International Journal of Current Advanced Research
ISSN: O: 2319-6475, ISSN: P: 2319-6505, Impact Factor: 6.614
Available Online at www.journalijcar.org
Volume 8; Issue 11 (A); November 2019; Page No.20355-20358
DOI: http://dx.doi.org/10.24327/ijcar.2019.20358.3973

Research Article

COMPUTER SECURITY POLICY AND MECHANISM SURVEY

Jemal Ayderus and Sheik Omer

Jigjiga University, Ethiopia

A R T I C L E I N F O

Article History:
Received 4th August, 2019
Received in revised form 25th September, 2019
Accepted 18th October, 2019
Published online 28th November, 2019

Key words:

Computer Security Policy and Mechanism Survey

A B S T R A C T

Ensuring the security of corporate computer security policy mechanism that is increasingly in the stored, processed and disseminated using security of the Technologies has become an extremely complex and challenging activity in the scenarios. This is a particularly important concern for knowledge-intensive in any of the organizations, such as universities, as the effective conduct of their core teaching and research activities that is becoming ever more reliant on the availability, integrity and accuracy of computer-based security mechanism survey resources. One increasingly important mechanism for reducing the occurrence of security gap and the breaches, and in so doing, protecting corporate information security policy.

INTRODUCTION

Def: Computer Security: is refers to Techniques for ensuring the data that is stored in the computer system's and the computer cannot be read or modified it again or compromised or the way of reaching the agreements by any individuals without authorization of the user. The *computer security* has many different interpretations based on what era the term describes. Early on, computer security specialized in keeping the glass houses in which the computer is core was positioned safe from deliberately destroying, along with providing the access and constant cooling and electricity. As computers has becoming more dispersed in terms of the security became more and more of an issue of preserving data and protecting its validity as well as keeping all the secrets secret As computers moved onto the desktop computers and into the home, computer security is main tool to took the form of protection against data thieves and the network attackers. The modern computer security includes considerations of *business and application* A threat is an indication of an approaching the points or the context of the circumstances that form the setting in an for an event, statement, or idea, and in terms of which it can be fully understood computer security, refers to anything that has the potential to cause serious harm to a computer system. The adversary goal, or what a might try to do to a system.

It is also described as the capability of an adversary is an enemy or someone who opposes someone else. to attack a system (1) swiderski & snyder, 2004).

Corresponding author:* **Jemal Ayderus
Jigjiga University, Ethiopia

This ability mitigates and something less serve in the interruption interference, intervention, intrusion, obtrusion, or loss regardless of the threat, and more importantly, develops rational systems that estimate and offset risk.

Goals of Security

Prevention

It means failure of an attack on the computer system or resources.

It involves implementing mechanisms that a system of parts working together unauthorized users cannot override and that they are implemented correctly is that the attacker cannot defeat the mechanism to alter it. E.g. use of passwords

Detection

These mechanisms aim to determine can be to occur in a particular way or to have a particular nature if an attack is underway, have already occurred and report such details effectively. It is useful if the prevention mechanisms fail. E.g. it gives the warning when a user enters an incorrect password 4 times.

Recovery: It takes two distinct forms. It stops the attack. It then assesses and repairs any damages caused by the attack. E.g. if a file is deleted, the recovery mechanism will be to determine which documents have been deleted and then restores them from backup tapes and records. It may also involve identifying and fixing vulnerabilities to prevent the same attack/breach. System works correctly while an attack is underway.

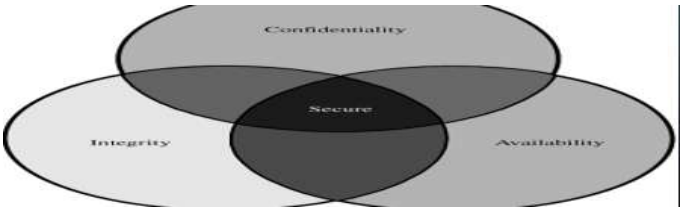
Definition of Terms Security

- ***Attacker threat agent*** is the Threat Agent is used to indicate an individual or group that can manifest a threat. It is fundamental to identify who would want to exploit the assets of a company, and how they might use them against An entity that attacks, or is a threat to, a system
- ***Attack****:* is to setup to set upon or work against forcefully. How to use attack in a sentence. Synonym Discussion of attack. An assault on system security that derives from an intelligent threat; a deliberate attempt to evade security services and violate security policy of a system.
- ***Countermeasure****:* is an action or device designed to offset another the most well-known countermeasure by a physician is a malicious-persecution suit against the lawyer who sued him and failed to prove a case. An action, device, procedure, or technique that reduces a threat, a vulnerability, or an attack by eliminating or preventing it, by minimizing the harm it can cause, or by discovering and reporting it so that corrective action can be taken.
- ***Risk****:* is the uncontrolled loss of something of value. Values such as physical health, social status, emotional well-being, or financial wealth can be gained or lost when taking risk resulting from a given action or inaction, foreseen or unforeseen

An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.

