SMACS (Social, Mobile, Analytics, Cloud and Security) Technologies for Business

Block

5

SECURITY TECHNOLOGIES FOR BUSINESS

Editorial Team

Prof. R. Prasad
IFHE (Deemed-to-be-University), Hyderabad

Dr. Sindhuja
IFHE (Deemed-to-be-University), Hyderabad

Dr. Sanjay Fuloria
IFHE (Deemed-to-be-University), Hyderabad

Dr. Nasina Jigeesh
IFHE (Deemed-to-be-University), Hyderabad

Content Development Team

Dr. Y. V. Subrahmanyam
IFHE (Deemed-to-be-University), Hyderabad

Prof. G. S. B. Subramanya Choudary
IFHE(Deemed-to-be-University), Hyderabad

Prof. V. Srinivasa Murthy
IFHE (Deemed-to-be-University), Hyderabad

Prof. Venkata Dharma Kumar
IFHE(Deemed-to-be-University), Hyderabad

Prof. R. Muthukumar
IFHE(Deemed-to-be-University), Hyderabad

Proofreading, Language Editing and Layout Team

Ms. M. Manorama
IFHE (Deemed-to-be-University), Hyderabad

Mr. K. Venkateswarlu
IFHE(Deemed-to-be-University), Hyderabad

Ms. C. Sridevi
IFHE (Deemed-to-be-University), Hyderabad

Ref. No. SMACS-IFHE – 092022B5

For any clarification regarding this book, the students may please write to The ICFAI Foundation for Higher Education (IFHE), Hyderabad specifying the unit and page number.

While every possible care has been taken in type-setting and printing this book, The ICFAI Foundation for Higher Education (IFHE), Hyderabad welcomes suggestions from students for improvement in future editions.

Our E-mail id: cwfeedback@icfaiuniversity.in

Centre for Distance and Online Education (CDOE)
The ICFAI Foundation for Higher Education
(Deemed-to-be-University Under Section 3 of UGC Act, 1956)
Donthanapally, Shankarapalli Road, Hyderabad- 501203

BLOCK 5: SECURITY TECHNOLOGIES FOR BUSINESS

Security Technologies for Business is a very important block as today the major focus is centered around this work area. The need and process of data security in business organizations, the required network security followed by information security in the cloud environment are discussed in this block.

Current business activities depend largely on the computer networks. Thus the business executive needs to be exposed to data, information and network security.

There are three units in this block.

Unit 16: All the business transactions generate voluminous data and thus learner needs to be exposed to various existing data security technologies. *Data Security in Organizations* is an essential unit which explains the various security build methodologies. It covers the possible threats, risks for not addressing data security, privacy and security procedures, encryption methodologies, anti-virus procedures, server and router security, standards and physical security procedures.

Unit 17: The present day organizational activities are centered around social media marketing, digital marketing, ecommerce, digital payments, intranets, internet etc. Thus the learner needs to be exposed to necessary security mechanism to protect the network environment within the organization. *Network Security in Organizations* details on the network resources in an organization. It details possible security threats, internet attack methods, technology supportive of internet security, wireless network security, network security testing and the future of network security.

Unit 18: As data is received and processed, lot of information files like Management Information System, Executive Information System are in operation on cloud for the organizations. Thus learner needs to get complete awareness of securing the information system on clouds. *Information Security in Cloud Environment* narrates about governance framework, architecting information security plan, implementing planned programs, monitoring and measuring, improving information security and closes with steps involved in building information security in clouds.

Unit 16

Data Security in Organizations

Structure

"*It's like we are building cars that go 500 miles per hour but only building brakes that can cope with 30 mph.*"

- Malcolm Marshall, Global Head of Cyber Security Practice at KPMG International

16.1 Introduction

Technology wise we have entered fourth revolution (AI and Robotics) but security wise, we have not enough for third revolution.

In the previous unit, various aspects of cloud for social marketing like, opportunities and risks, Web 2.0, social media marketing, email campaigns, and segmentation for social marketing were discussed.

Information and information systems are recognized as key assets for an organization of any size. The information technology assets (which have value) provide a competitive advantage to organizations in this rapidly changing, competitive marketplace. Most modern organizations are heavily dependent on information systems to run their operations. There is a very thin line between information systems and business systems. As such, securing such assets has been

recognized as very critical for sustaining and growing business operations. The adoption of "SMACS (Social, Mobile, Analytics, Cloud and Security) Technologies" by organizations in a big way has thrown up new security challenges for organizations.

This unit looks at the meaning of data security, various kinds of security threats and the risk mitigation strategies to be implemented by organizations. It starts with technical threats and then goes on to look at issues related to data privacy and protection of employee and customer data. Anti-virus procedures are followed by different techniques. Encrypting and decrypting sensitive data is another security protection measure. The issues related to security of servers and routers are looked at, followed by procedures for physical security for information processing facilities. Overall security procedures needed to be followed by any organization are described in detail for understanding and appreciation by the student.

Data security is a set of technologies and standards that shield data from accidental or intentional modification, destruction, or disclosure. Data security can be imposed using a range of technologies and techniques, including physical security, administrative controls, logical controls, organizational standards, and other protection techniques that limit access to illegal or malicious processes or users.

The main elements of data security are confidentiality (ensures that the data is accessed only by authorized users), integrity (ensures the data is reliable and accurate), and availability (ensures that the data is available and accessible to authorized users to satisfy business needs). This is a security guide for organizations to keep their sensitive data protected from data exfiltration and unauthorized access.

16.2 Objectives

After studying this unit, you should be able to:

- Explain the technical data security threats to information systems
- Define data security risks for Small and Medium size Businesses (SMBs)
- Discuss the data privacy and security procedures
- Define the overview of encryption methodology
- Explain anti-virus procedures, server and router security procedures
- Discuss data security standards and encryption

16.3 Technical Data Security Threats to Information Systems

In information security, a threat is something which will exploit the vulnerability (weakness) in the system and cause damage. For example, if anti-virus software is not up-to-date, any virus can exploit and cause damage to the documents and data, and that is vulnerability.

The following are major technical data security threats to information systems:

- Information systems are exposed to the threat of malicious code in the form of computer viruses, worms, Trojan horses and logic bombs.
- Threat from mobile code is another major security issue which information systems are vulnerable to. Mobile code is a code (program) which transfers from one computer system to another and executes with little or no user interaction. These mobile codes along with malicious code can create havoc. Even if a malicious code is not involved, the unmanaged mobile code uses system resources in an unauthorized way and may cause disruption.
- If networks are not properly secured, information in the networks can be stolen, modified or manipulated.
- If the media is not properly disposed of, there can be theft of information.
- If patches are not regularly applied to operating systems, there is a threat of unauthorized access and probable damage.

Malware

Software which is specifically designed to disrupt, damage, or gain authorized access to an otherwise unauthorized computer system. Thus it is a major technical threat for computer users.

Explanation of major malware activities are as follows:

- **Virus:** A computer virus is a malware program which on execution, replicates itself in the programs' data files or hard disks. Viruses perform some kind of harmful activity on infected hosts, such as stealing disk space or processor time. That may lead to corruption of data or code and may lead to malfunction or disruption.
- **Trojan Horse:** Unlike viruses, Trojan Horse is not self-replicating. But, it carries a malware program which will do the damage in the form of data loss or system disruption.
- **Worms:** A self-replicating computer program that spreads malicious codes, computer worms make use of the network to send copies of the original codes to other PCs or it can be propagated through copying files from pen drive. It can also go to the extent of affecting transferring documents utilizing the email of the user.
- **Keylogger:** Also known as a keystroke logger, Keyloggers can track the real-time activities of a user on his computer. It runs as a background process and

records all keystrokes made by a user and sends the information collected to the hacker with the aim to steal banking details and passwords.

- **Rootkit:** Rootkit appears as a legitimate file and deceives the user of the computer. So it is considered enormously dangerous of all malwares. This shows warms and viruses as necessary files. Only an antivirus software with the anti-rootkit feature can detect and remove a rootkit.
- **Spyware:** It is a program or software that tracks the user activities on computer and send collected information to interested party. These are usually dropped by viruses, warms or Trojan horses. Once dropped in the computer they install themselves and works silently to avoid detection.
- **Bots:** This is an advanced form of worms and they have automated processes designed to interact over the internet without human interaction. Malicious bots can infect one host and after infecting, it will create connection to the central server or server from remote location which will provide commands to all infected hosts attached to that network called Botnet.
- **Scareware:** It is a malware that make the victims to buy malware software by displaying fake virus alerts on the system. A scareware affected PC may get pop-ups of fake malware threats and to get rid of those, users are impelled to purchase a fake anti-malware software.

Computer malware does not have to be introduced consciously or manually. Basic software packages installed on desktop computers such as Firefox, Internet Explorer, Flash or Adobe Acrobat Reader have their own share of security vulnerabilities. These security weaknesses are enthusiastically exploited by malware writers to robotically infect victims' computers. Such attacks are known as drive-by downloads because the user does not have knowledge of malicious files being downloaded onto his or her computer.

Then another type of attack called "social engineering attacks", which refers to a set of techniques whereby attackers make the most of weaknesses in human nature rather than flaws within the technology. A phishing attack is a type of social engineering attack that is normally opportunistic and targets a subset of society. A phishing email message will typically look very familiar to the end-users – it will make use of genuine logos and other visuals (from a well-known bank, for example) and will, for all intents and purposes, appear to be the genuine thing. When the end-user follows the instructions in the email, he or she is directed to reveal sensitive or private information such as pin codes, passwords, and credit card numbers.

Baiting is another such attack, Baiters may leverage the offer of free movie or music downloads, for example, to trick users into handing their login credentials. Baiting attacks are not restricted to online schemes, either. Attackers can also focus on exploiting human curiosity via the use of physical media. Back in July

2018, for instance, KrebsOnSecurity reported on an attack campaign targeting state and local government agencies in the United States.

Example: Ransomware Attack sends US County Back to 1977

Somerset County, New Jersey, was hit by a ransomware attack that affected business operations by making unavailable essential data.

Services such as land records, vital statistics, and probate records could not be provided to the citizens. Request for title searches could be taken up only on manual records prior to 1977. The attack affected email services for county government departments. The citizens could get in touch with the officials through private email services like Gmail or through a voice call.

Source: https://www.theregister.com/2022/05/29/security_roundup/ Accessed on 02/06/2022

Activity 16.1

Possible Threats and Vulnerabilities

a. Identify the possible threats and vulnerabilities of various kinds, especially in view of usage of mobile devices and BYOD (Bring Your Own Devices) policies adopted by organizations.

b. List out instances where organizations paid a heavy price for not implementing the necessary security controls.

Answer:

Check Your Progress - 1

1. How are information and information systems classified for an organization?
   a. Key assets
   b. Major tools
   c. Depreciable assets
   d. Changing technology
   e. Costly assets

2. Which of the following replicates itself and causes damage?
    a. Virus
    b. Trojan horse
    c. Logic bomb
    d. Computer bacteria
    e. Computer pathogens
3. Which of the following malware programs carries malicious code?
    a. Virus
    b. Trojan horse
    c. Logic bomb
    d. Vector
    e. Spider

16.4 Data Security Risks for SMBs

Some of the major data security risks SMBs (Small and Medium size Businesses) should be aware of and need to put their security controls to mitigate the risks, are:

- Attack by malware like virus, Trojan horse, etc.
- Improper disposal of media, enabling others to get access to the private data
- Vulnerability due to non-application of latest patches to operating systems, especially mobile operating systems
- Allowing staff to use their own devices like pen-drives that expose to new kind of risks for getting the virus along with it
- Allowing unauthorized access to systems and networks due to improper access rights and privileges and not using strong passwords that can be easily breached
- Not enforcing separation of duties, thereby providing unwanted access to the data and information to more than one person
- Not having a proper background check of employees
- Not having a policy on deactivating user accounts on employee resignation or retirement
- Not having enough or proper security controls for the office spaces and equipment
- Not having a proper mechanism to ensure availability of supporting utilities like power, network services, etc.

- No proper data recovery plan to withstand the natural calamities like flood, earthquake, etc.
- Risk due to social unrest that may cause an attack on corporate office and subsequently the partial/complete loss of data
- Untrained staff can be a very big risk since wrong handling of the system may cause a partial/total loss of valuable data
- Risk of cyber-attacks which is one of the prominent causes of loss of data/ information
- Not having a robust backup facility that may create an irreversible loss of data
- Restricting access to the Internet when in office

Example: Illinois Housing Development Authority addresses a Security Breach

Illinois Housing Development authority. The rental payment portal of Illinois Housing Development authority was targeted by a cyber-attack. The organization noticed the breach when some of the tenants could view applications of other tenants. The portal was closed for two days and was restored in 2 days. The investigation showed that it was a coding error which was corrected. The investigation also located which applications were affected. They tested the software after the correction so as to ensure the problem is resolved for all test cases.

0Source: Breach Exchange: Illinois Housing addresses security breach (seclists.org), January 06, 22, Accessed on 14/06/2022

Check Your Progress - 2

4. Which of the following is a risk mitigation option?
    a. Taking backup of important data
    b. Untrained staff
    c. No background check on employees
    d. Floods
    e. Damaged power cables

16.5 Data Privacy and Security Procedures

Data privacy is defined as the proper use of data. When merchants and companies use data or information that is provided or entrusted to them, the data should be used according to the agreed purposes. The Federal Trade Commission enforces penalties against companies that have negated to ensure the privacy of a customer's data. Data security is clearly referred to as the confidentiality, integrity

and availability of data. In other words, it is all of the processes and practices that are in place to ensure data is being accessed or used by authorized parties or individuals. Business organizations are legally obliged to secure data and protect the privacy of their customers' information. Similar legal obligations also exist for employee data. These laws and regulations vary from country to country and organizations are expected to have a thorough understanding before bidding for overseas contracts, else the cost estimates may not be accurate since the extra resources for regulatory compliance will be an unknown quantity and can even wipe out the business enterprise. With the increase and escalation in cybercrime threatening both the private and public sector, it's essential for organizations to have a data security policy in place.

A privacy policy should clearly document how the business organization collects and stores data. It also deals with what is planned to be done with that private data. Attention should also be paid to the controls on sharing this information with third parties, where the legal issues can throw up. There is another dimension to privacy. Unsolicited commercial emails with commercial motive are illegal, so a policy needs to be implemented to take care of permissions to send messages to contacts.

Employee awareness and code of conduct play a critical role. The staff should be told about the policy in every forum and also the code of ethical conduct should also be given wide publicity. The consequences of violations need to be clearly articulated. While signing customer contracts, the legal department should thoroughly understand the conditions for data privacy and advise the management.

Another important aspect is that the organizational structure has to support this; depending on the size of the organization there is a need for full time or part-time (as additional responsibility) data protection officer.

Organizations need to be worried about the loss of business due to customer dissatisfaction on account of privacy issues. When formulating a data security policy, it is important for the organization to look at all threats arise while implementing and to cover more than just the basics (Refer Exhibit 16.1 – how IBM Security Guardium Analyzer, a SaaS offering, helps users efficiently evaluate database security and compliance risk).

Exhibit 16.1: IBM Security Guardium Analyzer

IBM security guardium analyzer, a SaaS offering, helps users efficiently evaluate database security and compliance risk. It can support the organization's risk assessments for GDPR, PCI, HIPAA, CCPA, LGPD and

Contd….

other regulations by helping identify databases most likely to be at risk of failing an audit by using next-generation data classification techniques, risk-scoring, and vulnerability scanning. The risk scoring prioritizes the on-premises and cloud databases containing at-risk personal and sensitive personal data, helping organizations gain insights into where they may need to focus and prioritize their data security and risk remediation efforts.

