IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

Computer Security

Yaquob H. A. Alkandary[1], Eng. Fawzyeya M. A. Alhallaq[2]

Public Authority for Applied Education and Training, Computer Department

The Higher Institute of Telecommunication & Navigation, Kuwait City, Kuwait[1,2]

Abstract: The meaning of the term computer security has evolved in recent years. Before the problem of data security became widely publicized in the media, most people's idea of computer security focused on the physical machine. Traditionally, computer facilities have been physically protected for three reasons: To prevent theft of or damage to the hardware, To prevent theft of or damage to the information and To prevent disruption of service. Strict procedures for access to the machine room are used by most organizations, and these procedures are often an organization's only obvious computer security measures. Today, however, with pervasive remote terminal access, communications, and networking, physical measures rarely provide meaningful protection for either the information or the service; only the hardware is secure. Nonetheless, most computer facilities continue to protect their physical machine far better than they do their data, even when the value of the data is several times greater than the value of the hardware.

Keywords: Security, Data loss, Disaster, Backup.

I. INTRODUCTION

Computer security is information security as applied to computers and computer networks. The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Computer security also includes protection from unplanned events and natural disasters.

II. SECURITY AND SYSTEMS DESIGN

Although there are many aspects to take into consideration when designing a computer system, security can prove to be very important. Cyber security remains the top priority. Cyber criminals are finding ways to continue their activities. Almost every type of cyber-attack is on the rise.

III. SECURITY MEASURES

A state of computer "security" is the conceptual ideal, attained by the use of three processes:

1. Threat Prevention
2. Detection
3. Response

- **Useraccount access controls** and cryptography can protect systems files and data, respectively.
- **Firewalls** are by far the most common prevention systems from a network security perspective as they can (if properly configured) shield access to internal network services, and block certain kinds of attacks through packet filtering.
- **Intrusion Detection Systems** (IDSs) are designed to detect network attacks in progress and assist in post-attack forensics, whileaudit trails and logs serve a similar function for individual systems.
- **Destruction of compromised system** is favored in some special cases where not all the compromised resources are detected.

Today, computer security comprises mainly "preventive" measures, like firewalls or an Exit Procedure. A firewall is a way of filtering network, data between a host or a network and another network. It can be implemented as software running on the machine, hooking into the network stack to provide real-time filtering and blocking.

Another implementation is a so-called physical firewallwhich consists of a separate machine filtering network traffic. Firewalls are common amongst machines that are permanently connected to the Internet.

However, relatively few organizations maintain computer systems with effective detection systems, and fewer still have organized response mechanisms in place. Companies report losses are more through electronic theft of data than physical stealing of assets.

The primary obstacle to effective eradication of cyber-crimecould be traced to excessive reliance on firewalls and other automated "detection" systems. Yet it is basic evidence gathering by using Packet Capture Appliances that puts criminals behind bars.

IV. TERMINOLOGY IN COMPUTER SECURITY

The following terms used with regards to engineering secure systems are explained below:

- **Access authorization** restricts access to a computer to group of users through the use of authentication systems. It protects whole computer through an interactive login.Methods for identifying and authenticating users are by passwords, identification cards, smartcards and biometric systems.Authentication techniques used to ensure that communication end-points are who they say they are.
- **Anti-virus software** consists of computer programs that attempt to identify, thwart and eliminate computer viruses and other malicious software (malware).
- **Applications** with known **security flaws**, main entry used by worm should be turned off or patched or otherwise fixed or delete it and replace it with some other

application. It prevents spread to other systems connected to it. Security patching tool from website Secunia provides a search tool for unpatched known flaws in popular products.

• **Automated theorem proving** and other verification tools can enable critical algorithms and code used in secure systems to be mathematically proven to meet their specifications.

• **Backups** are a way of securing information; they are another copy of all the important computer files kept in another location on hard disks, CD-Rs, CD-RWs, tapes and more recently on the cloud. Locations for backups are a fireproof, waterproof, and heat proof safe, or in a separate, offsite location. Some individuals and companies also keep their backups in safe deposit boxes inside bank vaults. There is also a fourth option, which involves using one of the file hosting services that backs up files over the Internet for both business and individuals, known as the cloud.

