PAULO MÁRIO CHIPAKO

ID UD34136BMA42710

CONTROL AND SECURITY OF INFORMATION SYSTEM

ATLANTIC INTERNATIONAL UNIVERSITY

HONOLULU, HAWAII

June, 2015

Table of Contents

Introduction: Purpose of the topic

Information Security Control is being one of interesting topics in the arena of Information Technology. As possible pressures emerge and develop as headline newscast, network and systems administrators are required to step on new grounds, such as casual police officers, and as private detective. As the Internet progresses into experiences of mind-boggling evolution, powered by, amongst other issues, the ubiquity of some software servers, the quick growth of the available software server exposures and the difficulty of protecting the institutions´ main computers from the nasty assaults and so-called gentle instructions.

In this study we would like to bring up some of the reasons why the information systems are so susceptible to damage, fault, misuse, and structure excellence problem, at the same time we need to find out the adequate measures to follow in order to control the available information systems in at Lurio University as our main case study. For the commercial institutions might need to know what kind of measures to setup in order to guarantee the consistency, readiness and safety of electronic business and digital trade procedures.

Lurio University uses Linux servers, however there is no such a thing as a secure network server, the Linux operating system was intended to have a very sturdy attention on security, and its open-source character allows network administrators, developers, and end users to constantly audit it for vulnerabilities. It´s precisely this ability to look “under the hood” that brands Linux the platform of excellent in situations where security is just as significant as great readiness and ironclad stability.

This study focuses on what it takes to make Lurio University Linux servers as secure as possible, and how to ensure that they continue to be secure, even in the face of the ever mutating array of malicious threats that plague the Internet today.

There will be presented in this study practical step-by-step advice on how to harden a Linux installation, starting with a “stock” distribution using freely available software tools

Description

In order to have a clear understanding of security and control of information system, there is a need of breaking this theme into three main terms. Staring with the terminology Information System which defines the organized collection, processing, transmission, and dissemination of information in harmony with clear processes, in automatic way or manually. While the term security might be well-defined as policies, measures and technical methods used to avoid unlawful contact, change, robbery, or physical destruction to information systems. The term security is directly related to the term control, this term is described as means, procedures and organization processes that guarantee security of institution’s resources; correctness and consistency of its office accounts; and operative loyalty to management values.

Lurio University has adopted the usage of Linux servers. This choice has come up due to the number of reasons. One of it is cost, in comparison with other servers, most of Linux server are open sources. The second reason come in due its robustness, this is the factor in the discussion of this paper. The fact of being robust does not mean that it cannot be attacked by the hackers.

Like any other server, Linux has to be well configure with strong firewalls and the security principle have to be well applied in order for it to secure the data.

Information security is a very important issue, does not just affect the Linux Community, other technological areas are also affected. While the general aim of protecting the institution´s network is to retain illegal people from the severs, there is a growing necessity to permit public access to some the main computers serve. Perhaps, it is necessary to sustain a public web and FTP server, as well as public DNS server. The host that should be mostly exposed is the bastion, there it should never be located in the similar section as the private severs. It is a well-fortified host, henceforth the name. A bastion host is naturally considered and preserved by the system administration supervision who are

well-informed concerning the security matters involved in configuration of open servers such as these.

Thinking of the bastion host as the letterbox setup in the main entrance of the house, next to the gate. It´s accessible to anyone, but it is at a harmless space and it is actually parted from the house. Someone can desire to think of a bastion host as a lookout in a army division, safeguarding the rout before the core group.

The Information Technology Centre of Lúrio University is establishing a network systems with a strong administrative control, ate the same time should be physically separated from the private network. This type of segment is known as a demilitarized zone (DMZ). The DMZ is quiet a minor network, composed of a half-dozen of personal computers or only a number of bastion hosts. It is often connected to a different network card interface passing in a firewall. However, a DMZ sometimes may be placed as an midway section amid the firewall and the internet access router.

