clause number 6)
2. Operations management and communications (clause number 7)
3. Access control (clause number 8)
4. Acquisition , development and maintenance of information systems (clause number 9)
5. Compliance (clause number 12)

2.2 Method of Data Collection

To collect the data and materials research , the authors use data collection techniques interview , observation and Library Studies.

2.3 Analysis Tools

The method of analysis performed in this study are :

1. By analyzing the security level of data and analysis directly on the level of data security with the help of software.
2. Comparing Security Standard ISO 27001 information systems with actual circumstances.

3 RESULT AND DISCUSSION

3.1 Research Results

The results of this study is a model of data security in intranet network using Ethernet virtual desktop . By having a data security model it is expected that the data will be protected from people who are not responsible . From the analysis of the results has been done before it can be seen that there are many things that have not met 27001.Hal ISO information security standards that are not eligible include the following :

1. Physical and environmental security (protection of computer facilities) There is no protection against the physical server computer and its environment.
2. Operations management and communications (technical security controls in systems and networks) Remote server and web server are not separated , there is no protectionism remote server to the remote server.
3. Access control (restriction of access rights to networks , systems , applications , functions and data) Setting access only for local users, and restrictions on the right just under the right of the folder / file.
4. Acquisition, development and maintenance of information systems (security applications) There is no protection against web servers , database servers and application programs of academic administration
5. Compliance (ensuring compliance with information security policies , standards , laws and regulations) Has not made policies , procedures and information systems security standard.

3.2 Discussion

3.2.1 Security and the physical environment (Computer Facilities Protection)

3.2.2 Physical Computer Security Server

Computer servers must be protected by referring to the following :

1. Special room closed with a key that is only held by the server administrator.
2. Computer server room must have its own air conditioning.

3. The room should be free from the danger of flooding , and all sorts of animals that harm the server.

4. Make sure that the device is at least safe in a locked room.

5. Use the rack-mounted servers.

3.2.3 Data Security in hardsik

To maintain the security of the data on the hard disk of such harmful

1. Destruction of data

   To maintain that no data loss in the event of damage to the data on the hard disk it is necessary to perform backups of the existing data on the hard disk in accordance with the given period.

2. Data theft

   To prevent theft of data from a computer hard drive that is on the server , it must be encrypted disk partition and folder access rights must be set.

3.2.4 Security Uses USB port access and a DVD Drive

To keep data theft from the server , then access to data retrieval should be closed . Access data retrieval should be closed Mass Storage USB port , DVD drive.

3.2.5 Physical access security network

To maintain the security of the physical access network , it can be done by closing the access to the network , namely in the following way :

1. Close the access network via swich.

2. Close access via UTP cable.

3.3 Operations Management and Communication (Technical Security Control in Systems and Networks)

3.3.1 Remote Server , Web Server and Database Server Separated

Which is used as a remote server with a web server and a database server, which could endanger the security of the data, because the virtual desktop remote network server all resources accessible by the user. To overcome this, the remote server must be separated from the web server and database server.

3.3.2 Securing Virtual Server Remote Desktop

Security Server virtual desktop must be done to prevent users make virtual desktops on a remote server outside of his right, as do the following.

1. Deletion of a folder or file

2. Make changes to Windows settings
3. To install it or uninstall programs

To secure virtual desktop remote server can be done as follows :

1. Limitation of the right of access to the system, by providing a list hakakses content folder and read.
2. Restrictions on access rights to the data drive permissions list folder contents, read and write.
3. Restrictions on the right of access to the dektop folder with read rights.

3.3.3 Access Control (Restriction of access rights to networks , systems , applications , functions and data)

Control access to computer servers (web servers and database servers) needs to be set in accordance with the rights granted to the user . Distribution rights to the users who have access rights to the server to prevent data theft , data changes , loss of data by unauthorized people . To overcome this , it can be done by replacing the operating system on a server with windows 2003 server and its settings are as follows :

1. Setting domain and user logon and password settings
2. Setting user access time to the server
3. Computer settings for user access to the server
4. Audit user activity on seve

3.3.4 Acquisition , Development and Maintenance Information System (Security in the Application)

Securing data application program can be done in the following way :

1. Technical Threat (Security of virus attack).

   To maintain the security of data and applications in both the server computer and the client computer should be protected with a reliable antivirus can be updated every day.