This software has following features:

- This software-as-a-service offering helps the organization get started immediately with a guided setup process for data discovery and data classification.
- Specifically designed to help identify regulated data risks, this service analyzes on-premises and cloud databases to find and present users with prioritized risk information.
- It has pre-built functionality and dynamic dashboards surface data exposures, providing information such as: number of databases affected, severity breakdown, geographic breakdown
- This service combines the data classification and vulnerability scanning results to provide risk scoring and prioritization information so you can efficiently take focused steps to minimize risk.
- It helps compliance managers, data managers and IT managers get the information they need, at the right level of detail, to collaborate efficiently.

Source: https://www.ibm.com/us-en/marketplace/guardium-analyzer, 4th March, 2021, Accessed on 1/9/2022.

Example: Privacy Issue and Respective Corrective Action at Twitter

Twitter obtained data from users for explicit use of security. The company misused it for commercial advertisements. The company revenues grew but the privacy of around 14 crores users was affected in the process.

The regulators noticed serious lapses in this privacy violation issue. Twitter took corrective actions by appointing of a new data governance structure. A penalty of $ 150 million was imposed. Companies which fail to address privacy issues adequately, will have to pay heavy penalty and also lose customer trust which could affect the fortunes of the company severely.

Source: https://abcnews.go.com/Business/wireStory/twitter-pay-150m-penalty-privacy-users-data-84983063, 25-May-2022, Accessed on 02/06/2022

Check Your Progress - 3

5. Which of the following is true?
   a. Only employee data need to be protected
   b. Only customer data need to be protected
   c. Privacy laws are the same for all countries
   d. Both customer and employee data need to be protected
   e. The information collected can be passed on to third parties for free

16.6 Encryption Methodology

To prevent unauthorized access or interception of data, cryptography techniques are used. Encryption is used in connection with making the messages or data unreadable to unauthorized persons.

The normal data or ordinary readable text is called plaintext. Encryption uses an algorithm to convert plaintext to cipher text. This algorithm is called a cipher. The cipher text can only be deciphered by people who have the decrypting key supplied by the originator of the message. Others cannot decrypt. It may be possible, but it will require a lot of computation and is a hard job. Encryption alone cannot prevent interception, but the interceptors cannot get the contents of the message. There are two types of encryption:

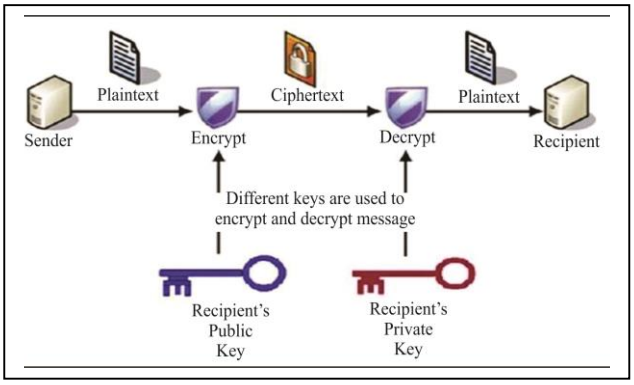
1. Symmetric encryption methods
2. Public key encryption

Symmetric encryption methods have the same key for encryption and decryption. The key is a secret between two parties and that requirement is considered as a drawback. They are also called private key schemes.

In a public key scheme, the key is publicized for encryption and the decrypting key is shared only with the authorized recipient. This is also called *asymmetric encryption* since the encryption and decryption keys are not the same. These schemes require two keys, one public and another private. The public key is used for encryption and private key or secret key for decryption. Public-key cryptography is used as a method of assuring confidentiality, authenticity and non-refutability of electronic communications and data storage.

Both public key and private key are mathematically related. For example, if Varma wants to send a message to Mary, he will use the public key of Mary to encrypt the message and since only Mary has the private key, she only can decrypt the data.

Another scheme using public key encryption is called *Digital signature*. A digital signature is an electronic form of a signature. This can be used to authenticate the identity of the sender of a message or the signer of a document. It also ensures that the original content of the message or document that has been sent is unchanged.



These ensure that the receiver knows the message has been sent by a known sender. These are like manual signatures and properly generated digital signatures are more difficult to forge. The sender cannot deny having sent the message (non-repudiation). Digital signatures are primarily used for software distribution and financial transactions. The sender uses his private key to generate the digital signature. The receiver can use the known public key to decrypt and know that the message has come from a known sender.

We can use some familiar situations to illustrate the public key scheme and the digital signature scheme. Suppose there is a locked mailbox with the address written on it (that is the public key). Anyone can drop mails into the box looking at that address, but only the owner who has the mailbox key (private key) can open and access mails.

The digital signature is like closing an envelope and putting a personal wax seal (private key). But anyone can open the envelope by breaking the seal, but the receiver is sure about the sender and that no tampering happened in the transit.

Example: Paytm Payment Gateway uses the most Advanced 128-Bit AES Encryption to Provide the Best Security for its Customers

Paytm payment gateway has best in class information security features for its merchants, both in terms of data security and smooth transaction flow. The company obtained RBI-recognized PCI DSS level 1 certificate. This provides maximum security for customer data. The company uses the 128-bit AES encryption. The payment gateway converts the 16- digit debit/credit card number into a unique identifier which is very difficult to decipher and thus safeguards sensitive user data. In India, 76% of users are worried about online fraud and steps taken by Paytm gateway addresses this concern.

Source: https://www.businessinsider.in/business/news/71-of-consumers-concerned-about-online-fraud-here-is-how-paytm-payment-gateways-security-features-are-helping-businesses-build-trust-/articleshow/91792691.cms, 26-May-2022, Accessed on 14/06/2022

Check Your Progress - 4

6. Where can encryption be used?
    a. To prevent interception
    b. To ensure contents cannot be read
    c. To converts cipher text to plain text
    d. only in defense
    e. Cannot be used as standards do not exist for encryption
7. A public key is used for
    a. Encryption
    b. Decryption
    c. Withdrawal
    d. Authentication
    e. Storage
8. Private key is used for
    a. Encryption
    b. Decryption
    c. Deposits
    d. Authentication
    e. Storage

16.7 Anti-Virus Procedures

Anti-virus procedures must be implemented to make safe ambience for data security against data theft, virus attack, unauthorized intrusion, etc. Creating a safe environment for data security is a cost-effective method since re-creation cost of data is considerably high and loss recovery may be impossible in most of the cases.

Following are the anti-virus promotion and use procedures:

- All systems in the organizations need to be loaded with anti-virus software and there should be mechanisms to continuously update the anti-virus software to protect against new viruses generated.
- Employee awareness training should clearly indicate the protective measures to be taken in the organization against risks in dealing with getting data and software from external networks.
- The policy clearly states that any new computer/storage device should be checked for viruses before making them part of the network.

- Mail attachments must be checked for viruses before use. These checks can be at the server level or desktop level or where networks interface with external networks.
- Web pages must be checked for malicious code.
- Despite all the care taken, virus attacks still occur. The procedure should be clear about what needs to be done. Practices like isolating the affected system from network need to be a part of the procedure. If the data is corrupted, the procedure for recovery from the backup has to be revoked.
- The organization should regularly collect information on new viruses from reputed journals and websites. It can even subscribe to mailing lists.
- The organization may plan for automatic updates of anti-virus software on desktops.
- Care has to be taken during emergency or maintenance procedures (when anti-virus controls may not be in place) to protect against malicious code.

The anti-virus software detects viruses based on signatures. Some software use heuristics based approach (problem-solving by trial and error) for detection. As far as containment is concerned, the anti-virus software quarantines the affected part or deletes the part based on user feedback. The user can also take containment measures like disconnecting the affected device/machine, etc.

An anti-virus server may be configured to push latest updates to all systems and devices in the network. Also, the end users should not be allowed to make changes to the settings for the anti-virus client program on the desktops; only system administrators can do those changes. This ensures that the desktop is not exposed to virus attacks intentionally or by mistake. Periodic review of logs containing virus attacks will provide an insight into the nature of threats for better preparation for security in the organization.

Check Your Progress - 5

9. At what level are mail attachments are checked for viruses?
   a. Server level only
   b. Desktop level only
   c. At network interfaces only
   d. Server, Desktop and Network Interface levels
   e. At the vendor server level

16.8 Server and Router Security Procedures

Server security is one of the mandatory terms to be followed in all relations of data transactions. Since the server is the common transaction element between

multiple computer systems, it needs a secure environment to keep data and applications intact and in safe custody.

Similarly, the router's security is equally important. Wherever the routing element is installed, the danger of password stealing, redefining routing, eavesdropping, etc. are present.

Some of the key issues which form part of the server and the router security procedure are:

- *Change management*: All changes need to be controlled. Someone has to propose and the change control board needs to evaluate the impact of the suggested changes to the system/router configurations and either approve or reject. This will ensure that the changes done with malafide intentions are not allowed by mistake.
- The procedure should take changes on a testing system before taking them on to the production system. The changes need to be communicated to all concerned parties.
- Segregation of duties is another important aspect of the procedure. The person initiating the request cannot be the one who authorizes. It may not be feasible for small organizations to ensure separation of duties, but in those cases, rigorous audits, management reviews and other monitoring controls should be in place.
- Similarly, the organization may go in for separation of development, testing and operational systems. These test systems should simulate the operational systems as close as possible. It is a good practice not to load sensitive data for testing purposes. Developers and testers, having access to the operating system, may lead to intentional or unintentional damage or they may compromise security.
- Capacity management is another important consideration for server/storage and network bandwidth. The system performance cannot be allowed to degrade because of full capacity utilization. Then the availability issue of security will come into play. Future requirements need to be planned and capacity needs to be enhanced when a threshold (say 75%) is reached; especially, better planning is required for equipment with long lead times or high costs.
- Anti-malware software is to be installed on servers.
- Controls must be in place for controlled execution of mobile code on servers.
- Security incidents do happen even with all precautions taken. So a backup of data and software is mandatory. Similarly, the recovery procedures must be in place.

- Logging data on servers and routers should be mandatory; and so is the periodic review of the log.
- Clock synchronization procedures should be in place. This will ensure all logs are time-stamped with actual time which will be of great help in investigations when security incidents happen.
- Access control policies and procedures dealing with user privileges, user access and user password management are the key factors for ensuring right access to the right people and systems.
- Access control procedures for access by remote users need to be in place.
- Routing controls should be based on positive source and destination checking mechanisms for addresses.
- All routers in the organization need to have encrypted passwords.
- Access rules are added as and when the business rules are added with approval from the information security officer.
- For the selected ports on the router, access should be restricted.
- Block malicious packets coming to the router.
- Restrictions to be imposed on SNMP (Simple Network Management Protocol). Even though SNMP is very convenient for the network administrator to get some routine information, it is a good source of exploitation by mollified attackers. Hence, the need for restrictions.
- All unused services on routers are to be disabled.
- IP source routing needs to be disabled.
- IP directed broadcasts need to be disabled to avoid Denial of Service (DoS) attacks.

Example: California Health Network Reports Data Breach Due to Vulnerability in the Network

Non-profit Community Medical Centres (CMC), is based in Stockton. The chain caters to poor patients, migrants, and the homeless in the Northern California. Secured health records of 656,047 patients were compromised in a security incident. Some unusual network activity was noticed by the company and the network was closed instantly. The incident was investigated with the help of a cyber security expert agency. Digital evidence found that hackers had got access to the network. The hackers exploited some vulnerabilities in the network configuration. The company took steps to improve network security.

Source: https://www.infosecurity-magazine.com/news/california-health-network-reports/, 01-November-2021, Accessed on 03/06/2022

Activity 16.2

Server and Router Security

a) Server Security

Cisco IT uses many different techniques to protect its network from distributed denial-of-service (DDoS) attacks. When attacks originate from a broad range of spoofed addresses and target mission-critical servers, which server security procedures does Cisco need to implement?

b) Router Security

Snapdeal is setting up a new operations center in Mumbai. It is procuring and installing IT and network infrastructure. As part of its network infrastructure, it decided to procure a sophisticated router and respective software. As an IT expert, advise Snapdeal on what parameters are critical when assessing the capability of router security solutions in a given tool/software solution?

Answer (a):

Answer (a):

16.9 Data Security Standards and Encryption

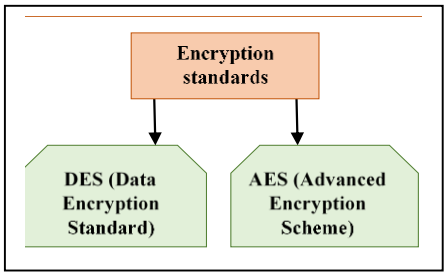
The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information standard for organizations that deal with branded credit cards like Visa, Master Card, etc. The standard was created to have control on cardholder's data and this avoids or prevents card related frauds.

The 12 requirements of PCI DSS are as follows:

- Install a firewall configuration for cardholders data
- Do not use vendor-supplied default passwords

- Protect the cardholder data
- Encrypt transmission of cardholder data across open, public networks
- Use and regularly update anti-virus software on all systems
- Develop and maintain secure applications
- Allow access to cardholder data only on the need-to-know basis
- Assign a unique ID to each person with access to systems
- Restrict physical access to cardholder data
- Track and monitor access to network resources and cardholder data
- Regular testing of security systems and processes
- A comprehensive information security policy needs to be in place to cover all aspects
- A new set of guidelines is added to deal with wireless security issues.

Encryption standards are of two kinds:



i) ***DES (Data Encryption Standard)***: This is a symmetric encryption standard where the same key is used by both sender and receiver. This is an outdated standard. This standard uses block cipher where encryption is applied on blocks of data and not on individual bits. Normally 64-bit blocks are used. This is subject to brute force attack since the encryption can be deciphered by brute force trials.

ii) ***AES (Advanced Encryption Scheme):*** This is a symmetric encryption algorithm as a replacement for aging DES and to prevent brute force attacks. This standard is implemented in both hardware and software. Rijndael cipher was selected and published as a standard. It is the most popular algorithm used both by the government and private industry. It is stronger in view of longer key lengths. Each cipher encrypts and decrypts data in blocks of 12 bits using cryptographic keys of 128-, 192- and 256-bits. That is the reason why we talk about 128-bit encryption. More confidential information generally uses key lengths of 192 or 256 bits.

Example: Hackers Steal ₹ 7.38 Crores from Razorpay by Exploiting Security Vulnerabilities

Razorpay conducted an internal investigation and found out 831 transactions against 16 merchants of Razorpay were found to be unauthorized. An amount of ₹ 7,38,36,192 was siphoned by hackers.

Contd….

The authorisation process was manipulated to authenticate some hundreds of failed transactions. Fiserv, a fintech and payments company indicated to Razorpay that these transactions had failed and were not authorised or authenticated. As a result, false 'approved' messages were communicated to Razorpay. This happened at merchant premises using an earlier version of software.

Source: https://www.thenewsminute.com/article/hackers-fake-customers-steal-rs-738-crore-razorpay-164213#:~:text=Hackers%20and%20fraudulent% 20customers%20have, by%20the%20payment%20gateway%20company, 21-May-2022, Accessed on 03/06/2022

Activity 16.3

Data Encryption

- Research for the brute force attacks related to DES encryption implementations.
- Research for credit card frauds and give reasons for them.
- Research for criticism against PCI DSS (Payment Card Industry Data Security Standard).

Answer:

Check Your Progress - 6

10. What is PCI DSS?
    a. Proprietary standard
    b. Standard used by all card companies
    c. Standard where user ids can be shared
    d. Standard where there is no specific mention of anti-virus software
    e. Standard where security policy is not insisted on

16.10 Physical Security Procedures for Computing Resources

The physical security procedures are the methods of keeping physically safe and inaccessible valuable computing resources, out of the reach of unauthorized persons. Commonly, the physical security has two objectives, i.e., to keep the computing resources safe and out of the reach of unauthorized persons and to keep it safe from disasters like a natural calamity, etc.