General Analysis

With the beginning of the internet revolution came the capacity of hundreds of geographically spread software developers to collaborate on projects that would had been incredible just years before. It was the fall of 1991, and while the Internet hadn´t yet become the household name that it is today, a global team of talented software junkies was hard at work crafting what would become the most successful public-domain software offered of all time: the Linux operating system.

There are four basic goals for the Information security, namely:

Confidentiality of the Data: In this progressively open world, sustaining the secrecy of the data in an institution is a round-the-clock duty of a server administrator. Since many workers completely depend on network main computers in most of the daily activities in the office. Consequently, they rely to keep the secrete and reserved information into these facilities. The introduction of cryptography has empowered the administrator of Linux Server systems with an vital device to guarantee privacy by letting workers to encrypt complex data kept in the main computers. Linux cares the main two keys which are private and public encryption, these are the two major ways of cryptographic encryption.

Data integrity :when the hacker manages to get hold of the institution´s data in the process of internet transition, a hacker has the opportunity of doing any of these:

- ✓ Utilize the data for wicked aims, such as changing it or use for economical gain.
- ✓ change the information just before reaching its proposed target.
- ✓ Abolish completely all the information.

One of the main priorities although it is not confidential is to guarantee the integrity of the information during the process of the internet transmission. In the instance, take in mind a web-driven facility over which a client can download security patches to firm´s software products. While the patches themselves can be downloaded in the clear, it is serious that the client be guaranteed that the patch has not been wickedly changed.

Cryptography, is again necessary when using the digital signatures involved to the patch distribution, the client has the opportunity to confirm the legitimacy of the software that wants to install in the computer.

Access Control and Authentication of Users: Authentication is one of oldest needs of mankind. Since the origin of communities with diverse rights and privileges, the man has been requiring to have a legitimate authentication a member of the particular community or group. The visual inspection has been the most obvious authentication of mankind, for example; “I know, you look like Mary, for surely, you´re Mary”. A little more erudite method of authentication is based on the possession´s subject of a symbol that is distinctive to the theme’s uniqueness and that only the theme should be capable of producing (in instance, a password or a driving license). In the terms of Internet, it is noted as a meek username/password authentication, which is the major method of authentication in online systems.

The Availability of Data and services: Some have come to conclude that in the modem error of networking and wireless communications the only truth fully protected system is a brick-nothing goes in and nothing comes out. This might be true, nevertheless, network administrators cannot just take this drastic attitude. The truth is, the concert of most system administrators is usually dignified by their skill to retain the systems continually up and available from the communal network. There are clear motives why the network administrator would like to keep up the servers continually.

The main purpose of the Lurio University´s security strategy, device and strategy application, and formation management is to meet each of the above aims.

Lurio University is adopting the implementation of Linux servers; however, this operating system is no longer invulnerable to threats than any other Unix variation. Being an open-source produce, it is under the responsibility of developing team and client societies to guarantee that at any time when a susceptibility is located, it is publicly exposed and the right solution is made accessible at the right time. Linux is well known in this aspect. The other aspect that make Linux become an excellent choice of the operating system platform among many information system administrators has to do with the frequent analysis to which the source code is exposed almost every day.

Nevertheless, no matter how diligently, we might secure the Linux server, chances are that the server might get attacked. There are four well known character natures that can be used to characterise the invader community as a whole. These are: Joy riders, Cult members, spies and insiders.

Actualization

According to the UK Online for Business, Information Security is defined as the practice of safeguarding the information from being read, head, changed, broadcasted so that cannot be used other people who do not have the right.

Information systems have to be protected if they are to be trustworthy. Since many institutions are seriously dependant on their information systems for key business process (e.g. webs ites, productions scheduling, transaction processing), Information Security should be looked upon as a key are in managerial success.

Question that can be asked is “what might be incorrect with the information systems?” Data elements are always vulnerable in every information system;

there are a number of factors both internal and external. Here are some of the errors such as human, technical, accidents, disasters, frauds, commercial espionage as well as malicious damage.

Looking at the above risks, the question that might follow might be; “how to secure the Information Systems?” In fact, in the world of technology, there cannot be found any reliable safety for information systems.

