British Journal of Applied Science & Technology

British Journal of Applied Science & Technology
4(31): 4380-4394, 2014
ISSN: 2231-0843

SCIENCEDOMAIN *international*
www.sciencedomain.org

Computer Security Measures, Tools and Best Practices

O. Kadiri Kamoru[1*], Ibikunle Frank[2] and Ajiteru Yemi[1]

[1]Department of Electrical/Electronics, Federal Polytechnic, Offa, Kwara State, Nigeria.
[2]Electrical and Information Engineering Department, Covenant University, Nigeria.

Authors' contributions

This work was carried out in collaboration between all authors. Author OKK designed the study, performed the statistical analysis, wrote the protocol, and wrote the first draft of the manuscript and managed literature searches. Authors OKK, IB and AY managed the analyses of the study and literature searches. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/BJAST/2014/9140
Editor(s):
(1) Mark Vimalan, Department of Physics, Syed Ammal Arts and Science College, India.
(2) Rodolfo Dufo Lopez, Electrical Engineering Department, University of Zaragoza, Spain.
(3) Singiresu S. Rao, Department of Mechanical and Aerospace Engineering, University of Miami, Coral Gables, USA.
Reviewers:
(1) Fatty M. Salem, Department of Electronics, Communications and Computers, Faculty of Engineering, Helwan University, Cairo, Egypt.
(2) Anonymous, G. Pulla Reddy Engineering College (Autonomous), India.
(3) Anonymous, East Carolina University, USA.
(4) Anonymous, Lovely Professional University, India.
(5) Anonymous, University of Michigan Health System, USA.
Peer review History: http://www.sciencedomain.org/review-history.php?iid=635&id=5&aid=5930

Original Research Article

Received 23rd January 2014
Accepted 29th April 2014
Published 1st September 2014

ABSTRACT

Unauthorized computer access is one of the most common, troublesome and potentially destructive behavior problems facing society. It is the high-tech equivalent of breaking and entering a home or business. Once the unlawful entry has been accomplished, what happens next depends on the level of the intruder's destructive intent, computer skills,

[*]Corresponding author: E-mail: kadiritoyin2007@yahoo.com;

and the value of the property available for destruction or theft. This paper highlights the tools needed to fight computer insecurity and the best practices that are needed to guide our infrastructures from being accessed in an unauthorized setting.

Keywords: Computer network security; authorization; authentication; security measures.

1. INTRODUCTION

When computer was first invented, it was meant to stand alone. But as time goes on, the Computer Engineers developed computer network which makes it easier for two or more computers to be connected together and communicate with a view to sharing resources, such as printers, telephone lines, fax machine, scanner, drives etc. Since the invention of network, the issue of network security has been a major challenge simply because a computer network is prone to attacks from virus, worms, intruders etc than a standalone computer.

Computer network is the connection of two or more computer systems together in order to share resources, such as printers, drives, internet, telephone lines, fax machine, applications etc. They are in the following broad categories:

a) Local Area network
b) Metropolitan area network
c) Wide area network

1.1 Local Area Network

This is a connection of two or more computers or workstations within a small geographical area, such as building, offices, schools etc.

1.2 Metropolitan Area Network

This is a connection of two or more computers or Workstations within metropolis. It is a connection of two or more LAN within metropolis.

1.3 Wide Area Network

This is a connection of two or more computers within a large geographical area, such as one country to another, from one city to another or from one state to another or one country to another e.g. Nigeria to Ghana, and Nigeria to India etc. While the Internet, which is usually referred to as World Wide Web is the world's largest network that originated out of a US Department of defense funded project. It is a unique collection of networks with vast proportions [1].

1.4 Computer Security

Generally, the terms privacy, integrity and confidentiality are loosely constructed to be synonymous with security. These however have different connections with respect to data or information; they also address different areas of information systems.

Data or information security is the protection of data against accidental or intentional destruction, disclosure or modification. Computer data security refers to the technological safeguards and managerial procedures, which can be applied to computer hardware, software and data to ensure that organizational assets and individual privacy are protected. Privacy is a concept applied to an individual. It is the right of an individual to decide what information he or she wishes to share with others or is willing to accept from others [2].