The following physical security procedures are followed as per ISO 27001 standard:

1. Critical or sensitive information processing facilities are to be kept in secure areas which are protected by security guards or access control systems.
2. Bars, alarms and locks may be used as appropriate.
3. Information processing facilities managed by third parties may be isolated from those maintained by the organization directly.
4. The visitor registers with details of name, organization, time of entry, person/ department visited and departure time need to be maintained.
5. Access control systems with smart cards need to be implemented for secure areas where critical servers and other equipment are kept.
6. Identification cards of various colors may be issued to staff/vendors/visitors, etc., and all of them are expected to wear these cards while on the premises.
7. Access rights need to be reviewed regularly and revoked if the need is not there anymore.
8. Physical protection against fire, flood, earthquake, civil unrest and other forms of natural and man-made disaster need to be designed.
9. Firefighting equipment should be readily available and staff trained for emergencies.
10. Backup data need to be kept at an off-site location.
11. No hazardous material to be kept near or inside secure areas.
12. No one should be allowed to work in secure areas without supervision. Only authenticated persons should be allowed to work in secure areas. And the authentication should be verified all times.
13. Cameras, camera phones and other devices not to be allowed inside the premises.
14. Areas for loading and unloading of received materials or material being sent out need to be isolated from secure areas.
15. Eating, drinking, etc. not to be allowed in working areas.
16. All supporting utilities like power, water, and air-conditioning should be adequate for the systems they are supporting. All backup arrangements, as may be appropriate, need to be designed and provided for.
17. UPS capacity needs to be reviewed from time to time. Preventive maintenance to be ensured periodically.
18. All cables are to be neatly arranged and checked periodically.
19. All equipment are to be maintained as per supplier recommended service instructions.

20. When equipment is carried outside, extra precautions are to be taken.
21. Adequate comprehensive and transit insurance needs to be taken.
22. When equipment, like disks, needs to be disposed of, it should be ensured that sensitive data is deleted from them.
23. Proper authorization must be insisted upon for moving equipment from one location to other.

There are multiple methods to keep up the physical security of computing resources. However, each method is condition-specific, like we can keep CDs (Compact Discs) safe inside a drawer too, but this cannot be done with UPS (Uninterrupted Power Supply). The decision of physical security implementation, therefore, depends on the article to be secured, the appropriateness of a particular security implementation, etc.

Example: Cerento Selects Teleporte Keyless Access Control to Centralize Access Management

Cerento Inc., is an EPC (Engineering, Procurement and Construction) Company based in Canada. The customers had serious issues access to sites. Loss of access codes, breaking of locks was leading to delays in access to IT infrastructure. The company went for a centralized Teleporte keyless access system to solve these issues. Armoured keyless pads can be taken to new locations easily. With a technical automated solution, the company could spend its time to work on operations. Physical security is one layer which is equally important aspect of any security architecture.

Source: https://www.einnews.com/pr_news/574147839/cerento-selects-teleporte-keyless-access-control-to-centralize-access-management, 01-June-2022, Accessed on 03/06/2022

Activity 16.4

Physical Security Procedures for Computing Resources

Do a little research on the Internet. Find out how "Amazon Web Services (AWS) Identity and Access Management (IAM)" tool provides physical security of data centers in organizations? What parameters need to be checked when buying any given solution for security provision? Also, list some specific procedures adopted by your own organization.

Answer:

16.11 Summary

- Data security in an organization is concerned with protecting data from intentional or accidental threats, and also it should ensure confidentiality, integrity and availability of data to achieve business goals.
- There are various data security threats which can affect the organization's data. Some of them are virus, warm, Trajan horse, rootkit, spyware, bot, etc. Data security can be ensured by implementing various data security techniques and standards.
- All kinds of organizations need to recognize information and information processing facilities as key resources of the organization. Every organization should prepare a security policy and detailed procedures for various aspects. Especially, these become critical with the extensive use of web services and use of mobile devices.
- Physical controls, network related controls and controls at the server level need to be catered. Encryption needs to be used where appropriate. If the organization is involved in the credit card business, the PCI-DSS (Payment Card Industry Data Security Standard) standard needs to be enforced.
- Enough controls for safeguarding customer data and employee data as per law need to be catered. If organizations do not take these seriously, there is a huge loss due to lawsuits and loss of customers. Employee training plays a key role.
- Commitment from top management is another key factor for successful implementation of security procedures. A periodic audit by third-party auditors and rigorous internal reviews are critical factors for success.

16.12 Glossary

Cipher: A simple encryption system where each character is substituted for another.

Cryptovirology Leakware: Cryptovirology studies how to use cryptography to design powerful malicious software. Leakware is a cryptovirology attack invented by Adam L. Young that threatens to publish stolen information from the victim's computer system rather than deny the victim access to it.

Digital Signature: A digital signature is a mathematical way to guarantee that a given message was sent by a specific sender.

Information Processing Facilities: Any information processing system, service or infrastructure.

Information Security: Preservation of confidentiality, integrity and availability of information.

Information Security Incident: Occurrence of system service or network state indicating a breach of security.

Malware: A generic term used to describe any type of software or code specifically designed to exploit a computer or the data it contains, without the owner's consent. Malware includes viruses, Trojan horses, spyware, adware, most rootkits, and other malicious programs.

Public Key Encryption: The encryption breakthrough of the 1970s. With public key encryption, two confidants can communicate securely, even if all of their communications are intercepted, without taking the risk of sending a secret key and having the code broken.

Private Key: A private key is a bit of code that is paired with a public key to set off algorithms for text encryption and decryption. It is created as part of public key cryptography during asymmetric-key encryption and used to decrypt and transform a message to a readable format. Public and private keys are paired for secure communication, such as email.

A cryptographic key that can be obtained and used by anyone to encrypt messages intended for a particular recipient, such that the encrypted messages can be deciphered only by using a second key that is known only to the recipient (known as private key).

Trojan Horse: Malicious programs disguised as legitimate software. They are not self-replicating but can cause damage.

Virus: A computer program file capable of attaching to disks or other files, and replicating itself repeatedly.

Vulnerability: Weakness of an asset or a group of assets that can be exploited by one or more threats.

16.13 Self-Assessment Test

1. Describe the major technical security risks to information or information processing facilities.
2. Describe the procedures for anti-virus implementation in organizations.
3. Describe different encryption techniques. Describe public key, private key and digital signature.
4. What are the physical security controls for information security?
5. What are the things to be taken care of, for server and router security?

16.14 Suggested Readings / Reference Material

1. Rodney Heisterberg and Alakh Verma (April 2022). “Creating Business Agility: How Convergence of Cloud, Social, Mobile, Video and Big Data Enables Competitive Advantage,” Narrated by Stephen Graybill.
2. Jonathan S Walker (2021). Social Media Marketing For Beginners - How To Make Money Online: Guaranteed Strategies To Monetizing, Mastering, & Dominating Any Platform For Your Brand, JW Choices.

3. Barry Connolly (2020). Digital Trust: Social Media Strategies to Increase Trust and Engage Customers, Bloomsbury Business.
4. Seema Gupta (6 August 2020). Digital Marketing McGraw Hill; Second edition.
5. Tracy L. Tuten, Michael R (15 June 2020). Solomon et al, Social Media Marketing, SAGE Publications Pvt. Ltd; Third edition.
6. Paul Martin Thomas Erickson (2019). Social Media: Usage and Impact, Global Vision Publishing House, 2 edition.
7. Steve Randazzo (2019). Brand Experiences: Building Connections in a Digitally Cluttered World, Paipen publishing.

16.15 Answers to Check Your Progress Questions

1. (a) Key assets

Information and information systems are considered as assets on par with other assets for an organization.

2. (a) Virus

Only virus replicates and may create havoc; others do not replicate or they are not valid threats.

3. (b) Trojan horse

Trojan horse carries malicious code and not others.

4. (a) Taking backup of important data

Taking backup of important data is a risk mitigation option whereas others are risks.

5. (d) Both customer and employee data need to be protected

In an organization, both customer and employee data need to be protected.

6. (b) To ensure contents cannot be read

Encryption cannot prevent intrusion but ensures that intercepted data cannot be deciphered.

7. (a) Encryption

In cryptography, the public key is used for encryption, which converts plain text to ciphertext.

8. (b) Decryption

A private key is used for decryption, which converts a ciphertext to plain text.

9. (d) Server, Desktop and Network Interface levels

Mail attachment needs to be checked for viruses at all server, desktop and network interface levels to ensure maximum security.

10. (c) Standard where user Ids can be shared

Users need to be given unique IDs to track the persons in case of incidents.

Unit 17

Network Security in Organizations

Structure

"As we've come to realize, the idea that security starts and ends with the purchase of a pre-packaged firewall is simply misguided."

- Art Wittmann

17.1 Introduction

Network security is a major issue to be addressed by all types of organizations across industries as more and more devices are connected to a network to collect and share data for communication among the various units of an organization.

There is a misconception among some companies that purchasing some hardware and software will take care of the network security concerns. While they are important, it needs to be coupled with processes, awareness among people connected with the organization. Technology, Processes and People form the three legs of any security program.

The previous unit discussed data security covering encryption, data encryption standards, data security risks and physical security procedures. With the advent of technology, the Internet became popular worldwide. Almost all devices like PDA (Personal Digital Assistant), laptops and PC, etc., are interconnected through the Internet. The Internet is a viable tool for everyone to share their data in the most prominent way. But in this run, none shall be unaware of their data security which will be a major concern in network security.

This unit initiates discussion with a brief history of network security. Further, in order to understand the vulnerability and attack methods, different internet attacks have been elaborated in this unit. However, the business applications use different devices like firewalls making intranet withstand the security challenges at the enterprise level. US federations implement the network security testing that utilizes the technique of encryption. Network security deals with components, interfaces, sub-systems and external interfaces (an interface is a device or a system that unrelated entities use to interact, while external interference refers to barriers occurring outside the system.) to the internet. Architecture involves mainly taking technological and cryptographic decisions. Design involves considering different level protocols.

In this unit, types of exposures to different risks on the web, approaches to make good security countermeasures to oppose threats such as cryptography and password protections are explained. Moreover, an overview of the organization security and control areas is also discussed through the network security testing program.

17.2 Objectives

By the end of this unit, you should be able to*:*

- Define different categories of network attacks
- Discuss methods of internet attacks
- Discuss the internet security application approaches
- Define cyber-attacks and countermeasures
- Discuss security risks on web and malware
- Explain wireless security options and network security testing approaches

17.3 History of Network Security

Network security has been a concern since the inception of networked computers. Networks led to new terminology like:

Network: A computer network is a set of computers connected together for the purpose of sharing resources like a printer or a file server. The most common resource shared today is connection to the internet, which itself can be considered a computer network.

Internet: The internet is the global system of interconnected computer networks that use the internet protocol suite (TCP/IP) to link devices worldwide.

Cyberspace: Cyberspace is defined as the interdependent network of information technology infrastructures, and includes the internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.

Web: The Web, or World Wide Web (W3), is basically a system of internet servers that support specially formatted documents. There are several applications called Web browsers that make it easy to access the World Wide Web; popular being Firefox, Chrome and Microsoft's Internet Explorer.

Before the 90s, networks were relatively uncommon and the general public was not made-up of heavy internet users. There were several high profile violations of security during the 90s, including the popularization of the term "hacker" by the movie War Games. But few serious network security methods were taken to limit the damage. The public networks also posted the secure items over the non-secure lines due to lack of security protocols in the underlying architecture.

As the Advanced Research Projects Agency Network (ARPANet) developed by the US Department of Defense (DoD) gave birth to the Internet, small services like email and sharing of data are equated to that of routine post office work. But as the Internet is changing the world, it has also opened doors for hackers. Cyber fraud has emerged as a challenge for the government to secure their confidential data. Government agency responsible for the development of ARPANet has worked with other network users to take care of network security. As a result, birth of first network security organization took place in 1988 in the form of Computer Emergency Response team (CERT). It spreads awareness about network security protocols amongst network users and takes care of security breaches through research.

A new security mechanism called firewall program was designed by a NASA researcher to deal with virus attach. To defend and withstand the attacks on the network, security has to be managed and controlled by ensuring the firewalls, using suitable anti-virus solutions and providing users with login credentials.

Because of increased dependability of world on networks makes it more vulnerable towards different types of network security threats.

To mitigate these threats different solutions in the form of Network Behavioral Analysis (NBA), Web Application Firewalls (WAF), Reputation engines and Denial of services (DoS) protections are provided by various companies.

With the demands of security in ad-hoc networking, dynamic networks are empowering users to access remotely and cost-effectively. And this enables the exchange of data with more security.

Check Your Progress - 1

1. Which of the following entities brought internet?
   a. ARPANET
   b. APRANET
   c. DNS
   d. Internet Service Provider (ISP)
   e. WWW (World Wide Web)

17.4 Different Categories of Network Security Threats

With the explosion of attacks, security becomes a basic concern for every network design. For managing and developing, the user must understand the security policy. Network security consists of the policies and practices adopted to prevent and monitor, unauthorized access, misuse, modification or denial of computer network and network accessible resources. In the past twenty years, it is seen that the easiest way to secure the network is to separate the network from outside like intranet; but this is not convenient and new developments increased significantly with the development of policies for which tools need to be downloaded from internet sources and implemented. But this downloading and wrong implementation might pose severe attacks. That is the reason why users must understand the need to secure and also about the type of attack intended, and only then follow the policy to defend the same.

On deeper understanding, attacks on the network have been categorized into two:

a. *Active Attack* - Those attacks are caused by disrupting the network, for the benefit of the perpetrator. They are carried out by viruses, worms or Trojan horses. Such attacks are accumulated beside a network backbone, develop information in transit, electronically enter an enclave, or attack an authorized remote user during connection which results in the dissemination of data files, DoS or modification of data.

   e.g.: Denial-of-service attack, DNS (Domain Name System) spoofing, Man in the middle, ARP (Address Resolution Protocol) poisoning, Smurf attack, Buffer overflow, Heap overflow, Format string attack, SQL injection, and Cyber-attack.

b. *Passive Attacks* - Such attacks occur when attackers intercept the information but do not affect the network. They are more dangerous as they cannot be detected easily. These attacks occur through traffic analysis, monitoring the unprotected communications, decrypting the weakly encrypted traffic and capturing authentication information which results in the disclosure of information to an attacker without the consent or knowledge of the user, e.g., Wiretapping, Port scanner, Idle Scan.

There are number of techniques to utilize in cyber-attacks and a variety of ways to administer them to individual or establishments on a broader scale. Attacks are broken down into two categories:

- *Syntactic attacks* – These are straightforward attacks includes malicious Software which consists of viruses, worms and Trojan horses.
- *Semantic attacks* – semantic attack modifies and disseminates correct as well as incorrect information. Information modified could have been done without the use of computers even though new opportunities can be found by using them. To set someone into the wrong direction or to cover users tracks, the dissemination of incorrect information can be utilized.

Example: Popular Gaming Service Battle.net was Taken Offline by a Distributed Denial of Service (DDoS) Attack That Took Services Down for Several Hours

Battle.net (a gaming services company) was forced to shut down operations for many hours due to a DDOS attack by hackers.

The attack resulted in disconnections for some play. When the server is bombarded with abnormal requests, this kind of attack occurs. The bandwidth was full and genuine user request for services could not be handled. To initiate a DDoS attack, the hacker takes the help of devices called botnets who send the fake requests and fill the bandwidth.