2. Administrative and Physical Threat (Data protection with password).

   In order for a web application is not hijacked by people who are not responsible, then the web server must be protected with a password. Prevent data leak, changed or lost. then to be able to access the database server (MySQL) user must enter a user name and password.

3. Web Application Security Program.

   To maintain the security of data can be done through web application security program by requiring the user to fill in your user name and password when accessing the web foundation, web applications and web stie academic administration. By providing a layered security program it is expected that the application will be safe from hacker attacks.

4. Security (encrypt) password data.

   Password data stored in the database server is not encrypted then it will be easily read by the user, it would be very dangerous.This application system user can find out the password the user will be able to easily change the password and this will result in the system can be controlled by the user irresponsible. To overcome this, the password must be encrypted using MD5 encrypted.

5. Security (encrypt) data packets sent.

   Data packets are sent if it is not encrypted, it will be known by the user is not entitled, it makes the data leaked or stolen by others. To overcome this, the data packets are sent should be encrypted.

6. Observation of the web server access activities.

   To find out early existence that aims to steal user data or want to take control of the system, the necessary observations to the web server access activity view using Microsoft software Netword Monitor.

3.3.5 Compliance (kesusuaian Ensuring security policies in accordance with the standards , laws and regulations)

Security policy is the basis of the implementation of technical security , security policy has become so important that the security settings to be more effective and focused . The security policy includes the following :

Policy (Policies) security

1. Computer use policy
2. And maintenance of data backup policy
3. password policy
4. Network access policy
5. Security policy server .
6. Physical security policy
7. Campus Information Systems Policy
8. Policy protection against viruses

Security procedures

1. The procedure of scanning the computer for viruses.

2. Data backup procedure on the server.
3. New hardware installation procedure.
4. Application installation procedures.
5. Procedures of disaster fire, flood, riot.
6. The procedure of making a password.
7. Procedure replacement of faulty hardware.
8. Procedure file storage.
9. Network access procedures.
10. Procedure use of campus information systems.

Standard Security
Standard data security in STIE Mulia Dharma Primary using the ISO 27001 standard reference.

4 CONCLUSION

In the data security in intranet network using an ethernet remote desktop there are a few things that should be implemented to maintain the security of the data refers to data security standard ISO 27001 at 6.7 standard , 8,9,12 dalah as follows :

1. Physical security of servers, physical security includes physical security of the server computer and physical security of data on the server.
2. Full Technical Security in Systems and Networks, this control can be done through a separate remote server with a web server and database server.
3. Restriction of access rights to networks, systems, applications, functions and data , restrictions on the right can be done through windows server 2003.
4. Security in the application, to maintain the security of the application can be done through the protection from virus attacks and require the completion of a user and password to access.
5. Ensuring compliance in accordance with standard security policies, laws and regulations can be done through the development of policies, procedures and safety standards.

4.1 Advice

As for some suggestions that need to be delivered from this research include:

1. Implementation of the security model required an adequate IT readiness of personnel, facilities, infrastructure and security policy management support.
2. To further ensure thorough safety standards should apply across the ISO 27001.

3. To further ensure the security should there are three computers to the server computer server is a virtual remote desktops, computer to a web server, database server for the computer.

References

Naname,(2014), http://www.deltaprima.net/konsultan-iso-27001-consultant/ accessed on January 22.

Rahardjo, B., (2002), Internet-based information security system. Indonesia PT Insan Communications. duo.

Widyo, (2013), *www.docstoc.com ¿ Technology ¿ Computers & Internet ¿ Software Widyo.staff . Gunadarma . Ac . id / ... / file s / ... / Modules ke_10_sim_PTIK.doc*

Zulkarnain, *(2012)http://zul03mkz.blogspot.com/2012/03/peripheral-input-dan- output - ncomputing.html accessed on October 17, 2013*