1.5 Breaches of Security

This reveals a number of the ways through which data loss or manipulation occurs.

a. Larceny of Laptop and Media: Destruction possible on a stolen device by means of false identification or false pretency.
b. Damage towards Breakage: Auxilliary storage like Floppies, CD ROM, USB Flash drive are prone damage either by envasion, PCs relocation, rearrangement and possible remove and replace of faulty hardware while troubleshooting.
c. Natural Disaster: Damage occurs on natural causes like storms, floods, electrical and other natural causes like fire or earth quake.
d. Environmental Damage: The manufacturer of devices give guide and recommendation on certain environmental conditions like temperature and humidness ranges, voltage limits etc.
e. Corruption/Loss: It is a common hazard that occurs as a result of using inferior media and unreliable cheap products which resulted to faliure and destruction of files as a result of constrait factors [3].

1.6 Physical Protection of Machine and Media

Control and observation of access to data from remote location depends on users integrity which should be clearly outlined, and responsible for guaranteeing selected tasks in line with modality of an audit procedural approach in a long way to ensuring adherence to ordered down prototype. There four defined principles for guaranteeing security and recovery just in case of breaches of security. They are:

1.6.1 Prevent

The simplest methodology is by stopping all breaches of security before they occur. The policy is an upshot of the principle of preventing.

1.6.2 Detect

There could be guarantee in total security if user is ready to notice breaches to security whenever it occurs at intervals the shortest attainable time. This facilitates harm assessment and conjointly in making any preventive measure. Minimizing harm is to contain the damage once losses occur to scale back the adverse impact of such harm.

1.6.3 Recovery

There should be enough resilience within the system to recoup the losses /damages and become useful by reinstating the standing at the earliest [4,5].

1.7 Denial-of-Service Attack

Unlike alternative exploits, denial of service attacks are not accustomed to gaining unauthorized access or management of a system with the scope to render entire system unusable. The attackers will deny service to individual victims by deliberately coming into a wrong parole three consecutive times and therefore, inflicting the victim account to be bolted, or overload the capabilities of a machine or network and block all users access mode. Distributed denial of service (DDoS) attacks square measure common wherever an outsized range of compromised hosts square measure accustomed flood a target system with network requests, therefore making an attempt to render it unusable through resource exhaustion. Another technique to exhaust victim resources is through the employment of an attack electronic equipment, wherever the assaulter takes advantage of poorly designed protocols on third-party machines like FTP or DNS, it therefore instructs these hosts to launch the flood. There are usually found vulnerabilities in applications that can not be accustomed to take charge over a pc. This creates the target application malfunction or crash whole system as a result of a denial-of-service exploit [6].

1.8 Direct Access Attacks

The act of gained access to a pc by installing different types of devices to compromise security, as well as software modifications, software system worms, key loggers, and covert listening devices. The assaulter simply transfers giant quantities of information onto backup media.for example CD-R/DVD-R, tape, or transportable devices like keydrives, digital cameras or digital audio players. Another common technique is in addition software contained on a compact disc or alternative bootable media and skim the information from the harddrive(s) in this fashion.

1.9 Indirect Attacks

An indirect attack is an attack launched by a third-party pc. By victimising somebody else's pc to launch an attack, it becomes much more tough to trace down the particular assaulter. There have additionally been cases where attackers took advantage of public anonymizing systems, like onion router system [6].

1.10 Computer Security Best Practices

Computer system can be secured in various ways by adopting protective practice to protect laptop, mobile phones, money,personal identity, Desktop computer and network facilities.These show major ways to minimise risks. Hackers have thousands of tools at their disposal to require advantage of users as well as tools like keystroke loggers. Keystroke loggers record each single keystroke user sort on laptop, and other computer devices. These include users sign in for non-public email messages, checking account information and mastercard number. With the use of web via a high-speed association (DSL or cable), hackers attempt fliping laptop into a "zombie" to launch attacks against thousands of different users and computers [7].

The research focuses on Microsoft Windows users since the bulk of laptop users nowadays use a version of this software package in their home and workplace computers. whereas not as frequent as targets of hackers with different operational systems like macintosh OS and Linux also which are liable to attack.

1.11 Data and System Security Measures

These measures apply to anyone, World Health Organization accesses, uses or controls, University pc and knowledge resources, including, however not restricted to school, directors, staff, students, those engaged in the University, guests, tenants, contractors, consultants, visitors, and/or people approved by related establishments and organizations [6].