Source: https://www.techradar.com/news/battlenet-hit-by-huge-ddos-attack, May 12, 2022, Accessed on 03/06/2022

Check Your Progress - 2

2. What can cause passive attacks?
    a. Masquerade
    b. Interception
    c. Modification
    d. Phishing
    e. Encryption

3. What does ARP stand for?
    a. Address Resource Procedure
    b. Address Resource Protection
    c. Address Resolution Protocol
    d. Address Resolving Protocol
    e. Arpanet

17.5 Internet Attack Methods

The U.S. government's National Information Assurance glossary defined security as shielding the information systems from alteration whether accumulated or in action, and adjoining the denial of service to authorized users including the actions necessary to perceive, file and offset the threats.

Some attacks get personal information, such as eavesdropping and phishing. Some can interfere with the system's intended function, such as viruses, worms and Trojans. There are also other forms when the resources are consumed uselessly, i.e., as seen in Denial of Service (DoS) attack. Intrusions include land attacks, smurf attacks and teardrop attacks. These attacks are not as well-known as DoS attacks, but they are used in any form even if they are not known by name. Some of the well-known are as follows:

- **Eavesdropping**- When the information is intercepted by an unauthorized party, such attacks can be caused. It may be of both types, passive as well as active and the attackers steal the sensitive information.
- **Viruses -** These propagate infections by attaching themselves to data files and replicate during each execution. This can be verified, when the recycler virus attaching each parent name empty folder into consecutive folders, after a virus attack. It cannot infect until the user accesses a particular program.
- **Worms -** This is also similar to virus but it doesn't need any data file to propagate. It directly targets the host network and infects the host on the network by mailing the targeted. It is only a sub-class of virus. It does not need any external agent to transmit. Worm gets invoked by itself and self-replicates while taking advantage of information transport features on the system. Hence, this is like a worm tunneling into a system for the infection to continue down the line of systems to the last.
- **Trojan horse -** It is tricky and apparently useful software. It damages the system once installed or when run on the computer. It appears to the user as legitimate software. It deletes the files and destroys the information on the system. It is not a self-replicating or a propagating one but once installed on the PC it changes the icons and varies the desktop on the system.
- **Phishing -** It is a trick which might be applied onto browsers to steal the confidential data like credit card numbers, bank details mostly done on purchasing sites for making fraud purchases by others cards.

- **IP spoofing-** It is a technique where the attacker changes its IP (Internet Protocol) as if it is a trusted or authenticated IP of the system and somehow manages to create an impression to other systems that they are in fact communicating with a trusted party. In this, the attacker hides such that it cannot be detected and monitored.
- **Denial of service -** This is a practice in which the attacker sends continuous requests to the system to the extent of flooding so that it is unable to handle the same and thus keeps the requests in the waiting queue. Consequently, this keeps the resource busy and the system halts. This can be seen when one mail is sent many times to overcrowd the mailbox which will crash the resources and its mails will be disseminated over the internet.
- **Man-in-the–Middle Attack (MIM)**: A man-in-the-middle attack is a type of cyber-attack. A malicious actor/player inserts him/herself into a conversation between two parties. He/she impersonates both parties and also gains access to information that the two parties were exchanging or trying to send to each other A man-in-the-middle attack allows a malicious actor to intercept, send and receive data irrelevant to the two present parties, or data not meant to be exchanged at all, without either outside party knowing until it is too late.

Example: Global car Rental Company Sixt has Confirmed it Suffered a Cyber-Attack Due to Vulnerabilities in its DNS (Domain Name Servers)

Car rental company Sixt found IT irregularities on 29 April,2022. The company was a victim of an information security attack. The company operates from around 2,000 locations in 110 countries and was able to contain the effect of the attack quickly.

The incident led to disruption of business operations and the company was forced to record bookings on paper.

Vulnerabilities in the Domain Name System (DNS) was exploited by the hackers.

The vulnerabilities are located at the point where the company network meets the internet. This data is not encrypted and so the hackers exploited. The company is also vulnerable to man-in-the-middle attacks. So it is reviewing its security architecture to plug the vulnerabilities

Source: IOTW: Car rental customers face chaos during Sixt cyber-attack | Cyber Security Hub (cshub.com), 2022, Accessed on 03/06/2022

Activity 17.1

Internet Attack Methods

With the growing credit card frauds using the Internet, State Bank of India has decided to strengthen their IT security policies and go ahead with required security measures. As part of their exercise, as an IT security expert, you have

been asked to devise needed security policies. What are the different types of spoofing attacks? What are the steps to prevent them? What can be the effects if proper care is not taken? **Answer:**

17.6 Technology for Internet Security

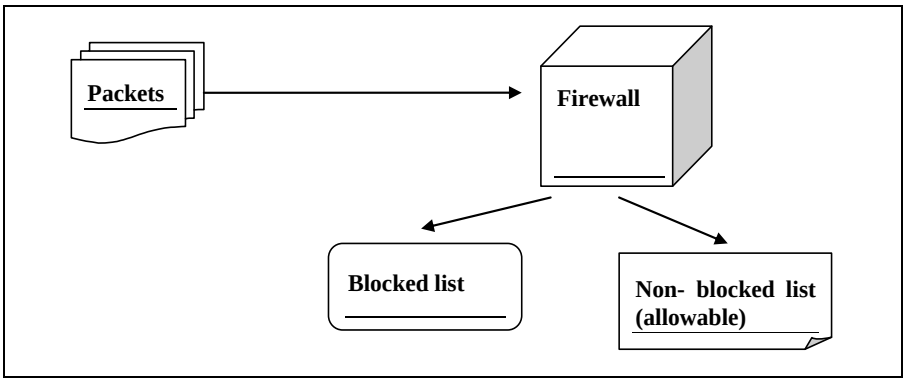
Thus, various internet threats will become a major concern in the emerging technical world which by and large depends on the internet for their services. Network security will work on three basic principles, those are –

1. Protection – Network settings should configure systems and networks as correctly as possible.
2. Detection – Set mechanism should be able to identify when the configuration has changed or when some network traffic indicates a problem.
3. Reaction – after identifying problems quickly, system must respond to them and return to state as rapidly as possible.

Though all the different mechanisms for defending attacks are not possible to be presented, the most significant ones are as follows:

1. *Firewall* - It is a type of filtering process where a set of rules are built in to filter the incoming packets and manage the packets intelligently which are suitable for network and remove the non-trusted ones as shown in Figure 17.1. This is one way to defend and secure the private LAN (Local Area Network) from the outside. Firewalls are available both in forms of software and hardware separately. They are also available in both as in coupling.

Figure 17.1: Firewall Filtering the Packets on Set of Rules



Source: ICFAI Research Center

2. *Cryptographic systems* - Encryption techniques transform the data into a form which cannot be understood nor even be retransformed into its original format without the trusted key. The encrypted data is known as ciphers. This is the best-known technique to date to secure any information.
3. *Intrusion Detection Systems (IDS)* - These are the automated hardware and software combination tellers which try to analyze the packets and monitor the network. After monitoring and analysis, each packet is blocked and alarmed to give the system about the knowledge of the attack and save it for future analysis for faster detection.
4. *Anti-Malware software and scanners* - Since many malware or malicious software have been launched in the market to attack the resources, to withstand such malware, anti-malware are also being developed to detect and cure the infections caused by malware.
5. *Secure Socket Layer (SSL)* - It is a protocol suite designed between the browser and website to secure the channel and protect any information underlying on this channel. It uses SSL certificate to authenticate the trusted party to access the payment information or the credentials information like passwords, credit cards, etc., mostly seen on email suites and payment sites like PayUmoney.
6. *Access Control* – This is mechanism in which system should be able to block unauthorized users and devices from accessing network resources. Only permitted users can access the resources in the way defined under access control mechanism.
7. *Network Segmentation* – There are many kinds of network traffic. Each type of traffic is associated with different security risks. Network segmentation allows or grants the right access to the right traffic, while restricting traffic from suspicious sources.
8. *Virtual Private networks* – VPN mechanism authenticate communication between secure networks and an endpoint device. Remote access VPN generally use IPSec or Secure Sockets Layer (SSl) for authentication, creating an encryption line to block other parties from eavesdropping.
9. *Web security* – Through web security mechanism organization ensures safe web access when connected to an internal network. It prevents web based threats from using browsers as access point to get into the network. Web security includes hardware, policies & tools to prevent threats.
10. *Wireless security* – Wireless networks are less secure than wired networks. It requires strict wireless security measures to prevent security risks.

Example: Bharath Forge Limited Implements Trend Micro's Virtual Patching Capabilities

Bharath Forge Limited Implements Trend Micro's Virtual Patching Capabilities to Shield its Critical Systems Against Malware. Pune-based Bharat Forge Ltd. (BFL) is a global leader in metal forming and a major supplier of products for the defence sector.

The company wanted to have a system where vulnerabilities can be patched virtually. It also wanted to add many layers of security protection to its end devices to effectively protect against attacks like malware.

The company chose Trend Micro's solutions which included features for advanced threat protection, anti-malware, command and control blocking, browser exploit protection, application control, behaviour monitoring, web threat protection, vulnerability protection, and more.

Source: Bharat Forge | Trend Micro, 2022, Accessed on 03/06/2022

Check Your Progress - 3

4. What is the full form of DoS?
    a. Denial of Service
    b. Deviation of Service
    c. Deployment of Service
    d. Denial of Survey
    e. Denial of Security
5. What does IDS stand for?
    a. Intrusion Detection System
    b. Information Detection Security
    c. Internet Detection System
    d. Internet Detection Security
    e. Information Detection System
6. What is the data which cannot be understood nor even be retransformed into its original format without the trusted key known as?
    a. Malware
    b. Virus oriented
    c. Firewall protected
    d. Ciphers
    e. embedded

7. How is malware removed?
    a. Anti-theft
    b. Anti-virus
    c. Scanner
    d. Anti-malware
    e. Bloatware

17.7 Cyber Essentials

Cyber essentials scheme was launched in 2014 by the Department for Business, Innovation and Skills, the UK to protect information security and hygiene. Cyber Essentials is a United Kingdom government information assurance scheme operated by the national Cyber Security Center (NCSC) that encourages organizations to adopt good practice in information security. It incorporates an assurance framework and simple set of security controls to protect information from internet threats. Cyber Essentials was developed in collaboration with industry partners, including the information Security Forum(ISF), the information Assurance for Small and Medium Enterprises Consortium (IASME) and the British Standards Institution (BSI), and is endorsed by the UK Government. Since the attackers are always keen to attack other networks and security channels, the Government/business lobbies have come up with some strategies to keep track of the networks of their own country and to monitor the activities of the attackers.

Hence, whichever is the industry or organization that starts to implement their cyber- based business, they should first recognize government-endorsed standards of cyber hygiene. Those standards are of two levels that are as- Cyber Essentials and Cyber Essentials Plus.

17.7.1 Cyber Essentials Certification (CE)

At this level, the organizations' questionnaires on self-assessment with answers are verified by a certified body (CB). These CBs are licensed by Accreditation Bodies (ABs) for Cyber Essentials evaluations and certify organizations which comply with the requirements of the scheme. But the accreditation bodies are licensed by Communications-Electronics Security Group (CESG). Some verifications done at this stage are as follows:

- Basic controls must be implemented correctly and the organization must be capable to answer the questionnaire. This brings confidence.
- Define network boundaries, location and management control
- Check the technical cyber protection
- Declaring the compliance with the cyber essentials requirements
- Declaration must be endorsed by CB

17.7.2 Cyber Essentials Plus Certification (CEP)

At this level, organization's systems are tested by CBs and the level-1 Cyber Essentials are integrated into the organization's information risk management. This stage includes the following for independent testing:

- Checking technical capability
- Vulnerability testing from inside as well as outside the organization
- There should be no compromise in protocols
- Recertify every year to meet specific procurement

But still, the concern of security is not fully addressed. The recertification is done by developing the assessment framework by the Council of Registered Ethical Security Testers (CREST). Basically, cyber essentials cover five main key controls:

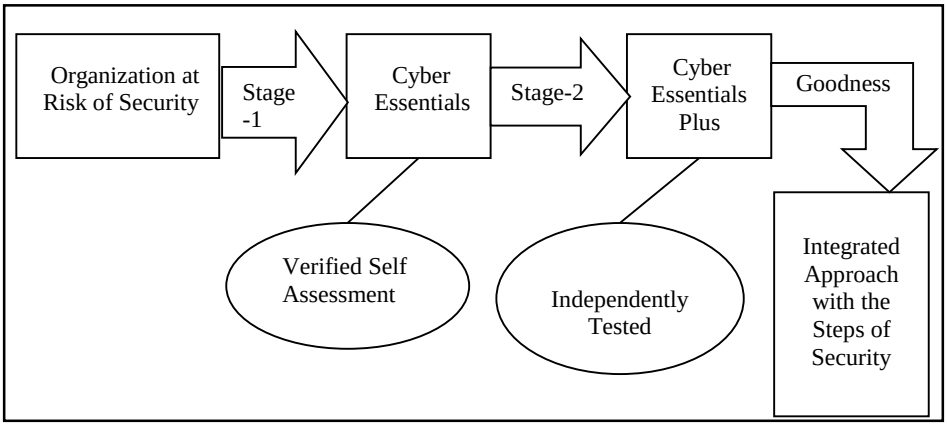
1. *Boundary firewalls and internet gateways* - firewalls and the gateway tables must be configured so correctly that there should be no unauthenticated access.
2. *Secure configuration* - hardware must be kept up-to-date to ensure protection.
3. *Access control* - right accessibility to right data should be kept in mind and accordingly update the file directories level.
4. *Malware protection* - Some extraordinary software must be installed to prevent malware.
5. *Patch management* - Necessary patches must be updated.

Even after following the Cyber Essentials scheme, an organization is not able to find the capabilities of third parties totally safe, in order to get in contact with them. For such an assurance, a framework has been developed to demonstrate security to clients. This can be shown in many ways:

- By marking their certification level against the competitors in the market
- By exposing the cyber risks clearly in the contract
- By mentioning the benefits of adoption
- By Offering the right balance between providing additional assurance and low-cost mechanism

Organizations should also ensure risk management while maintaining a robust cybersecurity. However, since June 2014, the above assurance framework has been replaced by embedding both CE and CEP in two stages in the latest framework which can be seen in Figure 17.2. This will supplement other security arrangements as well as cover good controls to defend against unsophisticated attacks.

Figure 17.2: Stages of Cyber Essentials



Source: ICFAI Research Center

Example: Lane Electronics Depends on Cyber Essentials Certification for Protecting its Defence/Industrial Clients

Lane Electronics is a major distributor for many of the leading electrical and electronic connector manufacturers. The company renewed its industry standard Cyber Essentials Certification which is a must for suppliers to the UK Defence Industry.

Cyber Essentials Certification gives an assurance to the stakeholders that the highest and the best in class counter measures are in place to face and prevent all types of common attacks. Certification requires compliance to a few IT-related control parameters including firewalls, user access control, malware protection and patch management.

Source: https://www.automation.com/en-us/articles/may-2022/lane-electronics-cyber-essentials-certification, Accessed on 03/06/2022

Activity 17.2

Assume your organization would also like to go for cyber essentials certification. Design the information system controls, guidelines and characteristics your organizational IT systems should have.

Answer:

Check Your Progress - 4

8. Who are licensed by accredited bodies?
    a. CE
    b. CESG
    c. Certified Body
    d. Private Body
    e. CEMG
9. What does CEP stand for?
    a. Cyber Endorse Procedure
    b. Cyber Essentials Plus
    c. Cyber Essential Protection
    d. Cyclical Encryption Protocol
    e. Criminal Enterprise Protection

17.8 Cyber Attacks

It is an offensive maneuver played by individuals or whole organizations (targeting organizations) that targets information security by various malicious acts into a susceptible system. Although security can be compromised through a variety of means, this chapter looks at malicious actions and the attackers that carry them out. Most of the time, an organization talks about the risk but none knows exactly what the risk means. In cybersecurity terms, a risk is possible when a danger (a person or thing that is likely to cause damage) utilizes a vulnerability (a flaw, feature or user error) and the outcome is in the form of some negative impact.