- ***Security Policy****:* A set of rules and practices that specify how a system or org provides security services to protect sensitive and critical system resources.
- ***System Resource Asset****:* Data; a service provided by a system; a system capability; an item of system equipment; a facility that houses system operations and equipment.
- ***Threat****:* A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.
- ***Vulnerability****:* is the weakness which can be exploited by actor, such as an attacker, to perform unauthorized actions within a computer system. To exploit a **vulnerability**, an attacker must have at least one applicable tool and the Flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy. However, the system may disable non-essential functions. These values are incorporated and Computer and system security is defined as the art or science of protecting computer resources from unauthorized access use or alteration. And two key challenge in making security usable is determining exactly who the users are all too often, we consider only end users and ignore the sometimes convergent, sometimes conflicting usability needs of developers and systems administrators. Computer security rests on confidentiality, integrity, and availability**. (2)** Jansen (2011).This posits that threats outside the organization can be from outsiders not working for the organization .threats caused by human actions such as insiders or hackers which cause harm or risk in systems **(3)** abdulkadir, &dzarma, 2015; shaluf, 2007)..The interpretations of these three aspects vary, as do in the contexts in which they arise. The interpretation of an aspect is in a given environment is dictated by the needs of the individuals, customs, and laws of the particular organization.

These are the three mian goals in computing Security.



1. Confidentiality
2. Integrity
3. Availability.
4. VULNERABILITY

Confidentiality: involves the set of rules and ensures and can also be the protection of personal information or a promise and the usually executed through confidentiality agreements that limits access or places restrictions on certain types of information and make that computer basic related assets are accessed only by authorized parties. Study identified three categories of information threats such as accidental or unintentional contributory or instrumental, and deliberate or intentional greitzer, strozer, cohen, more**,(4)** Mundie, &Cowley, 2014; afyouni, 2006).

Confidentiality is sometimes called secrecy or privacy. The confidentiality is the concealment and act of that keeps in the information and resources is the basics. The basic need for the information in the form of secret arises where a person gives property to another, communicating to that person an intention that the property be dealt from the use of computers in sensitive fields such as government or the people who control and make decision and industrial parking need to be safe. The best example is the military and civilian institutions in the government often restrict access to information to those who need that information. The second formal work in computer security was motivated by the military's attempt to implement controls to enforce a need to know principle. (5) (Bompard, huang, wu, &cremenescu, 2013). That principle is also applies to industrial firms, which keep their proprietary designs secure lest their competitors try to steal the designs. All types of institutions keep personnel records secret. Access control a way of limiting access to a system or to physical or virtual resources the computing is any activity that uses computers that can manage process and communicate information for various purposes.(6) (jouini, rabai, &aissa, 2014). It includes development of both hardware and software. And the access and the control mechanism is a process by which all the users are granted acce**ss** and certain privileges to systems, resources or information. Mechanisms are in the support and the confidentiality and one access control mechanism for preserving confidentiality is cryptography in which scrambles data to make it incomprehensible. A cryptographic key controls to the unscrambled data, but then the cryptographic key itself becomes another datum is also a piece of information to be protected for the Resource hiding is another important aspect of confidentiality. often wish to be conceal their configuration and as well as what systems they are using in the

any organizations may not wish others to know about specific equipment It can be used without authorization and instruments of the users or in the inappropriate ways of company renting time from a service provider may not want others to know what resources it is using. Access and control mechanisms provide these capabilities as well.

Integrity: is the top quality of being honest or it means that trustworthiness of data and/or resources assets can be modified only by authorized parties or only in authorized ways. Integrity it means that assets can be modified only by giving permission or authorized parties or only in authorized ways. Mention or allude to. The trustworthiness of data or resources and an action or strategy which may be adopted in adverse circumstances that is usually phrased of preventing improper or unauthorized change. Integrity can be included data integrity the content of the information and origin integrity the source of the data, often called authentication. The source of the information may bear carry bring transport move convey in the accuracy and credibility and on the trust that people place in the information can be contrast between two things that are or are represented as being opposed or entirely different of the principle of that the aspect of integrity known can be as credibility is central to the proper functioning of any system. Integrity mechanisms part of the systems that is used to produce fall is the to descend freely by the force of gravity into two or more classes and prevention and mechanisms and detection mechanisms. The Prevention and acting of mechanisms seek to maintain the integrity of the data by blocking any unauthorized attempts to change the data or any attempts to change the data in unauthorized ways. The distinction between these two types of attempts is important. The former happens or exist when a user tries to change data which he/ she has no authority to change. The latter occurs when a user authorized to make and not having any doubt or changes in the data tries to be changed the data in other ways. Detection is the process of discovering and finding the mechanisms do try to prevent violations of integrity; they simply report that the data's integrity is no longer trustworthy. Detection mechanisms may analyze system events (user or system actions) to detect problems or (more commonly) may analyze the data itself to see if required or expected constraints still hold.