When the information administrators are designing security controls for the information, factors such as prevention, detection, deterrence and data recovery have to be well addressed.

Going back to the case study, Lurio University will device and sustain managerial, physical, and technical security that will safeguard correctly the privacy, reliability, and disposal of universities data that it generates, obtains, keeps, or diffuses.

The information strategy set up by the university gives the details of information security control used in order to guarantee the reliability of the universities information. This will be achieved if both the information system that is software and the hardware as well as the entire technology infrastructure are well secured. The main goal of this strategy is to guarantee the best mode of access of the minimum licence and partition of obligations for the setup, usage, and propagation of the data.

A lot of effort has been devoted to the security of Information System at Lurio University, there is a firewall built, however, the intruders will never be left to penetrate into the gateways of the main computers. The safety strategy that is being implemented begins at the centre of the servers, and goes on moving to the safety tools out of the structure itself. The defence has to cover the network structure of the main computer, the network applications that run on the main computer, the limit of the communal network, and even the distant contact of the client done by road fighters to get hold of the corporate resources from the public Internet.

Discussions

Information system security is one of the main factors in the success of any institution; however, managing information system security is seen in most cases by many managers as a very difficult task to deal with. It is commonly alleged as an addition cost to a business by concentrating on “negatives”, especially when questioning the wrong that might go on.

It is very costly to maintain first of all the information system manager in an organization; consequently, many institutions prefer to put their information at risk. The second challenge has to do with the cost hardware and server software, however, with the advent of the open-source such as Linux Server operating system, the cost of has dropped, although, some still hold on to the enterprise software which are indeed very costly.

However, the benefits obtained from the well secured information system are numerous, for instance:

- ✓ The accuracy and efficiency are guaranteed when the system is frequently updated and secured
- ✓ The capacity of the institution increases when the information system is secure, for example online sales can increase as the customers a able to buy 24 hrs a day 7 days a week.
- ✓ The losses are reduced as the risks of management are effective.

General Recommendations

Plain and simple, Lurio University needs to secure the most important information resources, that might compromise the functionality of the institution. The decision has to be taken, of which data to secure and how it should be done. Till now has not yet been calculated the cost of if the system might crash or if the data is stolen or even damaged by the malicious changes. The institution has to put this as one of the privileged activities and should be well budgeted.

One of the main challenges is that in the age of information in which we are now, some companies are merging up with the exclusive purpose of changing the integrity and availability of the data, this comprises online information, banks, investments and profits administration organisations, and the awesome popular of business-to-business dealings by internet. Therefore, it is necessary to guarantee that the information in the data centre is secretive and accessible to the right people ate the right moment, this will ensure the reliability of the data.

The safety of data should not be seen just as a product or a software nor just an excuse for a consultation engagement. It´s a subject needed to be considered in decision the information system manager needs to undertake as a network and system administrator. Information Security has neither beginning nor end. Security is not installed by the system administrator, and can´t even be bought by anyone. Rather than, it trained, documented, designed decisions, and implemented. Above all, safety is intensive care and polishing the safety strategies when necessary.

A security policy should be the master document for any information system administrator, is also a task declaration, and the decisive font that states the rest of co-workers what is the manager desires to protect and how he needs to

protect. Some institutions may rent an outsider specialist to drawn from the tap this strategy, this often falls back on the plate of the network administrator.

Another important issue in the security control is to limit the administrative privileges to a reduced number of users with a good understanding of the need to administer both the operating systems and the requirements of the business. The main purpose of this is to avoid the installation of the illegal software and other manipulations of administrator rights. In order to accomplish this Lurio University will designate an administrator responsible for the information system with the respective sub managers who will be given different administrative rights.

For example under the SIGUL – management integrated system of UniLurio, the registrar will be responsible for the both the registration of the students as well as managing the records – modifying if necessary. While the assistants will be given only the right of registering the students into the system, they cannot modify any data of the students without the permission of the registrar.

