ISSN:0971-1260
Vol-22-Issue-10-November-2019

Analiticalstudy Of Computer Network Security In It Infrastructure Management

Dr. Sachin Chavan

(Associate Prof. Department Of Management, Zeal College Of Engineering and Research, Narhe, Pune.)

Mob: +91:9850919264 Email: sachin.chavan@zealeducation.com

Ms.Aishwarya Darekar

(PG Student, Department Of Management, Zeal College Of Engineering and Research, Narhe , Pune.)

Mob:+91:9689791921 Email: aishwaryadarekar13@gmail.com

Dr. Snehal Sashte

(Assistant Professor Department of Management, Zeal College of Engineering &Research, Narhe, Pune 41 Mob.9790899922. Email. snehalsashte4@gmail.com)

ABSTRACT

This paper analyzes that how the organizations manage thereInformation technology security. computing system security is one of the most important issues that businesses all over the world strive to deal with. However, the world has now changed and in essential ways. The desk-top computer and workstation have appeared and proliferated widely. The net effect of all this has been to expose the computer-based information system, i.e. its hardware, its software and its software processes, its databases, its communications to an environment over which no one not end user, not network administrator or system owner, not even government has control.

Keywords assurance; computer security; information security; introduction; risk management; security controls; security required

Introduction

All Organizations are mainly used information technology (IT) services to run their day-to-day business. Security id most important for all the organisation.

Network security is very important for all industries like information technology, Manufacturing industry, Automation industry.

Network security is important for business world networks. Also mostly for homes with high speed internet connections have one or more wireless routerd switches which are unsecured if not properly configured. Network security helps to data loss and also get secured from thefting of

ISSN:0971-1260
Vol-22-Issue-10-November-2019

data.The main aim and the purpose of network security system is to secure network and also secures that several hardwares and software used in the orginasations.Network system security protects the organisational systems safety, integrity and reliability and usability.

There are various types of Networking and there security.

What is Networking and What are the types of networking and networking topologies are studied in this report.

What Is Network

Networking means the total process of creating and using computer networks with respect to the hardware, protocols and software which includes wired and wireless technologies.

An example of networking is exchanging information with people interested in similar areas. An example of networking is aquiring information between various departments of the same organisation to share information and solve the business problems.

- **COMPUTER NETWORK SECURITY OVERVEIW**

1. Prevent unauthorised network access
2. Protect the privacy, integrity and sensitive information of users in the network
3. Protect the network from external attacks, hacks and prevent unauthorised users from gaining access to the network
4. Protect the network from malware from different attack types
5. Protect the all data,stored and in- transit and to secure all information in the network from being stolen by malicious users
6. To ensures availability of the network.

LITERATURE SERVEY

Computer system security and information technology security are the most important issues that all over business world struggle. IT security issues understood in 1960s and how to secure

ISSN:0971-1260
Vol-22-Issue-10-November-2019

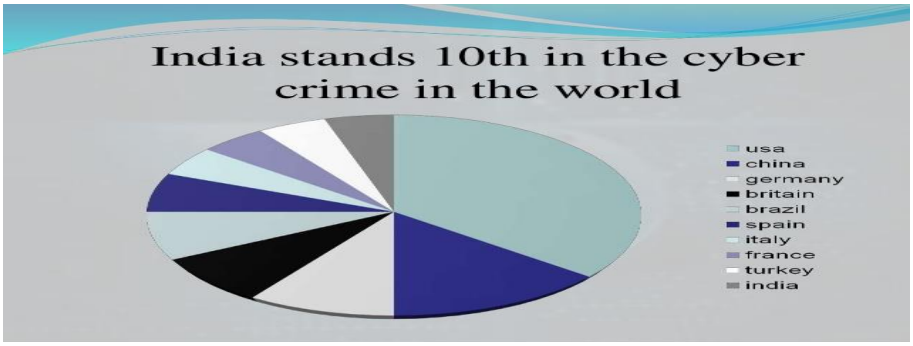
computer system from unauthorised access. and it also includes issues of protecting software against illegal change and and secure the entire system.