○ Backups are also important for reasons other than security. Natural disasters, such as earthquakes, hurricanes, or tornadoes, fire, an explosion may precipitate crisis. It is recommended that the alternate location be placed where the same disaster would not affect both locations. World Trade Center I and the recovery site inWorld Trade Center, both of which were destroyed in the 9/11 attack. Also, having one's primary site and recovery site in the same coastal region are vulnerable to hurricane damage. Backup should be moved between the geographic sites in a secure manner, in order to prevent them from being stolen or destroyed.

• **Capability and access control list techniques** can be used to ensure privilege separation and mandatory access control.

• **Chain of trust techniques** can be used to attempt to ensure that all software loaded has been certified as authentic by the system's designers.

• **Confidentiality** is the nondisclosure of information except to another authorized person.

• **Cryptographic techniques**can be used to defend data in transit between systems, reducing the probability that data exchanged between systems can be intercepted or modified.

• **Data integrity** is the accuracy and consistency of stored data, indicated by an absence of any alteration in data between two updates of a data record.

○ **Encryption** is used to protect the message from the eyes of others. **Cryptographically secure ciphers** are designed to make any practical attempt of breaking infeasible. Public-key encryption using digital certificates can provide a practical solution for the problem of securely communicating when no key is shared in advance.

○ **Endpoint security software** helps networks to prevent data theft and virus infection at network entry points made vulnerable by the prevalence of potentially infected portable computing devices, such as laptops and mobile devices, and external storage devices, such as USB drives.

○ **Firewalls** are an important method for control and security on the Internet and other networks. A network firewall can be a communications processor, typically a router, or a dedicated server, along with firewall software. A firewall serves as a gatekeeper system that protects a company's intranets and other computer networks from intrusion by providing a filter and safe transfer point for access to and from the Internet and other networks. It screens all network traffic for proper passwords or other security codes and only allows authorized transmission in and out of the network. Firewalls can deter, but not completely prevent, unauthorized access (hacking) into computer networks.

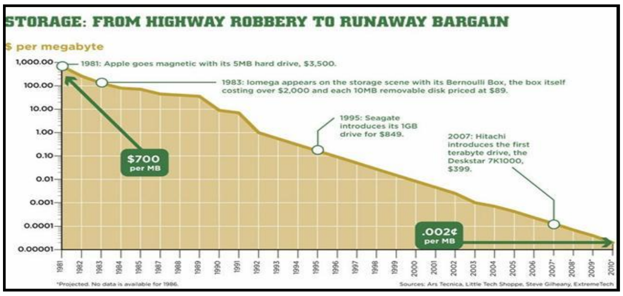
○ **Firewalls** can provide some protection from online intrusion.

○ **Honey pots** are computers that are either intentionally or unintentionally left vulnerable to attack by crackers. They can be used to catch crackers or fix vulnerabilities.

○ **Intrusion-detection systems** can scan a network for people that are on the network but who should not be there or are doing things that they should not be doing, for example trying a lot of passwords to gain access to the network.

V. DATA LOSS

Data loss is an error condition in information systems in which information is destroyed by failures or neglect in storage, transmission, or processing may be permanent .



Data loss, distinguished from *data unavailability*, which may arise from a network outage, which may be temporary.

Data loss can also be data spill. Data spills are possible without the data being lost in the originating side. Data spill incidents, such as in the case of media containing sensitive information being lost and subsequently acquired by another party.

However, Information systems implement **backup** and **disaster recovery equipment** and **processes** to prevent data loss or restore lost data.