1.12 Basic System Security Measures

These Basic System Security Measures apply to all or any systems , no matter the amount of their System Classification, it is a baseline, that all systems should meet. Note that for many personal workstations, these squares measure the sole measures that apply. Part of the necessities is word protection, that is, all accounts and resources should be protected by passwords that meet the subsequent necessities, that should be mechanically implemented by the system and it should be a minimum of eight characters long.

1.13 Intermediate System Security Measures

These Intermediate System Security Measures outline the safety measures that have to be applied to Medium Criticality and High Criticality systems. Note that except below special circumstances, they are really not apply to desktop and portable computer computers.

1.14 Authentication and Authorization

Take away or disable accounts upon loss of eligibility :Accounts that are no longer required should be disabled during a timely fashion automatic or documented procedure. Separate user and administrator accounts: Administrator accounts should not be used for non-administrative functions. System directors should be provisioned with non-administrator accounts for end-user activities, and a separate administrator account that is used just for system-administration functions.

1.15 Use Distinctive Passwords for Administrator Accounts

Privileged accounts should use distinctive passwords that are not shared among multiple systems. Credentials that square measure managed centrally, like the NetID/password combination, square measure thought-about one account, no matter what percentage of the systems they supply access to.

Throttle recurrent unsuccessful login-attempts: A most rate for unsuccessful logins should be implemented. Account opposition is not needed, however the speed of unsuccessful logins should be restricted. change session timeout:

1.16 Enforce least privilege

Non-administrative accounts should be used whenever attainable. User accounts and server processes should be granted the least-possible level of privilege that permits them to perform their operation.

1.17 Synchronize System Clock

The system clock should be synchronal to associate authoritative time server travel by organising a minimum of once per day.

1.18 Change System Work and Auditing

The facilities needed to mechanically generate, retain, and expire system logs should be enabled.

1.19 Follow Associate Applicable Log Retention Schedule

System logs should be maintained for 30-90 days and so destroyed unless any retention is important attributable to legal, regulatory, or written agreement necessities.

1.19.1 Audit in Logins

Generate a log message whenever a user with success logs in. Audit unsuccessful login: make an attempt to generate a log message whenever a user attempts to log in while not successful.

1.19.2 Security Partitioning

Systems could share hardware and resources solely with alternative systems that have similar security necessities, no matter their criticality classification. Systems that share similar security necessities have user communities of comparable size and character, similar firewall profiles, and similar technical necessities. As an example, Multiple systems of an equivalent criticality also share hardware and resources provided they need similar security necessities. Medium Criticality systems could share hardware and resources with Low Criticality systems on condition that all systems meet these Intermediate Systems Security Measures, and share similar security necessities.

1.19.3 Follow Merchant Hardening Guidelines

This document can not be comprehensive for all systems out there. But basic merchant recommendations to harden and secure systems should be followed.

Disable merchant default accounts and passwords: several systems accompany default accounts that square measure in public proverbial. These accounts ought to be disabled. Disable all extra network services: Processes and services that are not necessary to complete the operate of a system should be disabled.

1.20 Report Potential Security Incidents

Potential security incidents should be reported to head of IT department to prompt actions.

1.20.1 Security Review

Throughout the look of the technical design, a review of the system should be requested from ITS Technology Security Services.

1.20.2 Vulnerability Assessment

Before system readying, a vulnerability assessment should be requested from ITS Technology Security Services.

1.20.3 Physical Access

The system should reside during a barred facility, to that solely approved personnel gain access.

1.20.4 Documentation

Documentation should be produced and maintained by summarizing the business method, major system parts, and network communications related to a system [10-13].

1.21 Advanced System Security Measures

These Advanced System Security Measures outline the safety measures that should be applied to High Criticality systems. the necessities are:

1.22 Audit and Answerability

Change method auditing or accounting: change method auditing or accounting that generates log data regarding the creation of latest processes and their system activities. Audit privilege step-up or modification in privilege: Generate a log message whenever a user changes their level of privilege.

1.23 Audit Firewall Denial

Generate a log message once the host-based firewall denies a network association.