Information technology security or computing system security is one of themost important issues that businesses all over the world strive to deal with.Thus, IT security issue, as it was understood in the 1960s and even laterwas how to create in a computer system a group of access controls thatwould implement or emulate the processes of the prior paper world, plusthe associated issues of protecting such software against unauthorizedchange, subversion and illicit use, and of embedding the entire system in asecure physical environment with appropriate management oversights andoperational doctrine and procedures.The poorly understood aspect of security was primarily the software issuewith, however, a collateral hardware aspect; namely, the risk that it mightmalfunction or be penetrated and subvert the proper behavior of software.

For the related aspects of communications, personnel, and physicalsecurity, there was a plethoraof rules, regulations, doctrine and experienceto cover them. It was largely a matter of merging all of it with thehardware/software aspects to yield an overall secure system and operatingenvironment.However, the world has now changed and in essential ways. The desk-topcomputer and workstation have appeared and proliferated widely. TheInternet is flourishing and the reality of a World Wide Web is in place.Networking has exploded and communication among computer systems isthe rule, not the exception. Many commercial transactions are now web-based; many commercial communities have moved into a web posture.The "user" of anycomputer system can literally be anyone in the world.Networking among computer systems is ubiquitous; information systemoutreach is the goal.

The net effect of all this has been to expose the computer-basedinformation system, i.e. itshardware, its software, its software processes,its databases, its communications to an environmentover which no one—not end user, not network administrator or systemowner, noteven government—has control. What must be done is to provideappropriate technical,procedural, operational and environmentalsafeguards against threats as they might appear or be imagined,embedded in a societally acceptable legal framework. And appear threats did—from individuals and organizations, national and international.The motivations to penetratesystems for evil purpose or to createmalicious software— generally with an offensive ordamagingconsequence—vary from personal intellectual satisfaction to espionage, tofinancialreward, to revenge, to civil disobedience, and to other reasons.Information system security has moved from a largely self-containedbounded environmentinteracting with a generally knownand disciplined user community

India stands 10th in cybercrime. Geographical represnation shown in below diagram.



ISSN:0971-1260
Vol-22-Issue-10-November-2019

Research Objectives

- Preventing unauthorised users from using a system spitefully
- avoiding users from performing automatic operations that are capable of harming the system
- safeguarding data failures
- ensuring that services are not interrupted

RESEARCH METHODOLOGY

The following methodology has been used in this study.

Analytical Research:

Data analysis done by using Analytical Research Methodology and Primary Data collection method is used. Analysis is the process of gathering and comparing information about the web and its operation and use in order to improve the web's overall quality and to identify problem areas.

The purpose of the research is to discover answers to questions through the application of-scientific Procedures. The main aim of the research is to find out the truth which is hidden and which has not been discovered as yet. Though each research study has its own specific purpose, we may think of research objectives as falling into a number of following broad groupings:

To portray accurately the characteristics of a particular individual, situation or a group (Studies with this object in view are known as descriptive research studies);

To determine the frequency with which something occurs or with which it is associated with something else (studies with this object in view are known as diagnostic research studies);

Method of research

1.Network access Control
2.Application Security
3.Antivirus and Antimalware software
4.Email Security
5.Wireless security

DATA COLLECTION

ISSN:0971-1260
Vol-22-Issue-10-November-2019

It includes descriptive facts on numerical information, quantitative And qualitative information. Collection of data is an important stage in research. Quality of data determine the quantity of research**.**

1) PRIMARY DATA: Gathered through in-depth conversations, electronic surveys, Live chat, Email, Telephone interview or a series of informal discussions.