Types of data loss:

• ***Intentional Action***

○ Intentional deletion of a file or program

• ***Unintentional Action***

○ Accidental deletion of a file or program

○ Misplacement of CDs or Memory sticks

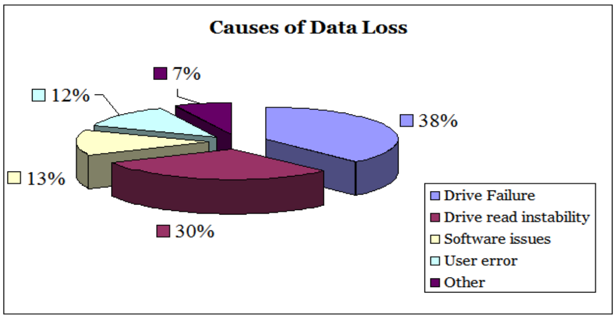
○ Administration errors

○ Inability to read unknown file format

• ***Failure***

○ Power failure, resulting in data in volatile memory not being saved to permanent memory.

○ Hardware failure, such as a head crash in a hard disk.
○ A software crash or freeze, resulting in data not being saved.
○ Software bugs or poor usability, such as not confirming a file delete command.
○ Business failure (vendor bankruptcy), where data is stored with a software vendor using Software-as-a-service and SaaS data escrow has not been provisioned.
○ Data corruption, such as file system corruption or database corruption.



- ***Disaster***

○ Natural disaster earthquake, flood, tornado etc.
○ Fire

- ***Crime***

○ Theft, hacking, sabotage, etc.
○ A malicious act, such as a worm, virus, hacker or theft of physical media.

Studies show hardware failure like drive failures or instability in reading it and human user errors are the two most common causes of data loss, roughly three quarters of all incidents. Another cause of data loss is a natural disaster.

The only way to prepare for such an event is to store backup data in a separate physical location.

VI. COST OF DATA LOSS

The cost of a *data loss event* is directly related to the value of the data and the length of time that it is needed, but unavailable. Consider:

○ The cost of continuing without the data
○ The cost of recreating the data

The cost of notifying users in the event of a compromise

VII. ORGANIZATIONAL RESPONSIBILITY

Recent statistics show the number of publicized data loss events involving sensitive data is on the rise, in part due to recent legislationofrequirements of notification of data loss. Legislationshave forced organizations to notify victims that their identity has potentially been compromised.

VIII. PREVENTION

The frequency of data loss and the impact can be greatly mitigated by taking proper precautions. The different types of data loss demand different types of precautions such as:

○ Multiple power circuits with battery backup and a generator only protect against power failures.
○ Using a journaling file system and RAID storage only protect against certain types of software and hardware failure.
○ Regular data backups are an important asset to have when trying to recover after a data loss event, but they do not prevent user errors or system failures.
○ A well rounded approach to data protection has the best chance of avoiding data loss events. Such an approach includes such tasks as :

- Maintaining antivirus protection and network firewalls
- Also, applying all published security fixes and system patches.

○ User education is probably the most important, and most difficult, aspect of preventing data loss. Nothing else will prevent users from making mistakes that jeopardize data security.

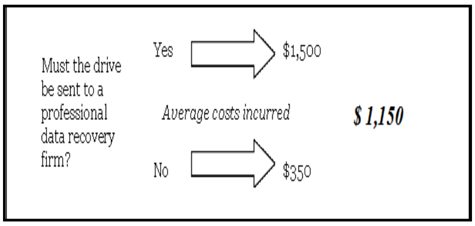
IX. DATA RECOVERY

Data recovery is often performed by specialized commercial services that have developed often proprietary methods to recover data from physically damaged media. Service costs at data recovery labs are usually dependent on type of damage and type of storage medium, as well as the required security or clean room procedures.

File system corruption can frequently be repaired by the user or the system administrator. For example, a deleted file is typically not immediately overwritten on disk, but more often simply has its entry deleted from the file system index. In such a case, the deletion can be easily reversed.

Successful recovery from data loss generally requires:

- Implementation of an effective backup strategy. Without an implemented backup strategy, recovery requires reinstallation of programs and regeneration of data. Even with an effective backup strategy, restoring a system to the precise state it was in prior to the *Data Loss Event*is extremely difficult.


Must the drive be sent to a professional data recovery firm?
Yes
$1,500
Average costs incurred
$ 1,150
No
$350

- Some level of compromise between granularity of recoverability and cost is necessary. Furthermore, a *Data Loss Event* may not be immediately apparent.
- An effective backup strategy must also consider the cost of maintaining and the ability to recover lost data for long periods of time.
- A highly effective backup system would have duplicate copies of every file and program that were immediately accessible whenever aData Loss Event was noticed.
- However, in most situations, there is an inverse correlation between the value of a unit of data and the length of time it takes to notice the loss of that data.
- Taking this into consideration, many backup strategies decrease the granularity of restorability as the time

increases since the potential Data Loss Event.