Before going into details of attacks, we must be concerned with those that cause risks. Are the organizations completely aware of the risks, when the latter is never known in the market? Some of them are as follows:

- Cybercriminals - They are fraudsters who make money by leaking or threatening to leak valuable information
- Industrial competitors and foreign intelligence - They gain an economic advantage for any company or country
- Hackers - Hacker is generally identified as a person- “a clever programmer" and “someone who tries to break into computer systems, with or without purpose”.
- Hacktivists - Those who attack for political or ideological motives
- Employees - Those who deliberately misuse for personal issues

To defend cyber-attacks, one has to have a holistic approach to remain secure. Despite good security measures, one can't imagine the power of the attacker. None have control over their capabilities and motivations, but one can make it harder for attackers by reducing the vulnerabilities. This is the ultimate truth that organizations should know.

After analyzing different types of attacks it is necessary to categorize the attacks accordingly - Untargeted and targeted attacks.

i) **Untargeted Attacks** - Here the attackers take advantage of the accessibility of the internet and indiscriminately cause damage to the number of the machines/services. The techniques used in such attacks are:

- **Phishing** - collection of sensitive information (such as bank details) by taking people to a fake website.
- **Water holing** - compromising with a legitimate server to exploit users
- **Ransomware** - disseminating disk by encrypting extortion malware
- **Scanning** - attacking wide swathes of the internet

ii) **Targeted Attacks** - They are more dangerous ones as they specifically target a particular company and find their best route to deliver, to exploit, directly into intranet/private LAN. They may be hired by somebody to exploit competitors in business. The techniques used in this attack are:

- **Spear-phishing -** mailing the attachments which on clicking downloads the malicious program on to the system and widely spreads it over LAN.
- **Deploying a botnet** - Employ DDOS (Distributed Denial of Service) attack
- **Subverting the supply chain** to attack the software

Note - *After every evaluation and testing of systems/networks, a company must not forget about the insiders. Without their proper training, insiders can also accidentally compromise a system or the information it holds.*

With the growing demand for solutions for security problems, today's market has come up with strategies to ensure that their customers are secured. Recently, software with ZERO DAY vulnerability unknown to the public becomes a flaw. Such vulnerability must be understood fully. The vulnerabilities are categorized into three, which are as follows.

- **Flaws -** It is unintended functionality. Flaws are caused due to poor coding and mistake committed at the time of deploying. They are mostly unknown at first but gradually become known to users over a long time.
- **Features** – Features are intended functionality. They become the way of choice for vulnerability by misusing the feature. One such attack is seen in MS office with the macros enabled feature, which is exploited by Melissa

worm. Another such feature, which is web browsers enabled, is JavaScript. By using such features, an attacker tries to mislead users to malicious sites and download malware in a hidden way that is not known to the user and which also bypasses the web filtering.

- **User Errors** - They are caused by users and the system becomes vulnerable. In such cases, the users are fooled and they give their passwords and personal information to attackers and it becomes easy for them to attack.

Stages of an attack

Regardless of which type the attack is, if the stages of attack can be understood, then half the problem can be solved by blocking the probing paths of the attack at different stages. Understanding these stages will help better to defend against such attacks.

Example: Phishing Campaign in Russia is Targeting Dissenters of War against Ukraine

Dissenters (citizens who do not approve of the war with Ukraine) in Russia faced a new spear type phishing attack. Government employees are warned through emails. The emails have attachments containing a Cobalt Strike beacon. By opening the attachment, the users hackers can spy on the employees. The emails looked like they were from valid government agencies.

Source: https://www.bleepingcomputer.com/news/security/phishing-campaign-targets-russian-govt-dissidents-with-cobalt-strike/, 30-March-2022, Accessed on 04/06/2022

Check Your Progress - 5

10. Which is an untargeted attack?
    a. Phishing
    b. Flaws
    c. Botnet
    d. Both (b) and (c) only
    e. MITM

17.9 Counter Measures

From the detailed discussion of cyber-attacks and controls in the above sections, it becomes evident that a good understanding of exposure risks can help the business. There will be more resilience to cope up with the attacks. To mitigate the risks, the following measures should be taken:

1. Web proxy, web filtering, content checking, and firewall policies are being employed to defend and block executable downloads, block access to

malicious domains, prevent users from directly getting connected to the internet. As such, filtrations process accessibility of company system to the internet.

2. Malware must be identified and should be removed or quarantined as per need.
3. Find the bugs in programs or the site ensuring the non-vulnerability.
4. Prevent the unknown installers from executing. Ensure that they can run on the system only when authenticated.
5. It is the same with hardware. The company utilizes the hardware binding in its network so that illegitimate machine cannot be connected in to their LAN.
6. Passwords must be good enough not to be breached by cryptanalysis.
7. Enforce correct privileges and their implementation to ensure the security.
8. Monitor the suspicious activities regularly.
9. Staff must be regularly updated with the unusual activities and impact.
10. Planning to deal with new ideas to reduce the risks.
11. Before publishing in open internet, one must filter the data so that it does not have anything that is valuable for an attacker. As in the social engineering process, attackers make use of published data by surveying sites. This is how risks in the survey stage can be mitigated.
12. By applying secure firewalls Squid servers' delivery of malware should be blocked. This is how delivery stage risks can be mitigated.
13. Well implemented access controls and patch management limit the breaching points. This is how breach stage risk is mitigated, by customizing the software.
14. Once the attacker gets complete access to the systems, it is difficult to identify their acts and avoid their existence.

Apart from above mentioned countermeasures there are three types of security countermeasures: hi-tech, lo-tech and no-tech. These three must be used in combination to create a layered and effective security programs.

Hi-tech Systems- It incorporates all electronic systems. Typically these include alarm/access control systems, video systems, communication systems, integrated security systems, specialized detection systems and computerized systems. Hi-tech systems serve to automate repetitive functions, monitor continuously without error and report to and facilitate communication and coordinated response by security staff.

Although there is an increasing focus on hi-tech systems in security programs, they should be the last element considered. Lo-tech and no-tech elements from

the basis for an effective security program and hi-tech elements amplify the capabilities of the lo-tech and no-tech elements.

Lo-tech – These are the physical security elements that are usually among the most cost-effective security measures any organization can employ. It includes things as Locks and Barriers, Lighting, Fencing, Signage, Other Physical Barriers and Crime Prevention Through Environmental Design (CPTED) measures. CPTED comprises three basic elements – Territorial Reinforcement, Natural Surveillance & Natural Access Control. Lo-tech elements can be used to funnel people to controlled access points, alter visitors to security policies, prevent entry to unauthorized people, provide a deterrent, and stop intruders cold with unexpected barriers.

No-tech – no tech elements are those security elements that have no technology:

- A Comprehensive Risk Analysis
- Policy and Procedures
- Security Awareness and Training
- Law Enforcement Liaison
- Investigations
- Dogs and other nontechnology related programs.

These are most effective primarily due to their active nature. No-tech elements are the parts of the security program that users notice most. Every interaction with a Security Officer is somehow memorable; the same cannot be said for every interaction with a card reader. Users are more likely to criticize or complain to or about their interactions with security officers than their interactions with technology.

Successful security programs mix hi-tech, lo-tech and no-tech countermeasures to achieve an effective and cost-effective program.

Example: United Airlines Takes Counter Measures to Prevent Cyber Attacks Like Phishing by Creating Awareness Among Their Staff

United Airlines considers the importance of counter measures to face the attacks as very crucial for sustaining the operations on a sustainable basis. It is aware of the dangers of even one employee committing a mistake due to negligence. So, employee awareness as a critical counter measure is recognized by the Airlines.

The Airlines has directed its staff to report suspicious emails. United's Cybersecurity team conducts simulations of phishing attacks to make the staff aware of the possibilities and how to respond.

Source: https://liveandletsfly.com/united-airlines-cyber-attacks/, 16-June-2021, Accessed on 04/06/2022

Activity 17.3

Counter Measures at a popular IT company

A biggest cyber theft happened at one of the popular IT companies. 500 million users' personal details such as name, address, phone numbers, and contacts were stolen. As an information security expert, how can you avoid such data thefts? Please mention the counter measures you will take to prevent the data theft.

17.10 Security Risks and Attacks on the Web

A website or a web service is an application used to publish, share and locate over a web which can be instantly accessed by a large number of people. Any web service is identified with a URL (Uniform Resource Locator) whose interfaces are designed using XML (Extensible Markup Language) in a WSDL (Web Service Description Language).

Generally, websites and web services use common technologies in terms of programming languages of the application. For instance, both use data stores and application servers as back-end and typically use the web server as a front end which runs over an HTTP. These types of similarities in architecture and technology inherit many common website security threats. There are many other complications which are inherent and make the web security more complicated.

i) **Capture and replay attacks:** A common threat or attack that any web service would deal with is that when the messages are transmitted over the internet, intruders may attack and gain access from the middle of the transmission. For example, a hacker may capture and replay a request to make the money transfer or modify the request before it reaches its destination which causes severe losses in the message exchange.

ii) **Buffer overflows:** Another frequent attack that any web application can suffer is from the unchecked input data. If the input given is not checked and not validated, a buffer overflow will become apparent where the data is created beyond the size of the memory allocated to hold the data. These buffer overflows may result in system crashes or it may allow the attackers to access sensitive information by compromising the security.

iii) **Denial of service attacks (DoS):** Denial of service attack (DoS) is instigated to see that web services are not available for the legitimate users. The two methods by which a DoS attack can be launched are: first, the attackers gain access to the system and send a query for large amounts of data so that the application is no longer available for the real users. In the second method, the attackers try to overload the application with a large number of requests by which the entire application fails and becomes inaccessible. As we see, attackers sometimes could combine these two approaches to maximize the damage.

iv) **Improper error handling:** Many times, the web server is unable to complete your request due to an internal server error. If such internal errors are encountered in an application server, it returns all the details which are stored in a stack and which help the programmers during development and debugging. But these details do not find their way to regular users if the application is installed, because these details may include information about the implementation and could expose vulnerabilities. Another example is if a request includes a wrong username or password, it should not be met with a response that indicates whether or not the username is valid; this would make it easier for an attacker to identify valid usernames, and then use them to guess the passwords.

v) **Broken access control:** Web applications grant permission to content and functions to some users and not for others. This is referred to as 'access control' or sometimes known as authorization. These checks are performed after authentication and govern what authorized users are allowed to do. Many times the objects are accessed directly without any authentication required. For example, if you want to access a report from the URL http://financialreport/2019-20/flipkart.pdf, the application doesn't require authentication and would allow direct access. The report is generated dynamically for logged in users, but the same report is accessible later without having to log in. Generally, in these cases, developers put the access control only on the function but not to the access.

vi) **XML external entity attacks:** Extensible markup language (XML) has the ability to build the data dynamically by pointing to a URL where the actual data is located. The attacker can fill malicious data in the place of actual content from where the data is being collected. The attacker could submit an XML request with some arbitrary URL, which points to some local XML files on the web service's file system. This results in XML parser reading large amounts of data to steal the confidential information or to launch DoS attacks on other servers.

vii) **Large Payloads:** The most common technical method the attackers prefer to damage is large payloads. These can be used to attack the web services in two ways. First, a web service can be blocked by sending a huge XML payload especially in a well-formed SOAP (Simple Access Object Protocol) request which is validated against the schema and second by producing large payloads by sending certain request queries that result in large responses. For example, if an attacker submits a request for all the available items having a common keyword in the database and if the query interface allows it, the attacker might send a request to return all the available items which would consume resources and lead to a DoS attack against the web service.

Since web services are present in different layers of the network, the web services' vulnerabilities can be extended to the operating system, network, databases, application servers, XML file system, application code and many more. The key to providing better security is to understand the threats described in the above sections, understand the different technical solutions for lessening these threats and then designing the process which takes security into consideration throughout the life cycle of the web service. Some of the practices developers need to consider are, to identify suitable web service security architecture, following the standardized practices and conducting effective testing procedures before they launch the web application. By these, one can assure complete web service security.

17.11 Malware

When we discuss cybersecurity, very often we hear the terms virus, worms, bombs and Trojan horse, etc. These are the types of infected programs (generally a piece of software) used by the attackers to infect the computers and networks. Today, all these terms are simply referred as ‘Malware’.

Malware is a portmanteau of two words ‘malicious’ and ‘software’. Malware is a computer program designed to perform malicious actions. Most of the cybercriminals try to install this malware into the computers, mobile devices or into a network to gain total control of them. The apprehension about malware is that it attacks only some specific devices with specific operating systems. But in reality, the malware can attack any kind of devices like smart-phones and tablets. The only target for the cybercriminals is to infect as many devices as possible so that they can make more money.

Malware is no longer created by enthusiastic people or by curious programmers, but by criminals, who have specific intentions like stealing the sensitive data, stealing passwords, identity theft, denial of service attack, etc. Producing the malware has become a full-time profession for many people who with dedication develop this malicious content for individuals as well as for organizations.

Once purchased, criminals make money by installing the malware on other systems and in networks; they control all the infected devices as a group without the owner's knowledge.

17.11.1 Protecting from Malware

The best way to protect from the malware is to ensure that the devices are updated and have the latest version of anti-virus software. Since attackers are innovating and developing new malware, all the anti-virus software cannot detect and stop the malicious content. To overcome these limitations, first users need to ensure that the operating systems and other applications are enabled to automatically install security updates. Secondly, users are the best ones to defend against malware. Most of the attackers are involved in social engineering where they play with the psychology of the users and play tricks or fool to install the malware. Finally, personal vigilance is the best method of protection against malware by having a continuous watch on the new links, content, software, emails, downloads, etc.

Example: Journalists with NK News (North Korea news website) were Subjected to Spear-Phishing Campaign Loaded with New 'Goldbackdoor'.

Hackers sent multiple phishing emails to the Journalists of NK News These appeared to be from the personal email address of the previously compromised former head of the South Korean National Intelligence Service, and contained Goldbackdoor malware. Believing they are from a genuine ex Intelligence Chief; the journalists opened the attachments assuring them to be useful information for their stories. The personal data was stolen in the process.

Source: https://www.nknews.org/2022/04/north-korean-hackers-steal-ex-intelligence-officials-emails-in-malware-attack/ Accessed on 04/06/2022

17.12 Phishing

Phishing is a type of attack where the attacker, also known as 'phisher', uses technical knowledge with social engineering practices in an attempt to gain the users' confidential and sensitive information illegally by imitating communications that are sent from a trustworthy or public organization. These are carried out largely by targeting user's environment and interface.

Various practices are developed to carry out phishing attacks which make them look less suspicious. Email spoofing is such a common phishing technique. Email spoofing is used to send fraudulent emails which appear to be from a legitimate sender so that the recipients believe in the received message and take actions based on the instructions. For example, a user receives a spoofed email which

comes from a website or a financial institution that he has a business with, and would probably take actions as instructed in email such as:

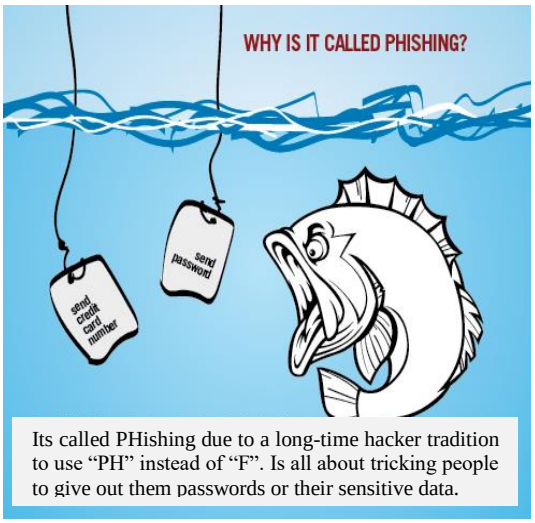
a) Reply the email with credit card number

b) Open his statement and enter the password

c) Download the PDF document and enter the credentials, etc.