The administrators will be recommended to do all remote administration of the servers, workstations and other devices using protocols with a strong security as such as SSH, telnet, RDP and VNC.

Conclusion: A new perspective

According to legend, security terrorizations has its origin from erudite script hackers with a very high knowledge of network and operative structures. These mythical individuals are inspired by a noble wish to force insensitive computer companies to mend their software. If this were correct, Lurio University servers running on Linux operating system would not be a target for security attacks. Altogether, Linux is an open-source script. None can come up to say that a commercial monument is getting hold of the script beyond reach. If these mythical characters were actually protestors contrary to the commercial structure, working to develop the safety of the software of operative system, they could be creating a fresh Linux code. Unfortunately this in not true, and Linux is among the greatest common goals of the attackers.

The reality of network attacks is both more sordid and more mundane than the mythology. Some attacks come from petty criminals out to steal credit card numbers. But most attack comes from inexperienced individuals who run small attack code that are so simple to use they are called “kiddie scripts.”

Clear, **open**-source script cannot be preventive. Individuals running attack scripts are not interested in “fixing” the structure; their aim is only to look for cool targets. My main task should be to ensure that the University´s Information system is not an easy target.

Good security is a fundamental part of good system administration. Security is essential to running a reliable Linux system. The university might be attacked and negotiated by users on the network. In order to diminish the currencies of prosperous attacks, limit the volume of destruction caused, and rapidly recover from the attack, there is a need of possessing the appropriate tools and abilities to use them.

Once the security policy is completed and implemented, the university data will be well secured. The policy which is still in draft mode comprises of both aspects of local users and internet users, both software and hardware security. The control will be incorporated into all applications regarding the administrative, physical and technical aspects.

There will be a Large Security Application system implemented not only to the software, but also to the routine activities that are require the correct functioning of the information system in the university. The routine activities will include software and hardware maintenance, updating the firmware and the control of all historical registers of all package changes.

There will be a division of responsibilities in order to implement the security and control policy of the information system. The information system manager will be responsible for the publishing and maintaining the guidelines for securing the large security application, operating systems and package software. He will also make sure that the supervisors are designated for each large security application and every application is given a security level already described in the policy. Finally, he will guarantee that all the hardware, operating systems and software packages security controls are functioning correctly.

The second responsibility will be given to the large security application manager who will organize the policy guidelines for the security of the Large Security Application hardware, operating systems and application software he will need to review the Large Security Application at least in very three years or at a period he might choose to be convenient.

The system security should never be affected whenever the repair and maintenance activities are being executed. In order accomplish this, there will be a need of designating an individual whose role will be to supervise the maintenance and repair activities. There also be established modes for the maintenance and emergency repairs.

Configuration management procedures will be documented for the maintenance of all applications including hardware. These procedures will include the control of the version associated to the system components in order to make sure that are proper and adequate.

Lurio University will make sure that all the necessary administrative, physical and technical controls are merged in the control and security policy of information system. Without a good and adequate policy, the data of the university will be vulnerable to any attack both internal and external.

References

- ✓ Critical Security control, https://www.sans.org/critical-security-controls/control/3, 15/July/2015
- ✓ Harrison, Peter, Linux Quick Fix Notebook, Prentie hall, New York, 2005
- ✓ Hotanon, Ramon, Linux Security, Sybex, London, 2001,
- ✓ Hunt, Craig, Linux Network Servers, Sybex, London, 2002
- ✓ Managing and Maintaining a Microsoft windows server 2003, Microsoft, 2005,
- ✓ McCoy, John, Mastering Web Design, BPB Publications, New Delhi, 1996
- ✓ OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources. 1996
- ✓ Sample Generic Policy and High level Procedures for Hardware and Application Software Security, xx Agency AISSP Handbook, May 1994
- ✓ Schroder, Carla, Linux cookbook, O´Reilly Media, Inc, Paris, 2004
- ✓ Sharp, Vicki, Computer Education for Teachers, Mc Graw Hill, New York, 2002
- ✓ Veeraraghavan,Sriranga, Shell Programming, sams, Indiana, USA,1999