1.24 Audit All Important Application Events

Log all important application events. Write audit events to a separate system: System logs should be written to a distant system in such a way that they can not be altered by any user on the system being logged configuration and maintenance.

1.25 Follow Advanced Merchant Security Recommendations

This document can not be comprehensive for all systems and applications out there. It should be adapted to best practices and proposals made public in merchant security whitepapers and documentation [8].

1.25.1 Host-Based and Network-Based Firewalls

Systems should be protected by each a host-based and a network-based firewall that permits solely those incoming connections necessary to meet the business would like of that system.

1.25.2 Configuration Management Method

Configuration changes should be regulated by a documented configuration and alter management process.

1.25.3 Partitioning

Systems could share hardware and resources solely with alternative systems that have similar security necessities, no matter their Criticality classification. Systems that share similar security necessities have user communities of comparable size and character, similar firewall profiles, and similar technical necessities. For example, Multiple systems of an equivalent Criticality is also collective along to share hardware and resources provided they need similar security necessities. High Criticality systems could share hardware and resources with Medium and Low Criticality systems on condition that all systems meet these Advanced Systems Security Measures, and share similar security necessities [9,10].

1.26 Data Handling Security Measures

These data Handling Security Measures outline the minimum security necessities that should be applied to the info varieties outlined within the Reference for knowledge and System Classification (www.nyu.edu/its/policies/sec_ref.html). Some data components, like mastercard numbers and patient health records, have extra security necessities outlined in external standards.

The best method to safeguard sensitive data is not to handle it in the least, and business processes which will be amended to scale back or eliminate dependence on restricted data to be corrected. For example, the University ID variety will typically be substituted for a Social Security variety and poses a lot of less risk if accidentally disclosed [11].

1.27 Necessities for Handling Confidential Data

Access control: Access to confidential data should be provided on a least-privilege basis. not everybody or system ought to tend access to the information unless needed by business method. In such cases wherever access is needed, permission to use the info should be granted by the info Steward [12].

1.27.1 Sharing

Confidential data is also shared among the internet community. It is going to be free in public solely in step with well-defined business processes, and with the permission of the information steward.

1.27.2 Retention

Confidential data ought to solely be held on for as long as is important to accomplish the documented business method. There should be incident notification, once there is a possible security incident that will place protected data in danger of unauthorized access, ITS Technology Security Services should be notified.

1.27.3 Collection

Restricted knowledge ought to solely be collected once all of the subsequent conditions square measure are met. There should also be destruction once restricted data is no longer required. It destroys victimisation strategies that square measure immune to data recovery, this makes an attempt like science data destruction utilities, on-site physical device destruction or certified data destruction service [12].

1.28 Measures against Security Breaches

This section checks up on the varied measures on the market to the laptop user, to make sure security of machine and knowledge regarding the principles enumerated in previous section. Data security should be an important area of concern for every business owners or organisation. With a few basic steps and some good online habits, user can prevent thier devices using essential data security measures.

1.29 Establish Strong Passwords

Implementing strong passwords is the easiest thing that a user can do to strengthen device security. The algorithsm of shares and crafting a hard-to-crack password; use a combination of capital and lower-case letters, numbers, and symbols, and make it 8 to 12 characters long gives exellent ways to secure access.

According to Microsoft, you should definitely avoid using:

- any personal data (such as birthdate)
- common words spelled backwards
- sequences of characters or numbers, or those that are close together on the keyboard.

Use their convenient password checker to see how strong yours is. As for how often user should change password at every 90 days freqently in other to safe guads remote access. Providing layout for individual to have his own username and password for any login system for computer devices. One should put up a strong firewall. In order to have a properly protected network, firewalls protects all network by controlling internet traffic coming into and flowing out of business.

1.29.1 Install Antivirus Protection

Antivirus and anti-malware software are essentials in user arsenal of online security weapons, as well. It serves the last line of defense blocking unwanted attack one gets through to network.

1.29.2 Update Programs Regularly

Making sure the computer is properly patched and updated on regular basis and this is a necessary step towards being fully protected so if there is a little point in installing software therefore, it requires a regular maintainance for maximum security. Security applications are good when they are constantly or regularly updated.