Availability*:* It is the quality of being improves that assets are accessible to authorized parties at appropriate times. Availability is the state of current to refer the ability to use the information or resource desired. Availability is the fact of that something that is an important aspect of reliability as well as of system design because an unavailable system is at least as bad as no system at all. The aspect or the directions of availability that is relevant to security is that someone may deliberately arrange to deny access to data or to a service by making it unavailable. (7) Halmstad University, 2010. System analysis and designs usually assume a statistical model role to analyze expected patterns of use, and mechanisms ensure availability when that statistical model that holds. Someone people may be able to manipulate use or parameters that control use, such as network traffic. So that the assumptions of taking upon one of the statistical model are no longer valid. Accomplish or to complete to availability called denial of service attacks, can be the most difficult to detect and because the analyst must determine if the unusual access repeated forms are attributable to deliberate manipulation of resources or of environment.

Vulnerability: Vulnerability is a weakness is sometimes called Creativity. Delegating tasks in the security computer system refers to the inability of a system or a unit to withstand the effects of a hostile environment. A window of vulnerability**.** Can intimidating appear in any element of a computer, both in the hardware, operating system, and the software vulnerabilities we might find as they apply to the assets of hardware or software, and data These three are the most assets and the connections among them are all potential security weak points.

Goals of the Security: One of the challenges in building a secure system is finding the right balance among the goals, which often conflict. A security policy's specification of secure mechanisms and no secure actions, these security mechanisms can prevent the attack, detect the attack, or recover from the attack. The strategies may be used together or separately.

Prevention means that an attack will fail. An example for attempts to break into a host over the Internet and that host is not connected to the Internet, the attack has been prevented. Typically, prevention can be involves implementation of mechanisms that users cannot override and that are trusted to be implemented in a correct. The attacker can defeat the mechanism by changing security .Preventative and mechanisms often are very cumbersome and interfere with system use to the point that they hinder normal use of the best system. But the main preventative mechanisms, such as passwords and in which aim to prevent unauthorized users from accessing the system), have become widely accepted.

Detection is most useful and when an attack cannot be prevented and also indicates a significances, but it can also indicate the effectiveness of preventative measures. Detection accept that an attack will occur; the goal is to determine that an attack is underway, or has occurred, and report it. The attack may be monitored to provide data about its nature, severity, and results. Typical mechanisms monitor various aspects of the system, looking for actions or information indicating an attack. Mechanism is a warning when a user enters an incorrect password three times. Recovery is more complicated or processing an instance of recovering especially an economic upturn as after a depression. How to use recovery in a sentence the system is also group of related parts that moves or work together or continues to function correctly while an attack is underway. This type of recovery is quite difficult to implement them because of the complexity of computer systems. It draws on techniques of an unattractive unpleasant to look and unsatisfactory feature, especially of work or in a person's character. As well as Techniques of security mechanism and is typically used in safety and critical systems. It differentiate from the first form of recovery, because at no point does the system function incorrectly. However, the system may be disable nonessential functionality.

A threat: is have capacity to develop an important software or a potential violation of security.

- Indication is piece of information that indicates of an approaching or imminent menace.
- Negative event can cause a risk to become a loss, expressed

That the violation need not actually be contarvertaial occur for there to be a threat. In the fact that the violation or acting of doing something that is not allowed by the might to express possibility and that occur means that those actions that could cause it to occur must be guarded or prepared for. Those actions are called attackers .Those who execute such actions or cause them to be executed and that are called is attackers.

CONCLUSION

In this kind of research work, we have studied the major concept of security and various threats in the computer security. The result of this study is that increasing day by day the reliance by business and the security of the computer system on the use of data processing system and the increasing use of network infrastructure and communications facilities to build distributed systems have outcome in a strong requirement for computer and network security.

The requirements for security are best assessed by examining the various methods of the security threats that is faced by any organization. The interruption of service of the computer security is a threat to availability. The interception of information is a threat to secrecy. Finally, both the modification of legitimate information and the unauthorized fabrication of information are threats to integrity.

Reference

1. EC-Council, Network Defense: Security Policy and Threats – 1st Edition (Apr 2010) Cengage Learning.
2. James Michael Stewart, Network Security, Firewalls and VPN-4th Edition (2011) Jones & Bartlett Learning Canada.
3. Willing Stallings. Operating System Internals and Design Principles – 3rd Edition New Jersey: Prentice-Hall International.
4. Avi Silberschatz, Peter Baer Galvin, Greg Gagne Operating System Concept – 9th Edition John Wiley & Sons.
5. B. Daya, "Network Security: History, Importance, and Future," University of Florida Department of Electrical and Computer Engineering, 2013.
6. J. E. Canavan, Fundamentals of Network Security, Artech House Telecommunications Library, 2000.
7. A. R. F. Hamedani, "Network Security Issues, Tools for Testing," School of Information Science, Halmstad University, 2010.
8. R. E. Mahan, "Introduction to Computer & Network Security," Washington State University, 2000.

How to cite this article:

Jemal Ayderus and Sheik Omer (2019) 'Computer Security Policy And Mechanism Survey', *International Journal of Current Advanced Research,* 08(11), pp. 20355-20358. DOI: http://dx.doi.org/10.24327/ijcar.2019. 20358.3973

****