ANALYSIS AND INTERPRETATION OF DATA

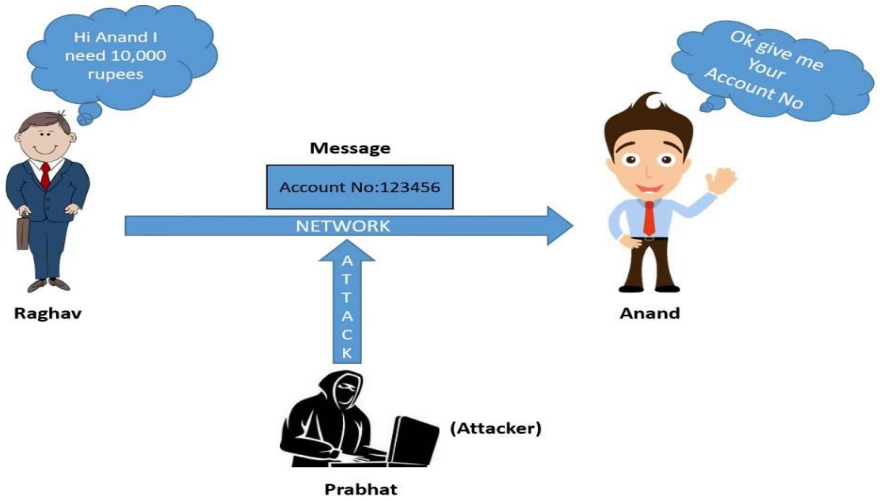
After the data has been analyzed and summarized the next step is linking the results with the research objectives, stating clearly the implications of the findings and doing all this with an objective and rational approach.

In Organization network infrastructure included so many years .Evolution of IT industry includes direct response to changing business needs.like any other changes ,network and security changes may result into some other fault.

Systematicapproach of evolution of it industry ensures that architecture technology and security policy of organization,management practices and plans are changed.

The process of collection of data nd studying that how the organization protect there computing systemadministratively and physically.
We have collected primary data by conducting questionnaires.The main aim of primary data is to gather the all information of the organization

- Personal data get protected by network security.
- Information shared between the computers are protected by network security.
- If we are using network security hacking attempt get reduced.
- External attacks also prevented by network security.
- Virus, spyware attacks not able to harm your system.



ISSN:0971-1260
Vol-22-Issue-10-November-2019

Fig: Basic concept of data Hacking

FINDINGS

Below are the findings of network security

- What are different security plans
- Is there Risk analysis in security plans
- What are the different security policies
- What are the different physical treats and disasters

Observation and findings based on survey

Intrusion detection system are highly required for computer network security. 93% companies agree that intrusion detection system is must for there computer network security.
It is observed that there is no single solution to protect your system ,there are multiple layer of security. Network security accomplished by hardware and software.
Network security system consist of many components, ideally combined layered approach minimizes maintainance and improves network security.Not any single too, provides the foolproof solution hence we require firewall and antivirus must together.

The most critical security threats to computer network security is unauthorised access, unauthorised access means gaining access to any computer or network without authorisation. this unauthorised access generally used for existing privileges and stealing privileges
95 % employees agree that highly confidential date is stored in there computers.
Security is mandatory because of confidential data stored on there system

Network security is associated with the cost like hardware cost, software cost, maintain ace cost, cost of incorrect decision making.
Compromise with security is associated with this cost.

100% organisation strongly agree that computer network securityis very essential because compromise with security associated with huge amount of cost. Compromises with security has financial consequenses.To reduce this all consequences requires network security.

Conclusion:

In this analytical study of network security we have studied that business and non-business organization importance of network security and they are able to protect there systems from unauthorised attacks, hacking, thefts and ensures that smooth running of these systems at all times. As internet usage increase.Security threats where analysed to determine necessary

ISSN:0971-1260
Vol-22-Issue-10-November-2019

security technology. Development of network security is not very impressive and significant. Therefore researches are rapidly involving developing and investigating the treats.

Reference:

WEBSITES
1.www.docplayer.com
2.www.studymafia.org
3.jocpr.com

BOOKS

1. Threats of cunter measures ,IEEE spectrum.Adam j 1992
2. Network and internet security AP professional Ahuja v 1996
3. Fundamentals of network security. By canavan
4. Firewall and internet security by Addison-wesely.