1.29.3 Secure laptops

Because of laptop portable nature, laptops are at a higher risk of being lost or stolen than average company desktops. It is important to take some extra steps to make sure that certain user sensitive data is protected.The Fig. 1 illustrates how a secured network could be protected against an attack. A secured network cannot be invaded or compromised while a strong fire wall is built for all clients on server domain.

1.29.4 Secure mobile phones

Since adoption of mobile technology like smartphones which hold so much data, therefore classify as valuable asset to individual and companies. Mobile phones are more easily lost or stolen. As such securing them is another must by practicing the following strategies

a. Encryption software
b. Password-protection
c. Remote wiping enabled

1.29.5 Backup Regularly

Scheduling regular backups to an external hard drive or in the cloud is a painless way to ensure that all data is stored safely.

The general rule of thumb for backups servers should have a complete backup weekly and incremental backups every night. With personal computers, back up should be accomplished completely every week, but user can do incremental backups every few days if possible. Getting data compromised is a painful experience, therefore having it all backed up will avoid losing data errornously.

1.30 Monitor Diligently

This great technology has no good unless user actually use it in righful manners. One good monitoring tool the expert suggests is data-leakage prevention software, which is set up at key network touchpoints to look for specific information coming out of user internal network. It can be configured to look for credit card numbers, pieces of code, or any bits of information relevant to business that would indicate a breach.If users do not monitor things, there could be a waste of time and a waste of resources. User will not know when devices and data been compromised until it is too late.

1.31 Awareness of Email, IM and Surfing the Web

It is not uncommon for an unsuspecting users to click on a link or download an attachment that they believe is harmless . Only to discover they have been infected with a nasty virus, or worse. Links are the number one way that malware ends up on computers and as an experts. Denoted that Links are bad so to be aware never click on a link that you are not expecting or do not know the sourcebin, an email or IM.