• By this logic, recovery from recent Data Loss Events is easier and more complete than recovery from Data Loss Events that happened further in the past.

• Recovery is also related to the type of Data Loss Event. Recovering a single lost file is substantially different from recovering an entire system that was destroyed in a disaster.

An effective backup regimen has some proportionality between the magnitude of Data Lossand the magnitude of effort required to recover. For example, it should be far easier to restore the single lost file than to recover the entire system.

X. INITIAL STEPS UPON DATA LOSS

If a data loss occurs, there are steps to take to increase the chances of a successful recovery.

- First, avoid all write operations to the affected storage device. Avoiding write operations includes not starting the system connected to the affected device. Many operating systems create temporary files or files required for booting, and these files may occupy or overwrite the area of lost data, rendering it partially or completely unrecoverable.
- Other writes operations such as copying, deleting, or altering the files should also be avoided, as well.
- Upon realizing data loss has occurred, it is often best to shut down the computer and remove the drive in question from the unit. Re-attach this drive to a secondary computer with a write blocker device, and attempt to recover lost data.
- Hardware theft is the theft of either your computer or your computers connected devices.
- Software theft is the illegal use or distribution of your software. These are serious threats to your privacy because thieves can get personal information from your computer or devices and software theft can be damaging to your software product and your ability to use it.

There are a lot of ways to protect your hardware and software from theft. To protect your hardware you can:

- use like physical means such as locking doors and windows, locking the devices to the surface that they are on, or installing alarms to alert you if someone tries to steal them.
- also use security devices such as passwords, possessed items, and biometrics to protect your information on the computer by preventing the thief from accessing it.
- always back up your files in a separate place in case the computer with your information is stolen.
- lastly make sure you never leave any portable computers, such as a laptop, tablet computer, or mobile phone, anywhere that someone can take them.
- To Protect against software theft there are a few things that you can do.
- Periodicalback up of any files or disks in case they are stolen.
- Prevent software theft is keep all of the originals in safe location.

XI. SECURITY STRATEGIES

The security methodology described in this document is designed to help security professionals develop a strategy to protect the*availability, integrity, and confidentiality* of data in an organization's information technology (IT) system. It will be of interest to information resource managers, computer security officials, and administrators, and of particular value to those trying to establish computer security policies.

The methodology offers a systematic approach to this important task and, as a final precaution, also involves establishing contingency plans in case of a disaster.

Data in an IT system is at risk from various sources—user errors and malicious and non-malicious attacks. Accidents can occur and attackers can gain access to the system and disrupt services, render systems useless, or alter, delete, or steal information.

An IT system may need protection for one or more of the following aspects of data:

• *Confidentiality*. The system contains information that requires protection from unauthorized disclosure. Examples: Timed dissemination information (for example, crop report information), personal information, and proprietary business information.

• *Integrity*. The system contains information that must be protected from unauthorized, unanticipated, or unintentional modification. Examples: Census information, economic indicators, or financial transactions systems.

• *Availability*. The system contains information or provides services that must be available on a timely basis to meet mission requirements or to avoid substantial losses. Examples: Systems critical to safety, life support, and hurricane forecasting.

Security administrators need to decide how much time, money, and effort needs to be spent in order to develop the appropriate security policies and controls.

Each organization should analyze its specific needs and determine its resource and scheduling requirements and constraints. Computer systems, environments, and organizational policies are different, making each computer security services and strategy unique.

However, the principles of good security remain the same, and this document focuses on those principles.

Although a security strategy can save the organization valuable time and provide important reminders of what needs to be done, security is not a one-time activity. It is an integral part of the system lifecycle.

The activities described in this document generally require either periodic updating or appropriate revision. These changes are made when configurations and other conditions and circumstances change significantly or when organizational regulations and policies require changes.