This spoofing technique can also be used to spoof websites, where web spoofing makes fake websites look similar to the legal ones and would collect sensitive information.

The entire phishing attack includes three types of phishers. Mailers do the mass mailing with fake emails, which takes users to a fake landing page of a false website. Collectors who generally maintain these false websites prompt users to provide confidential information and finally hackers use this information to achieve monetary gain.



Its called PHishing due to a long-time hacker tradition to use "PH" instead of "F". Is all about tricking people to give out them passwords or their sensitive data.

A phishing attack is not only restricted to websites and emails but has spread beyond which includes SMS, social networking sites, instant messaging, etc. Some of the categories in phishing are:

i) Cloned Phishing: Cloned Phishing is that in which the phisher creates a cloned email by getting information such as content and recipient address from a genuine email which has been delivered earlier and resends the same with links having malicious data.

ii) Spear Phishing: Spear Phishing uses a target group instead of hitting thousands of emails randomly. This is used to target the specific group which has something in common, like people from the same organization.

iii) *Phone Phishing:* Phone Phishing refers to messages which are issued from a bank asking users to dial a phone number regarding problems with their bank accounts. Once dialed, a voice prompts to enter his account number and PIN.

Since phishing uses social engineering technique, educating users will prevent these types of attacks. This also can be avoided by installing firewalls, encryption software, certificates or even two-layer authentication mechanisms, if the person falls in the phishing attack.

Example: Spirit Super Faced a Phishing Attack

Tasmanian-Based Industry Super Fund Spirit Super Faced a Phishing Attack. Personal data of around 50000 members of Australian Super Fund were subjected to a Phishing attack by hackers. Hackers got access to a mail box which contained the personal information of the members. Apart from data like name, address, the lost data also included balances. The attacker sent a mail which looked like from a trusted source and escaped authentication to get the password of an employee to do further damage. The company is taking steps to closely monitor activity on user accounts.

Source: https://www.itnews.com.au/news/50k-customers-caught-up-in-spirit-super-phishing-attack-580647, 30-May-2022, Accessed on 04/06/2022

17.13 Web Security Guidelines

For many organizations, a website is their brand and first point of contact with its customers. If it is not safe and secure, those critical business relationships can be compromised. Due to the rapid growth of web application consumption, it has created a more critical and complex situation for providing security. For many years, public and private organizations have depended on traditional security measures such as firewalls, anti-virus systems. However, in recent years more and more attacks are targeting the security defects in the design of web applications, such as SQL injections, Cross Site Scripting, Phishing, etc. Traditional security measures are not sufficient to safeguard from these threats.

Web server is a computer host connected to the internet, serves the web pages to users on request. Since these web servers can be accessed by the public from anywhere, these can be subjected to attempts by hackers to compromise the server. To improve the security of web applications, an open and freely-accessible community called the Open Web Application Security Project (OWASP) has set up guidelines to reduce the risks associated with the web applications.

To protect the web server, the users need to have a basic knowledge of identifying the internet threats and the symptoms associated with them. Some of the indications that one may experience if the web server is under attack are:

- Unsolicited emails in large number will be received due to the personal information collected by the cookies, which in turn are sent back to the cookie generator, and then sold to various online marketing organizations.
- When you visit certain websites, a form of spyware will be loaded into your computer without your knowledge and creates pop-ups to appear on your computer.
- Many a time the users observe their home page changing to some unknown website. This is because certain websites will load cookies into your computer which makes the home page change its destination.

- Once the spyware loads into your computer, it uses the same computer memory that is needed to run other important software programs. This results in the distribution of computer memory making all your critical software run slowly.

A combination of good and comprehensive anti-virus software will help to protect your personal information from all these and other internet threats. The following are the list of recommendations suggested by OWASP for strengthening the security of the web applications and protecting the data handled by such applications.

- Web applications need to be developed with the best coding and development practices for avoiding prospective attacks. All the members of the development team including security professionals should adopt the secure application coding practices to fight against the common web application security vulnerabilities.
- Organizations need to develop a security policy that defines the rules and regulates how to proceed with development and maintenance of web applications.
- Security and quality assurance plans need to be developed beforehand and the same need to be implemented. These plans shall include the quality assurance methods such as code review, penetration testing, user acceptance tests, etc.
- Finally, prepare a checklist which includes all the requirements that need to assess overall web application security before final production launch.

Along with the above discussed issues, users can take on the regular procedures to protect the web servers from the standard threats. The first thing anyone needs to identify is whether or not a spyware or any other threatening software has been on your computer. This can be achieved by having a good internet security analysis tool that can completely scan your computer including the hidden files. The right scanning software will identify all the malicious content like Trojan Horses, adware, cookies and other dangerous threats and will also review the websites that have been visited by anyone using your computer and alert you to any inappropriate content found on them.

Once the threats are identified on your computer, it is important to eliminate them as soon as possible. This requires a strong anti-spyware software program which can remove the cookies, adware Trojan Horses and other dangerous spyware found on your computer. Users can install safeguards like firewall, a comprehensive anti-virus to make your system safe from all the dangerous attacks and entities. The most effective and efficient way to gain total control of your computer content is to install a proven web-filtering software program. Any good web-filtering software lets you decide what is permitted onto your computer through your browser and what should be denied.

Web servers should be scanned periodically for vulnerabilities. There are many automated tools which scan all the system software installed on the web servers. Proper access control mechanism can be deployed to restrict the physical access to the unauthorized personnel of the servers. It is recommended not to use the remote authoring tools for editing the content directly on the website. The database is a key element stored as a back-end server to serve the web applications using the query languages. These databases need to be accessed by the authorized users to protect the confidential data. Finally, every web server needs a complete security audit to check the web applications that they are completely secured.

Example: Policy Bazar Enhances Visibility and Strengthens its Security Posture by Going for Web Security Tools

Policy Bazar is a major aggregator of insurance policies in India. The site provides a comparative analysis of various insurance products for the user to choose from. The company moved its applications to Amazon cloud. The security in the cloud has just gone out of the company`s direct control. The company has to share the responsibility with Amazon for its security requirements. The company went for a solution which takes care of data breaches and the consequent disruption in operations.

They chose Trend Micro's Deep Discovery Inspector which detects and protects against zero-day malware, document exploits, attacker network activity, web threats, email threats such as phishing and spear phishing, and more.

Security operations were simplified with a single management dashboard for all security capabilities, and multiple modules-including anti-malware, web reputation, intrusion prevention, integrity monitoring, and firewall protection-offering effective and efficient security against threats.

Source: https://www.trendmicro.com/en_us/about/customer-stories/policybazaar.html, 2022, Accessed on 04/06/2022

17.14 Wireless Network Security

Wireless network has become an indispensable technology. It has multiple qualifications over the wired networks, such as it is cost-effective, easy erection, faster than the wired media, etc. Following are some of the important facts to be remembered about the wireless networks.

1. Wireless technology has been deployed world over with the aim to access the internet. But it must be understood that wireless is overly preferred than the wired network to access and communicate. All the Wireless Local Area Network (WLAN) communicates by using high-frequency radio waves. But in all this, there is only one Wireless Access Point (WAP) which is a hardware device through which other wireless media devices are connected using

protection or no protection. This AP is also connected to the wired network so that it acts as a bridge between the wired and wireless network that provides wireless band the use of the internet.

2. For the safety features, each wireless AP serves with a SSID (Service Set Identifier) which acts as a shared password between the client and AP to connect the correct client. For further details, learners must know the options for more security to their LAN as mentioned.
3. *WiFi Protected Access (WPA and WPA2)* - In this option all the information gets encrypted and it ensures that none of their shared keys is modified and so it is more secure than WEP (Wireless Equivalent Privacy). It is also available in two types of authentication, i.e. WPA in which the same key is the shared key in a group and WPA2 or WPA2-Enterprise with different keys to different clients. It is also shared with a pre-shared key so that it is also called WPA personal.
4. *Wireless Equivalent Privacy (WEP)* - This is an outdated WEP key which can be broken easily within minutes by available automated tools in the market. Hence it is not considered as secure now.
5. *802.1X authentication* - It is a procedure to validate the clients while connecting to wireless networks and wired Ethernet networks. It is analogous to providing a valid visa while entering the country. With the 802.1x countervailed client gives his credentials to authenticator which is forwarded to the server for verification. If it is verified by the server then the client is allowed to communicate on the protected network.

Wireless intrusion prevention

There are three principal ways to secure a wireless network

- Small Closed Networks – Setting access restrictions through Access Point are the common way to provide security. It incorporates encryption, MAC address checking and wireless Intrusion Prevention Systems to secure wireless LANs.
- Commercial Providers – Hotspots and large organizations often uses open & unencrypted but completely isolated wireless networks as security mechanism. The users will at first have no access to the internet nor to any local network resources. Commercial providers usually forward all web traffic to a captive portal which provides for payment and/or authorization. Another solution is to use Virtual Private Networks (VPN).
- End to end encryption – In many offices intruders can easily hook up with organizational wireless networks. This can be prevented by providing end-to-end encryption with independent authentication on all resources that shouldn't be available to the public.

The most important qualification of a wireless network is that it makes distance restricted to enhance security, also known as the security within the campus. However, it may be taken as its disqualification as well, that restricts the working jurisdiction of this network within the walls.

Activity 17.4

Wireless Network Security

A high technology project at Infosys is using different wireless technologies in its team. They are executing this project for a Finland based customer for the duration of a year. What is the utility of WPA and WPA2? What is the utility of WPA-PSK? For the given IT services organization, Infosys, what steps are needed to utilize WPA-PSK and where is it useful?

Answer:

Check Your Progress - 6

11. What does WAP stand for?
    a. Wireless Address Protocol
    b. Wired Access Point
    c. Wireless Access Point
    d. Wireless Activation Point
    e. Wide Area Protocol
12. What does SSID stand for?
    a. Set Service Identifier
    b. Service Set Identifier
    c. Service Set Identification
    d. Service Set Indicator
    e. Secure Set Identifier

13. What is WiFi Protected Access is also known in short as?
    a. WPA
    b. WiFPA
    c. Web App
    d. WFPA
    e. Wireless Network
14. What is WEP?
    a. Wired Equivalent Privacy
    b. Wireless Environment Privacy
    c. Wireless Equivalent Privacy
    d. Wireless Equipment Privacy
    e. WE Protection

17.15 Network Security Testing

Network security is the major issue in today's highly digitized environment. There are advancements not only in technology but also in threats which need to secure swiftly and adapt to the latest changes. But enhancing the security option alone is not sufficient to mitigate this problem. Therefore, the U.S. Federal Regulations proposed systematic operational security testing program. This supports the following targets:

- Issues over how large the system is? Are they independent or not?, if dependent, interoperability functionalizing or not etc., are critical to security testing. Also one needs to try to fill the gap between the actual operation of the systems and the developed state after resolving all these issues.
- Calibrate and document the operational security position of an organization. The programs made by the developer for testing purposes must meet security demands, fast-changing threats, cost-demands and must be auto repairable.
- Must be systematic, comprehensive, ongoing, and priority-driven security testing so that enterprises can have a good reputation and be cost-effective.

It would be helpful if the tester can think like attackers/perpetrators and for that, one must analyze the system's working levels and vulnerability deeply as the attacker also finds the vulnerability by testing on each seed and then targets the level on which attack can be attempted. For this, appropriate security measures and procedures can be implemented at five levels.

On a different level, different security measures are arranged to secure the network. Therefore, network security testing should be conducted on a regular basis to determine the network mapping, vulnerability scanning, password

cracking, penetration testing, war dialing, war driving, file integrity checking and virus scanning. For example, when the testing is done on the perimeter level, it may not find any vulnerable point. Next, one should go to the second network level and if one finds some weakness, an improvement strategy must be applied. Thus, the process of discovering vulnerabilities should be verified by applying the recursive procedure at later levels. After completion of all the tests, it is assured that vulnerabilities are patched or mitigated.

17.16 Future of Computer Network Security

In future, a set of new emerging applications will drive the internet security. As advances in technology and development of applications progress, the internet will be entangled in more security issues. Moreover, security is analogous to the human immune system which fights with the attacks and also manages to save the immunity to defend for future purposes.

Many security approaches have been developed until now. The latest active technology is a combination of hardware and software. The biometrics that is used as in AADHAAR cards is an example. In future, such approaches will be ideal. In addition, various protocol suites have evolved rapidly to deal with further threats in the future. The future of network security might be far from clear-cut. One thing is clear –it will certainly be richer and more sophisticated than we have seen so far. Determining how to plan for a business environment in which everyone is connected and security expectations are high is not trivial. We all have to do it.

Example: Singapore in Order to Stay Ahead of Security Threats Depends On Quantum Computing Technology

Singapore is betting on enhancing its capabilities in quantum computing especially to use the computing power to attempt much more powerful encryption to ward off "brute force" way of attacks. Current encryption standard itself is difficult to break but quantum computing (speeds at 150 millions faster than current super computers) is going to change all that. What a today's super computer takes 10000 years to solve can be solved in minutes by quantum computers.

Source: https://www.zdnet.com/article/singapore-ups-investment-in-quantum-computing-to-stay-ahead-of-security-threats/, 31-May-2022, Accessed on 04/06/2022

Activity 17.5

Future of Network Security

McAfee is a world-renowned software security company. As on April 2017, Intel holds a 49% stake in this organization. What are the future challenges being faced by network security companies like McAfee while building necessary software to prevent security breaches and losses to different

companies in different industries**?** Discuss any case of an organization you came across which built network security in their operations. **Answer:**

Check Your Progress - 7

15. IDS (Intrusion Detection System) tests which of the following layers?
    a. Network
    b. Host
    c. Application
    d. Software
    e. Hardware
16. Internet Data Security Validation of password is done on which of the following layers?
    a. Host
    b. Application
    c. Perimeter
    d. Security
    e. Physical
17. When is network security testing done?
    a. Priority wise
    b. Protection wise
    c. Response wise
    d. Cost wise
    e. Route wise
18. Where does the future of network security lie?
    a. Sharing keys
    b. Credit logons
    c. Password protection
    d. IRIS
    e. Biometric security

17.17 Summary

- Network is the physical conveyer of data and information from one to another location. Therefore, there are many chances to get the man-made data pilferage for one's benefits. Such an unauthorized access to data is undesirable; thus, it needs to be immediately stopped. Therefore, the network security is important and vital for the organizations who handle delicate and sensitive data in terms of security.
- Network security is very vital for any organization. The importance of security levels is highlighted in the unit. Major methodologies, approaches and techniques to secure the network are discussed. The structured analysis, security analysis and testing to bridge gaps are discussed.
- Different application approaches such as perimeter tools, scanners and the different aspects of attacks are explained. The systematic and procedural security detection and testing strategy are described. The future of business development with versatility in security is explained in the unit.
- Different Categories of Network Security Threats: active attacks, passive attacks
- Various internet attacks include: Eavesdropping, Viruses, denial of service, man-in-the-middle attack, worms, phishing, IP spoofing, etc.
- Technology for internet security include: Firewall, cryptographic systems, intrusion detection systems, secure socket layer etc.
- Cyber-attack risks include: cyber criminals, hackers, hacktivists, etc.
- Malware is a computer program designed to perform malicious actions.
- Phishing is a type of attack where the attacker, also known as 'phisher', uses technical knowledge with social engineering practices.