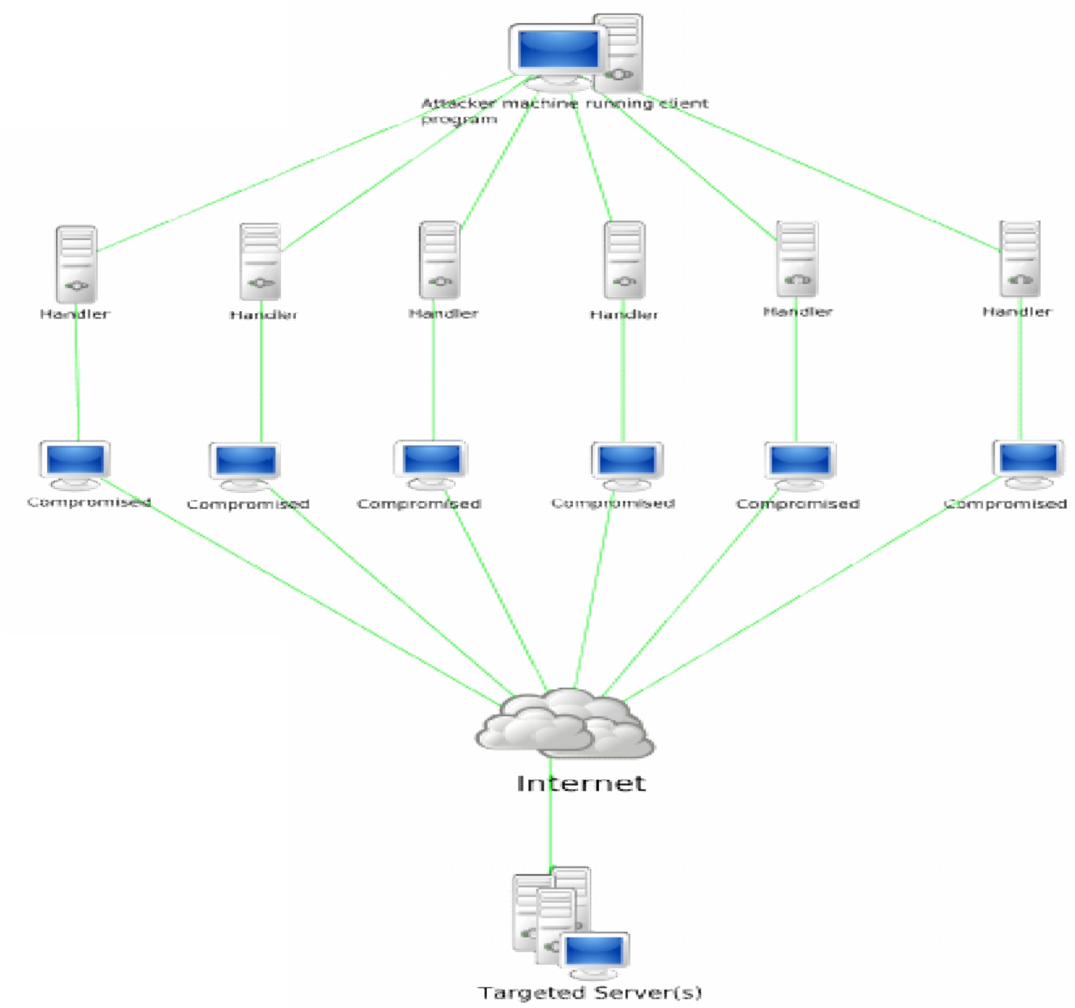

Fig. 1. A strong firewall on client machine

1.32 Educate Employees

Teaching employees and users about safe online habits and proactive defense is crucial. Educating them about what they are doing and why it is dangerous is a more effective strategy than expecting IT security staff to constantly react to end users bad decisions," Watchinski says. It is not easy: "One of the most difficult things to do is protect end users against themselves, But ultimately prevention is the best approach to handling data security. Make sure users and employees understand the importance of company's data which include personal profile, and all the measures they can take to protect it [10,12].

1.33 Physical Security

These measures arrangement and location of PCs within office settings where laptop could be in use by a private or being shared between two or a lot of users. Therefore, impact measures to be made are:

a) Physically bolt down the laptop to a table because leaving loosely can be nonchalantly left , dislocated and even taken away;
b) Locate the laptop in such the simplest way that is handily accessible to the user, however hidden from casual passers- by.
c) Set up likeable cabinets for floppies and keep on sight on easy access while use or not in use
d) Keyboard and laptop should be protected using locking device and mounted securely so that the laptop usage will be impossible unless these locks area unit are opened
e) Keep a record of all floppies, CD’s and flash in use; do not allow strange disk into the organization
f) Secure both entrance and exit of office or studio using reliable locker particularly PCs with sensitive data. Create observable locker to area.

1.34 Environmental Conditions

The PCs environemt is another factor to be considered for security measure because user enviroment depends on wide ranges of temperatures, humidity and voltages However, to ensure systems life cycle dependability and maintanability the following guide has to be taken into account the subsequent measures.

a. To ensure temperature and humidity gauges placed within the operational mode of PCs and Laptop system and keep an off-the-cuff watch to make sure that conditions square measure is within limits and switch if the bounds square measure exceeded.
b. If power grid provide is subject to giant variations of voltage and frequency or spikes, it is prudent to build backup power supply and automatice voltage regulator system for steadiness and effciency for the computer usage.
c. Ensure that excessive dust or paper scrap does not accumulate to computer system.
d. Secured the plug sockets outlet to match connections of cables and other interface links to terminals and ensuring it is secured properly and not left hanging [4,5].

1.35 Software Security

As a matter of clarifying treats in security varies among ethical use of softwares products on computer.There are square measure to be taken to ensure that information is not corrupted or changed by unauthorized users.The meansure of software security procedures are:

1) Use original code for software package, compilers or application packages. User should purchase original software to avoid hacking.
2) Adopt correct procedures for moving up and down the computer without shutdown also ensure all runing applicationa and file were close legally.
3) Apply password to any live applications which run database concurrently [4,13].

1.36 Network Security

The protection needed for network system is much in depth as physical security measures . it is a conjointly and extraordinary tough to detect host that gain access into network system using secured network protocols. In LANs layout, there should be one server that holds the shareable information on network and more so router that run services on requests nodes. The use of conventional methodology to countersign identity before granting access gives high measures that could be adopted as follows:

1. Keeping the servers away and limiting physical access to them.
2. Run servers within the background mode by rendering server a medium to reserve concurrent users within the network .
3. To be aware of network cables taping and bridging, therefore creating defend or conceal service retriction to stop simple access sometimes is attainable on fibre optics,
4. Use fiber-optic cables for sensitive networks since it is highly secure to break and tap thus, denying possesion and stealing information through sensing the perturbations of the fiber.
5. Prohibit the multiple attempt of passwords embedded access points by limiting attempt to maximum of 3 times before disable or barn user authentication.