This is an iterative process. It is never finished and should be revised and tested periodically.

DOI 10.17148/IJARCCE.2016.5101

XII. OVERVIEW OF HOW TO COMPILE A SECURITY STRATEGY

Establishing an effective set of security policies and controls requires using a strategy to determine the vulnerabilities that exist in our computer systems and in the current security policies and controls that guard them. The current status of computer security policies can be determined by reviewing the list of documentation that follows. The review should take notice of areas where policies are lacking as well as examine documents that exist:

1. Physical computer security policies such as physical access controls.
2. Network security policies (for example, e-mail and Internet policies).
3. Data security policies (access control and integrity controls).
4. Contingency and disaster recovery plans and tests.
5. Computer security awareness and training.
6. Computer security management and coordination policies.

Other documents that contain sensitive information such as:

1. Computer BIOS passwords.
2. Router configuration passwords.
3. Access control documents.
4. Other device management passwords.

XIII. TESTING

The last element of a security strategy, testing and reviewing the test outcomes, is carried out after the reactive and proactive strategies have been put into place. Performing simulation attacks on a test or lab system makes it possible to assess where the various vulnerabilities exist and adjust security policies and controls accordingly.

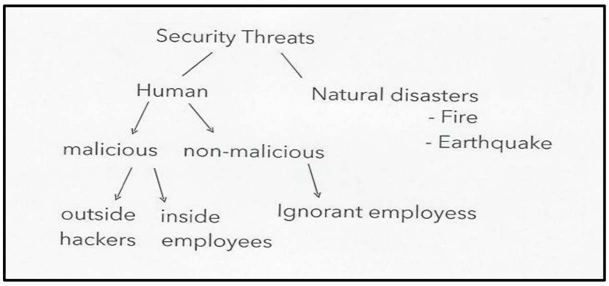
These tests should not be performed on a live production system because the outcome could be disastrous. Yet, the absence of labs and test computers due to budget restrictions might preclude simulating attacks. In order to secure the necessary funds for testing, it is important to make management aware of the risks and consequences of an attack as well as the security measures that can be taken to protect the system, including testing procedures. If possible, all attack scenarios should be physically tested and documented to determine the best possible security policies and controls to be implemented.

Certain attacks, such as natural disasters such as floods and lightning cannot be tested, although a simulation will help. For example, simulate a fire in the server room that has resulted in all the servers being damaged and lost. This scenario can be useful for testing the responsiveness of administrators and security personnel, and for ascertaining how long it will take to get the organization functional again.

Testing and adjusting security policies and controls based on the test results is an iterative process. It is never finished and should be evaluated and revised periodically so that improvements can be implemented.

➲Diagram 1: Threats to systems

Threats such as ignorant or careless employees and natural disasters do not involve motives or goals; therefore no predetermined methods, tools, or techniques are used to launch an attack. Almost all of these attacks or security infiltrations are internally generated; rarely will they be initiated by someone outside of the organization.



For these types of threats, security personnel need to implement separate proactive and reactive strategies, following the guidelines in Flowchart 1.

<u>For Each Type of Method of Attack:</u>

In order to launch an attack, a malicious attacker needs a method, tool or technique to exploit various vulnerabilities in systems, security policies, and controls. A malicious attacker can use different methods to launch the same attack. Therefore, the defense strategy must be customized for each type of method used in each type of threat. Again, it is important that security professionals keep current on the various methods, tools, and techniques used by attackers. A detailed discussion of these can be found in "Security Threats." Following is a short list of these techniques:

- Denial of service attacks
- Intrusion attacks
- Social engineering
- Viruses
- Worms
- Trojan horses
- Packet modification
- Packet replay
- Password cracking
- E-mail cracking

Physical Security:

- Are there locks and entry procedures to gain access to servers?
- Is there sufficient air conditioning and are air filters being cleaned out regularly? Are air conditioning ducts safeguarded against break-ins?
- Are there uninterruptible power supplies and generators and are they being checked through maintenance procedures?
- Is there fire suppression and pumping equipment, and proper maintenance procedures for the equipment?
- Is there protection against hardware and software theft? Are software packages and licenses and backups kept in safes?
- Are there procedures for storing data, backups, and licensed software off-site and onsite?