17.18 Glossary

Certification: It is about the strict protocols which have to be passed by a company or individuals for the security that has the potential to compete and withstand the various security risks. IT industry has different certifications available for software tester, project manager and developer.

Crypt Analysis: Cryptanalysis is the study of cipher text ciphers and cryptosystems with the aim of understanding how they work and finding and improving techniques for defeating or weakening them.

DoS: Denial of service is an attack in which mass packets are managed to be transmitted to a fixed target so that the latter fails to manage all the same. Packets and hard disk or the system might be overloaded to a crash point or ended in a halt state.

DDOS: Distributed Denial of Service is a type of DOS, wherein multiple compromised systems try to infect a single system causing Denial of Service attack.

Phishing: It is a masquerading practice adopted by an attacker to get driver technology used to collect username, password and sometimes account details on the internet and that may lead to scams. It is mainly done by sending mails and telephonic conversations to get bank details. It can be protected by awareness and caution over the internet.

Squid Servers: A caching and forwarding HTTP web proxy. Its use includes speeding up a web server by caching repeated requests, caching web, DNS and other computer network lookups for a group of people sharing network resources, and aiding security by filtering traffic.

Threat: A threat is an intention or an action tried to cause possible breaching of security. It is the way of malfunctioning the network or private LAN exposed to the vulnerabilities.

Validation: This is an authentication process where the client's password and other credentials are checked against those stored on the server to allow further communication.

Vulnerability: It is the weakness in the code or any system which compromises the system's safety thereby providing access to an attacker. It is managed by a repetitious process of identifying, classifying, remediating and finally mitigating vulnerabilities.

17.19 Self-Assessment Test

1. Explain the need to secure the network.
2. Describe the categories of network security attacks.
3. Differentiate between Virus, Worm and Trojan.
4. What are the levels employed in network testing?
5. How does IDS (Intrusion Detection System) work?
6. What is the future of computer security? Explain briefly.

17.20 Suggested Readings / Reference Material

1. Rodney Heisterberg and Alakh Verma (April 2022). "Creating Business Agility: How Convergence of Cloud, Social, Mobile, Video and Big Data Enables Competitive Advantage," Narrated by Stephen Graybill.
2. Jonathan S Walker (2021). Social Media Marketing For Beginners - How To Make Money Online: Guaranteed Strategies To Monetizing, Mastering, & Dominating Any Platform For Your Brand, JW Choices.
3. Barry Connolly (2020). Digital Trust: Social Media Strategies to Increase Trust and Engage Customers, Bloomsbury Business.

4. Seema Gupta (6 August 2020). Digital Marketing McGraw Hill; Second edition.
5. Tracy L. Tuten, Michael R (15 June 2020). Solomon et al, Social Media Marketing, SAGE Publications Pvt. Ltd; Third edition.
6. Paul Martin Thomas Erickson (2019). Social Media: Usage and Impact, Global Vision Publishing House, 2 edition.
7. Steve Randazzo (2019). Brand Experiences: Building Connections in a Digitally Cluttered World, Paipen publishing.

17.21 Answers to Check Your Progress Questions

1. (a) ARPANET

ARPANET is the US defense project for military communications which is the backbone of the internet.

2. (b) Interception

Interception only steals information without any modification to it. Just keep an eye to analyze and try to exploit the information by trying with small phrases.

3. (c) Address Resolution Protocol

Address Resolution Protocol is for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network.

4. (a) Denial of Service

Denial of Service, because it tries to make the system halt by overloading it with a continuous transmission of the packets and keeps the resource busy.

5. (a) Intrusion Detection System

Intrusion detection system is used to detect the intruder or attacker.

6. (d) Cipher

Ciphers are encrypted data, which cannot be read by intruders, and are transmitted over the network in a secure manner.

7. (d) Anti-malware

Anti-malware, as the name goes, is a program to protect from malware-related data loss.

8. (c) Certified body

Certified bodies are licensed by Accreditation Bodies (ABs) for Cyber Essentials evaluations and they certify organizations which comply with the requirements of the scheme.

9. (a) Phishing

Since phishing can be both targeted and non-targeted mostly intended to mass mailing suspects where the flaws and botnets specifically target a customer for their bank information.

10. (b) Cyber Essentials Plus

CEP stands for Cyber Essentials Plus.

11. (c) Wireless Access Point

Wireless Access Point is a device by which all others get connected to provide internet service.

12. (b) Service Set Identifier

It acts like a unique ID as an IP which is used to detect by wireless media to connect.

13. (a) WPA

Wi-Fi Protected Access is a Wi-Fi standard, designed to improve upon the security features of WEP.

14. (c) Wireless Equivalent Privacy

WEP (Wireless Equivalent Privacy) is a security protocol used for encrypting transmitted data in wireless networks.

15. (a) Network

IDS is a device or software application that monitors network or system activities for malicious activities or policy violations.

16. (b) Application layer

Validation of password is done on the Application layer.

17. (a) Priority wise

If the highest priority level vulnerability does not detect then it applies to the next lower level.

18. (e) Biometric security

It saves both biological credentials with cryptographic protections as in Aadhaar card enrollment.

Unit 18

Information Security in Cloud Environment

Structure

"If you spend more on coffee than on IT security, you will be hacked. What's more, you deserve to be hacked."

- Richard Clarke, Former Cyber Security Advisor,
White House Cybersecurity Advisor, 1992-2003.

18.1 Introduction

Cyber security is like everything else: you get what you pay for.

The previous unit discussed the history of network security, internet attack methods, technologies for internet security, wireless network security, testing and future of computer network security. A core challenge of information security is to reduce risk to an acceptable level in an organization. Information security protects against misuse of corporate data, loss of assets, unauthorized data disclosure and accessibility.

As many business processes and systems related activities are being moved to cloud nowadays, it is essential for the users to understand the security aspects of information security under cloud environment. This unit covers management of cloud based systems activities, the allied governance, preparing the plans for

deployment and security, actions for implementing the plans, controlling the actions and applications by measuring and monitoring the information systems. Focus is also on improving information security under cloud environment.

18.2 Objectives

By the end of this unit, you should be able to:

- Discuss the information security and governance framework
- Define the conceptual framework of security and governance
- Relate to the architecture of information security systems
- Discuss the implementation of an information security system

18.3 Cloud Information Security Management and Governance Framework

There is a need to identify ways to improve the existing information security steps involved in building information systems.

18.3.1 Information security governance

IT Security governance has many characteristics. Leading firms establish good governance systems and practices to achieve accountabilities and actions in an organization. The core objective of the IT security system is to achieve good governance and information protection. Information governance decides the overall strategy for information at an organization. Information governance takes care of information risks. It maintains balance between information risks and information value. Information governance guides for legal compliances, operational transparency and reducing expenditures associated with legal discovery. An organization can establish a consistent and logical framework for employees to handle data through their information governance policies and procedures. These policies help organizations and employees to store and safeguard electronic records in a legal way.

Information security governance is the responsibility of all the stakeholders in a company. The board of directors and all the executive members play a crucial role. A transparent and clearly defined policy makes the governance easy to be implemented. The Board of Directors has an inherent responsibility to visualize and create an ambience for implementing the IT policies. It should become a part of the company's culture. With ever-growing business requirements and processes, a clear policy determines a proper structure within an organization. The other senior executives will have the responsibility to operationalize the policy guidelines mentioned in the IT policy of the firm. IT security and governance should become one of the most important inherent objectives of the organization, and many organizations are spending heavily on security.

Principles of information security governance

There are six principles of information security governance

- Establish organization wide information security – Information security, or cyber security, concerns should permeate the organization's structure and function. All levels of management across organization should ensure that information security is integrated with information technology and other activities. Top level of management should ensure that information security serves overall business objectives.
- Adopt a risk based approach – Security governance including allocation of resources and budgets, should be based on the risk appetite of an organization, considering loss of competitive advantage, compliance and liability risks, operational disruption, reputational harm and financial loss.
- Set the direction of investment decisions – information security investments are intended to support organizational objectives. Security governance entails ensuring that information security is integrated with existing organization processes for capital and operational expenditure, for legal and regulatory compliance and for risk reporting.
- Ensure conformance with internal and external requirements- Mandatory legislation and regulations, certification standards & contractual requirements like external requirements and organizational goals and objectives like internal requirements should be ensured. To ensure conformance of these requirements independent security audits are accepted.
- Foster a security-positive environment for all stakeholders – security governance should be responsive to stakeholder expectations, keeping in mind that various stakeholders can have different values and needs. The governing body should take the lead in promoting a positive information security culture, which includes requiring and supporting security education, training and awareness programs.
- Review performance in relation to business outcome- From a governance perspective, security performance encompasses not just effectiveness and efficiency but also impact on overall business goals and objectives. Governance executives should mandate reviews of a performance measurement program for monitoring, audit and improvement that links information security performance to business performance.

Desired outcomes of information security governance

There are five basic outcomes of information security and governance policies. It is essential to understand their impact on the overall business strategy and risk management of the firm:

- Strategic alignment of information security with business strategy

- Risk management by executing appropriate measures to manage and mitigate risks
- Resource management by utilizing information security knowledge
- Performance measurement by measuring, monitoring and reporting information security governance metrics
- Value delivery by optimizing information security investments.

Benefits of Information Security Governance

An organization benefits greatly from having a good information security governance system. Mentioned below are some of the benefits.

- Secure Organization information in all its forms – Organizational information in the form of digital format, paper-based, intellectual property, company secrets, data on devices and in the cloud, hard copies and personal information is secured.
- Improves Company culture – The standard's holistic approach covers the whole organization, not just IT and encompasses people, processes and technology. This enables employees to readily understand risks and embrace security controls as part of their everyday working practices.
- Provides a centrally managed framework – Information Security Governance provides a framework for keeping your organization's information safe and managing it all in one place.
- Offers organization-wide protection – It protects your entire organization from technology-based risks and other more common threats such as poorly informed staff or ineffective procedures.
- Helps respond to evolving security threats – constantly adapting to changes both in the environment and inside the organization, Information Security Governance reduces the threat of continually evolving risks.
- Reduce costs associated with information security – Risk assessment and analysis approach of Information Security Governance can reduce costs spent on indiscriminately adding layers of defensive technology that might not work.
- Protect confidentiality, availability and integrity of data – Information Security Governance set policies, procedures, technical and physical controls to protect the confidentiality, availability and integrity of information.
- Increases resilience to cyberattacks – implementing and maintaining Information security Governance will significantly increase organization's resilience to cyber attacks.

Information related to thefts can be avoided and it protects the business operations from the increased vulnerability of attacks on the data. The civil and legal liability is protected for the organization. Risk management, process improvement and enhanced security, ensure optimum allocation of the limited resources in a firm and bring in greater productivity and profitability in the firm. The business valuation increases rapidly as a secure business framework is created. The Chinese walls and other security measures ensure that information security is maintained during market sensitive operations like mergers and acquisitions, BPR (Business Process Recovery) and also regulatory responses.

It also enhances the brand value of the firm and the trustworthiness of the organization. All the external stakeholders will have confidence and also problems related to the agency theory can be avoided.

Example: Zoom Executives Offer Deep Dive on Revamped, Post Pandemic Governance Framework

Due to coronavirus shutdowns which started in March 2020, companies started using platforms like Zoom for remote working, video meetings, and contacting family and friends. Subscriber base went from 10 million in December 2019 to 300 million by April 2020.

While the business grew, issues related to privacy and security issues surfaced. A large number of lawsuits were filed against the company, bad publicity was given in the media and ZOOM was banned by several Governments, companies and educational institutions.

The company is now investing efforts to fix security issues, win over customer trust, and save the business. Many of its problems were the result of lack of security governance related to security and privacy.

Source: Zooming In On Cyber Governance: Top Ten Actions For Boards And Execs (forbes.com), 14-July-2020, Accessed on 05/06/2022

Check Your Progress - 1

1. What is Information security governance?
   a. Defining core IT security principles
   b. Accountability and action of organization
   c. The responsibility of the Board of Directors
   d. Defining IT security principles accountability and action, responsibility of the board directors
   e. Nothing but corporate governance

18.4 Architecting Information Security Plan

Organizations today are facing constant change from various entities like the marketplace, competitors, emerging technologies and growing client expectations. Global changes like corporate governance reform, security concerns arising from terrorism and increased malicious Internet activity have required organizations to be resilient in times of competition and uncertainty.

Due to the changing business objectives, procedures in information security need to be constantly upgraded. These are governed by the prioritized set of principles that all organizations need to follow.

Seven Basic Principles of Information Security are:

1. Information security is an integral part of enterprise strategy
2. Information security impacts the entire organization
3. Enterprise risk management defines information security requirements
4. Information security accountabilities should be defined and acknowledged
5. Information security must consider internal and external stakeholders
6. Information security requires understanding and commitment
7. Information security requires continual improvement

Activity 18.1

Information Security at LIC

Life Insurance Corporation (LIC) of India has different branches, thousands of agents, and third-party vendors to provide specific niche services such as conducting medical examinations for proposed policyholders. Now, they are concerned about the security of their customer details. Please detail: Why information security must consider internal and external stakeholders? Who is a stakeholder and why is communications to stakeholders a vital activity? Can you discuss effects of a security breach in the given case including digital documentation?

Answer:

18.4.1 Characteristics of Security Architecture

Security has turned out to be the hot-selling need of organizations as well as most of the individuals who are concerned with handling data and information. The security architecture is one of the determinants of the security effectiveness, especially in the networked data–exchange applications.

People, processes, and tools need to work together to protect companywide assets. To integrate these components effectively, the security-related architecture needs to be designed and drafted by the policy. This policy shall state management's performance expectations, the architecture, implementation methods, and architecture enforcement methods. This enables the architecture to act as a guide to the management and the organization. This helps in ensuring that, the decisions are aligned and consistent throughout the entire IT landscape. The architecture needs to be strategic, and be structured in a way that supports the organization's business goals.

The components described herein should form part of an effective and carefully planned security architecture and should be evaluated during audits of the security architecture. These are:

- Guidance in the areas of incident response, baseline configuration, account creation and management, disaster recovery, and security monitoring.
- Identity management.
- Inclusion and exclusion of who and what is subject to the domain of the security architecture.
- Access and border control.
- Validation and adjustment of the architecture.
- Training.
- Technology.

Security architect needs to consider the normal flow of the application. Conditions such as the abnormal flows and failure modes need to be interrupted and prevented from failure.

18.4.2 Areas of Concern for a Security Architect

The security architecture requires multiple parameters to be followed while implementing the same, such as – the security audit, security authentication and authorization, etc.

The generally accepted areas of concern for the security architect are:

- **Authentication**: The effective way to identify a user or entity in an enterprise or system regarding access
- **Authorization**: The permitted capabilities for an entity or person whose specific identity to access an established resource

- **Audit**: The capability to provide accountability of an organization's data, attesting that the security policies have been in accordance with the defined systems.
- **Assurance**: The ability to verify whether the enterprise architecture has the required security attributes to support their listed security policies
- **Availability**: The enterprise system capability to perform without IT service interruption despite malicious events
- **Asset Protection**: To safeguard information assets from theft, unauthorized access and unintended use or disclosure
- **Administration**: The capability to execute security policy changes in an enterprise system

Various security parameters make a total security package to deal with security issues. Some of them are applied only to the user since the user is the first and most important cause for a security breach. Thus, authentication and authorization are applicable only to the user.