1.36.1 Protection against Virus

A number of measure is obtainable for reducing the chance of attacked by pc virus:

a. Build worker awareness of the high level risk involved.
b. Do not access the company services and programs outside company premises using strange PCs.
c. Try and acquire ASCII text file for necessary code in use and compile it in house.

1.36.2 Password Security

In most organizations where computer system is their sole authorization for information interchange so an administrator has the right countersign. This can be most appropriate step to handle password security process:

1.36.3 Identification

Identification of user code while entring password is denoted by asteric characters to firmly secure visualisation object with a novel identity allotted. So, it should not become authorization to access information without any check of user profile if match on data base.

1.36.4 Authentication

This method verifies that an individual or user is authenticated for recognition claimed to be. This might be achieved by asking some normal queries and obtaining correct answers. If the answers match, it then allows user to continue access on target system, the person or object could be attested. using biometric and different physical authentication processes to ensure data is not compromised.

1.36.5 Authorization

The is the final stage of user verification method. Setting response time to ensure that user on access request is a registered or recognised member before granted access to resources. Authentication required logistic procedures through scaning, writing, and verifying credential as a means of clearance.Some time, matrix or capture are created to point that users have entered correctly before granting full access to records or resources. Once user passes the matrix then allowed access, otherwise denied access on request.

2. RECOMMENDATION

Based on findings and search through articles, text book and other media, investigation shows the major dimensional high measures for a protected information on stand alone and networked PCs which required logistic syntax ways to intrusion. Attempting to introduce multiple access level is best practice using aforemention security tools and obligue access protocol access by ensuriing secure collection for online access. To secure complex or gain system requires major stress and expert joint efforts on strategic ways to protect, detect and recover mechanism on giant systems which required high security measure by taking some factors into consideration such as physical hardwares, licence softwares and provide multiple level access to all devices online and offline mode.

3. CONCLUSION

In this research, pc security has been mentioned underneath physical security, code security, network security, virus security and countersign security. The paper conjointly reveals a number of the ways in which information loss or manipulation will occur, conferred measures against security breaches with a need to making awareness, and that will finally give a guide against security breaches. It is necessary that management and observance the access to information, its usage by persons and it's integrity should be clearly outlined and responsibility for guaranteeing these should rest on persons selected for these tasks. An audit procedure would go a protracted means in guaranteeing adherence to set down pointers. data classification; responsibility for security; pointers for creation and changes of password; exploitation coaching to extend security awareness and propagation of do's and don'ts also are small print to be taken serious of these square measures relevant for pc primarily based MIS implementation.

COMPETING INTERESTS

Authors declare that there are no competing interests.

REFERENCES

1. Ayeni RO. Computer Fundamentals, National Open University of Nigeria; 2004.
2. Milan Milenkovic, Operating System Concepts and Designs, Second Edition. Tata, Mcgraw Hill.
3. William Stalling, Computer Organization and Architecture, Third Edition, Maxwell Macmillan.
4. William Stalling, Data and Computer Communication, Prentice Hall of India.
5. Preservtion Domain. Available: http://www.preservearticles.com/201012301941/security-measures-for-protecting-your-computer.html
6. Web Open Media. Available: http://www.webopedia.com/TERM/S/security.html
7. Entrepreneur artical. Avaialble: http://www.entrepreneur.com/article/217484
8. Web Wikipedia. Available: http://en.wikipedia.org/wiki/Computer_security
9. Business Inside. Avaialbe: http://www.businessinsider.com/10-essential-data-security-measures-every-business-should-take-2010-6?op=1
10. Computer Resources: Available: http://www.sdms.org/resources/computer.asp
11. Polycy data system; Avaialble: http://www.nyu.edu/its/policies/sec_datasys.html
12. Business Inside. Avaialbe: http://www.businessinsider.com/10-essential-data-security-measures-every-business-should-take-2010-6?op=1#ixzz2whAtMn9n

Peer-review history:
The peer review history for this paper can be accessed here:
http://www.sciencedomain.org/review-history.php?iid=635&id=5&aid=5930