DOI 10.17148/IJARCCE.2016.5101

Data Security:

- What access controls, integrity controls, and backup procedures are in place to limit attacks?
- Are there privacy policies and procedures that users must comply to?
- What data access controls (authorization, authentication, and implementation) are there?
- What user responsibilities exist for management of data and applications?
- Have direct access storage device management techniques been defined? What is their impact on user file integrity?
- Are there procedures for handling sensitive data?

Network Security:

- What kinds of access controls (Internet, wide area network connections, etc.) are in place?
- Are there authentication procedures? What authentication protocols are used for local area networks, wide area networks and dialup servers? Who has the responsibility for security administration?
- What type of network media, for example, cables, switches, and routers, are used? What type of security do they have?
- Is security implemented on file and print servers?
- Does your organization make use of encryption and cryptography for use over the Internet, Virtual Private Networks (VPNs), e-mail systems, and remote access?
- Does the organization conform to networking standards?

XIV. MINIMIZE VULNERABILITIES AND WEAKNESSES EXPLOITED BY A POSSIBLE ATTACK

Minimizing the security system's vulnerabilities and weaknesses that were determined in the previous assessment is the first step in developing effective security policies and controls. This is the payoff of the proactive strategy. By minimizing vulnerabilities, security personnel can minimize both the likelihood of an attack, and its effectiveness, if one does occur. Be careful not to implement too stringent controls because the availability of information could then become a problem. There must be a careful balance between security controls and access to information. Information should be as freely available as possible to authorized users.

XV. CONCLUSION

Computer security is a vital side that protect your system from damage to the hardware, to prevent theft of or damage to the information and to prevent disruption of service. Losing it is simply not an option. Unfortunately, computer fail, and often. Having a backup plan set before anything goes wrong is one of the most important tasks you will undertake as a responsible computer user.

REFERENCES

[1] Gartner Says Worldwide Security Market to Grow 8.7 Percent in 2013. Gartner, Inc, June 11, 2013
[2] Arcos Sergio. "Social Engineering".
[3] J. C. Willemssen, "FAA Computer Security". GAO/T-AIMD-00-330. Presented at Committee on Science, House of Representatives, 2000.
[4] P. G. Neumann, "Computer Security in Aviation," presented at International Conference on Aviation Safety and Security in the 21st Century, White House Commission on Safety and Security, 1997.
[5] J. Zellan, Aviation Security. Hauppauge, NY: Nova Science, 2003, pp. 65–70.
[6] Cashell, B., Jackson, W. D., Jickling, M., &Webel, B. (2004). The Economic Impact of Cyber-Attacks. Congressional Research Service, Government and Finance Division. Washington DC: The Library of Congress.
[7] Krebs, B. (2009, March). Massive Profits Fueling Rogue Antivirus Market. Retrieved 4 10, 2011, from Security Fix - Washington Post:http://voices.washingtonpost.com/securityfix/2009/03/obscene_profits_fuel_rogue_ant.html
[8] Symantec. (2010). State of Enterprise Security 2010.
[9] Richardson, R. (2010). 2009 CSI Computer Crime & Security Survey. Computer Security Institute. Computer Security Institute.
[10] "Firms lose more to electronic than physical theft". Reuters.
[11] Definitions: IT Security Architecture. SecurityArchitecture.org, Jan, 2006
[12] *The Hacker in Your Hardware: The Next Security Threat*August 4, 2010 Scientific American
[13] Waksman, Adam; Sethumadhavan, Simha (2010), "Tamper Evident Microprocessors", *Proceedings of the IEEE Symposium on Security and Privacy* (Oakland, California)
[14] "Sentinel HASP HL". E-Spin. Retrieved 2014-03-20.
[15] "Token-based authentication". SafeNet.com. Retrieved 2014-03-20.

BIOGRAPHY

Special instructor **Yaqoub Alkandary-** head of basic study department at Higher telecommunication & navigation, Kuwait, University of Tampa Florida, Coventry University, London in Computer- Kuwait.