Example: NASA Faces more Cyber-Attacks Due to Lack of Well-Defined Security Architecture

An audit conducted at NASA revealed that the number of cyber-attacks increased significantly in the last four years and more so after the pandemic. Shifting to work from home led to more violations of security policies by employees. The number of devices connected has also increased dramatically. The audit team found the agency does not have full-fledged risk management plan. IT security architecture is also work in progress. The evolving architecture has not been able to guide the agency related to extra risks due to shift to work from home. The agency had a fragmented approach to IT, with many separate lines of authority. So, decision making related to security was affected.

Source: https://www.secureworld.io/industry-news/nasa-cybersecurity-audit-2021, Accessed on 10/06/2022

Check Your Progress - 2

2. Which of the following is referred as the substantiation of the identity of a person or entity related to the enterprise or system in some way?
    a. Authentication
    b. Assurance
    c. Acceptance
    d. Asset protection
    e. Encryption

3. Which of the following is referred as the protection of information assets from loss or unintended disclosure, and resources from unauthorized and unintended use?
   a. Administration
   b. Audit
   c. Risk management
   d. Asset protection
   e. Security protocol

18.5 Implementing and Operating Information Security Program

Organizations need to build internal information security for activities to be done on cloud environment. We will outline the points to be addressed in building such policies/programs.

18.5.1 Development of Information Security Policy

The information security policy is a document which defines clear objectives, procedures, rules and regulations to be followed by the firm. It also determines boundaries for the stakeholders, especially the internal and external stakeholders to act in an ethical manner. The IT infrastructure of the firm needs to be monitored as effectively as most information in the organization is stored in electronic form. The major objective of the information security policy should be building a clear and unambiguous reference document to be understood and followed by everybody in the organization.

18.5.2 The Basic Stages of Information Security Policy

The basic stages of information security policy include:

- Understand the information security level in an organization
- Analyze the information obtained from the results
- Frame a schedule to develop information security policy
- Formulate an information security policy

Information documents contain the plans, policies, procedures, frameworks, etc. of an organization that needs security from unauthorized hands. It may have a competitive edge over others.

Following information documents are essential in any organization:

- Information security policy of the organization - a document that describes all the policies and frameworks related to information security in an organization.

- Regulations on information security, which reveal in more detail procedures and methods of providing information security in accordance with the basic principles and rules described in the policy.
- Other documents such as reports, registration periodicals, and other low-level leading documents.

18.5.3 Protection Against External Information Security Threats

Threats that emerge from the external environments need to be protected against, through different techniques.

These include:

- Control of information security risks
- Control of vulnerabilities
- Data leakage prevention
  - Content filter systems (internet, e-mail, ICQ, P2P);
  - The control of information-carrying media (USB devices – flash drives, external hard drives), print queues, access to network resources.
- Guarantee of confidentiality during storage and transmissions
  - Data link encryption (organization of VPN, SSL, PKI);
  - Storage media encryption (creation of secure containers, design of corporate encryption and data storage systems).
- Prevention of Internet-based attacks aimed at corrupting, destroying or stealing information, or otherwise denying the service of a company's information system
- Prevention of the spread of malicious codes – viruses, software Trojans, spy programs, internet worms
- Control of Unsolicited mail (spam)

External information security threats are always found to be important and uncontrollable in general terms since easy access to control point is not possible. Thus, the external security risk mitigation plan is required to be strong and must be implemented in continuous order to stop recurrence of the same. Thus, control of vulnerability, data transportation control, data-link encryption, etc., are to be taken proper care of.

Example: NEC Corporation of America gets Global Certification for its Information Security Program

NEC Corporation of America is a major global IT services company. The company received the industry standard ISO 27001 certification for its Information Security Management system.

Contd….

This certification is awarded to organizations based on established security policies, procedures, security controls, management reviews, internal audits, and external audits. The certification validates the best-in-class security policies of the company. The certification assures present and future customers that their data with NEC Corporation is protected. The external auditors verified the implementation of one hundred and fourteen controls as stipulated by ISO.

Source: https://www.businesswire.com/news/home/20220330005853/en/NEC%E2%80%99s-Information-Security-Management-System-Receives-Global-ISO-27001-Certification, 30-March-2022, Accessed on 11/06/2022

Activity 18.2

External Information Security Threats for a Bank

ICICI Bank is the largest private sector bank in India. It has outsourced its credit card issue and maintenance business to a third party. In a banking environment, which according to you are the external information security threats? Discuss both with reference to the bank and individual customer. Is third-party vendor a security breach area? How can you confirm?

Answer:

Check Your Progress - 3

4. Which of the following is a high-level document, which includes principles and rules?
    a. Information security policy
    b. Implementation document
    c. Annual report
    d. Process view
    e. Annual review
5. What are Trojans, virus, internet worms and spy programs?
    a. Spams
    b. Malicious codes
    c. Spyware
    d. Firewalls
    e. Routers

6. Which of the following is not a part of the basic stages of information security policy?
   a. Understand the information security level in an organization
   b. Analyze the information obtained from the results
   c. Frame a schedule to develop information security policy
   d. Formulate an information security policy
   e. Implement the policy with measures

18.6 Monitoring and Measuring Information Security Program

Monitoring and measuring information security program is a continuous process and an ongoing activity. Various industry standards like ISO 27004 can be applied. The steps mentioned in ISO 27004 in ISMS are as follows:

1. Identify the object or process for measurement

The scope of measurement has to define what needs to be measured. A well-documented process will bring consistency in the management of quality. An object includes plans, projects, processes, resources and systems. The object also includes the behavior of the employees and the activities of various departments responsible for information security.

- **Define Point of Reference:** Baseline values with an indicated point of reference are to be defined for each measurable objective. Every threshold value and targets at an acceptable level of performance need to be finalized.
- **Collect Data:** Data should be collected in a timely fashion. Today's organizations have multi-dimensional data for systems and processes. The data of critical activity needs to be maintained in understandable metrics. Automated data collection techniques can also be used to achieve the standardized data and reporting.

2. Understand and develop ISO method

As per ISO 27004, selected objects undergo various attributes in a logical, operational sequence for measurement. The output derived need to make sense for their stakeholder, further indicators to be used for performance improvement in information security programs.

- **Analyze the measured values:** 'Analysis and interpretation' is an important activity in terms of understanding the qualitative and quantitative aspects of the indicators measured. The analysis of results should identify the gaps between the baseline and the actual measurement value.

- **Communicate and control:** Output of the analyzed data should be communicated to all the relevant stakeholders. The measured values can be communicated using dashboards, charts, reports, etc. A consistent approach should be followed in the preparation of the report.

Example: Yahoo built a Culture of Cybersecurity by Innovatively Measuring and Monitoring its Information Security Program

Yahoo realized that just telling its employees to do something is enough for meaningful change with respect to the implementation of information security practices across the organization. The HR team in consultation with security experts and behavioural science experts distinguished between employee actions, habits, and behaviours. For example, just attending a training programme on password policy is an action. Over a period, making password changes through password manager is a habit and finally the desired security behaviour is not just using the password manager but making employees to generate and store credentials through a password manager whenever they were creating or updating accounts.

Based on a set of measurements the company is able to know what percentage of employees have changed the behaviour and take corrective actions any how to increase this percentage.

Source: https://hbr.org/2021/09/how-yahoo-built-a-culture-of-cybersecurity, Accessed on 11/06/2022

Check Your Progress - 4

7. Which of the following specifies monitoring and measuring of Information Security Measurement model?
   a. ISO24007
   b. ISO27004
   c. ISO9000
   d. ISO14000
   e. ISO18000
8. What does ISMS stand for?
   a. Information Security Measurement Space
   b. Information System Monitoring Sphere
   c. Information Security Management System
   d. Information Service Management System
   e. Institution Security Management Software

18.7 Improving Information Security

Discussed below are some crucial points to be focused by organizations, while addressing improvement in information security within the organization.

18.7.1 Improving Information Security with Automated Services in Managed Systems

In today's era, hackers and attackers on the information system are increasing. As the organization grows, it poses a continuous challenge to all those involved in the information security process. The efficiency and effectiveness of the information security should be continuously monitored and effort should be made to improve the same. However, basic security and virus protection software isn't enough to keep up with the barrage of attacks dealt against enterprise assets due to the expanding environments in which these services exist. For that, it's necessary for organizations to invest in system management assets.

Below mentioned tips improves information Security-

- Know what you need to protect – Ask following questions and decide
  - What are organization's most valuable assets?
  - Where are they?
  - Who has access to them and why?
  - When are they being accessed?
- Evaluate your security posture – As long as chance of exploitation exist, organization needs a process in place to continuously find the existing vulnerabilities.
- Take a data-centric approach- In order to protect organization from evolving IT changes and targeted attacks, Organization need to shift focus from trying to secure everything to protecting what matters most- securing sensitive data.
- Develop a clear understanding of cloud service models and security issues – organizations should develop a clear understanding of cloud service models, as security issues vary depending on the model being used.
- Consider a Cloud Access Security Broker (CASB) – CASBs enable organizations to manage and enforce security policies across disparate applications, providing much-needed insight into cloud activity, and a single point of control for multiple applications and services.
- Don't forget to address insider threats – It is no longer enough to simply look outwards and focus on what's coming in; security team must also look inwards to evaluate what's going on within the company and what's going out.
- Leverage threat intelligence – Commercial threat intelligence technology and services can help enterprise arm themselves with the strategic, tactical and operational insights they need to identify and respond to global threat activity and integrate intelligence into their security programs.

- Use deception to enhance detection and response – The mean time to identify (MTTI) breaches is known as dwell time. Lengthy dwell time enables lateral movement – the key to increasing hacker's chances of success. Deception technology helps to detect lateral movement and limit dwell time, so threat actors can't get what they need to progress through the kill chain. Endpoint detection and response platforms, IPS, next-generation firewalls (NGFWs), web application firewalls (WAFs) and Web application deception solution can also be used to facilitate deception initiatives.
- Work with a managed services partner to fill skill gaps – managed security services providers help give an organization the option and flexibility it needs to address constantly shifting regulatory requirements and threats. By monitoring IT infrastructure and devices at service levels that are customized to meet an organization's goals, they support robust security programs, while allowing organization to retain ownership of organizational policies, incident and change management.
- Prepare for the inevitable with comprehensive incident response plans – A comprehensive incident response plan will enable your organization to respond aggressively to an attack, minimize damage and align defenses to mitigate future intrusions.

18.7.2 Understanding Threats

It is essential to understand the landscape of threats and losses due to threats; efficient mechanism needs to be built into the process to curb the same. The corporation needs to make sure the threats from various communities and sources are tracked and up-to-date firewalls, anti-viruses are installed to continuously monitor the malware. Besides, if a company has to take a totally inside-out approach to business operations, that would rule out all the cloud, mobile, virtual or remote options. Instead, sufficient legacy and backup tools need to be maintained, ensuring that the safety measures are not breached.

Example: Lafourche Medical Group adopts Several Security Measures after an Information Breach

Lafourche Medical Group is an emergency care hospital in Louisiana. Recently the Group noticed that hackers have breached the security and got unauthorized access to the private, protected data of around 40000 patients. The incident resulted due to some employee responding to a spoofed mail. The company took the help of an external investigator. The back ground checking was made vigorous on employees. An IT vendor was appointed to re-evaluate its IT system and a tougher password policy was put in place, and staff were trained on security policies.

Source: https://www.hipaajournal.com/third-part y-phishing-attack-affects-up-to-34862-lafourche-medical-group-patients/, 08-June-2021, Accessed on 11/06/2022

18.8 Steps Involved in Building Information Security in Clouds

Today is the era of cloud computing. Cloud computing refers to a new internet storage technology, wherein it provides cost-efficient and flexible infrastructure to store a large amount of data of any organization. However, there are lots of technical baggage and gaps that exist which need to be addressed before an organization adopts cloud. The existing IT strategy must be reconsidered and possible cloud computing scenarios must be developed.

Following are the steps involved in building information security in clouds:

- Step 1: Good governance and compliance process
- Step 2: Auditing all the operational and business process
- Step 3: Identifying the roles and responsibilities and managing people
- Step 4: Data protection and information security
- Step 5: Enforcement of privacy policy
- Step 6: Assessing all the security provisions mentioned in the cloud applications
- Step 7: Manage security terms in the cloud SLA (Service Level Agreement)
- Step 8: Understand the fine print and the requirements from a company perspective to exit the process.

Example: Enforcement of Information Security Practices at a Cloud-Enabled Oil Firm

KCA Deutag is a major multi-national oil and gas services company. It operates from around 100 sites in 25 countries employing 9,000 staff. The company lays emphasis on safety in its operations. Since the operational sites are in some very remote parts, keeping hardware at such locations and sending data to centralized database for analysis was not a good idea. The company looked at a unified cloud Security approach so that there is no need for bringing all data to one central place from the remote locations. This should enable the company to enforce security policies in a consistent manner irrespective of the location of end points or end users. The company started inspecting as much traffic from endpoints as possible and implement more granular controls.

Source: https://learn-umbrella.cisco.com/case-studies/kca-deutag-customer-story, 06-January-2021, Accessed on 11/06/2022

Check Your Progress - 5

9. Which of the following is the sequence of steps involved in building information security in clouds?

    a. Enforcement of privacy policy, Auditing operational and business process, identify the roles and responsibilities and managing people, understand the fine print and the requirements

b. Auditing operational and business process, Identify the roles and responsibilities and managing people, Understand the fine print and the requirements, Enforcement of privacy policy

c. Identify the roles and responsibilities and managing people, Enforcement of privacy policy, Understand the fine print and the requirements, Auditing operational and business process

d. Auditing operational and business process, Identify the roles and responsibilities and managing people, Enforcement of privacy policy, understand the fine print and the requirements

e. Auditing operational and business process, Enforcement of privacy policy, Identify the roles and responsibilities and managing people, Understand the fine print and the requirements

10. What does SLA stand for?

a. Service Level Agreement

b. Source Lease Agreement

c. Service Lending Agreement

d. Service Level Arrangement

e. Systems Level Agreement

18.9 Summary

- Information security is an important activity of an organization so that the interests of all the stakeholders are protected. A proper policy document has to be framed to ensure transparency and consistency in adopting the information security policy throughout the organization.
- The valuation of the organization enhances with a robust information security system as it gives added confidence in the organization among all the stakeholders.
- The new era technology calls for cloud storage to have additional features to secure the information of an organization. However, one should not forget that if the information is stored outside the organization, it is certainly vulnerable to attacks unless managed properly.
- There needs to be an information policy document in an organization for effective monitoring and implementation of the ISMS (Information Security Management System). New automated systems improve the ISMS and cloud storage and computing is fast picking up across all industries.

18.10 Glossary

Access Control: It is a methodology by which availability of the information is restricted by way of authorization processes like passwords and other security checks. This ensures authorized personnel can only have access to any information.

Confidentiality: Is a characteristic that applies to information. To protect and preserve the confidentiality of information means to ensure that it is not made available or disclosed to unauthorized entities. In this context, entities include both individuals and processes.

Information Security Continuity: Refers to an integrated set of policies, procedures, and processes that are used to ensure that a predefined level of security continues during a disaster or crisis (when disruptive incidents occur or adverse situations exist). Continuity is achieved by identifying potential threats and vulnerabilities, by analyzing possible impacts and by taking steps to build organizational resilience.

Information Security Management System (ISMS) includes all of the policies, procedures, documents, records, plans, guidelines, agreements, contracts, processes, practices, methods, activities, roles, responsibilities, relationship, tools, techniques, technologies, resources and structures that organizations use to protect and preserve information, to manage and control information security risks, and to achieve business objectives. An ISMS is part of an organization's larger management system.

18.11 Self-Assessment Test

1. Explain the conceptual framework of information security governance.
2. How does one protect against an external threat to information security?
3. Describe the process of monitoring and measuring an information security program.
4. Mention the steps involved in building information security in the cloud.

18.12 Suggested Readings / Reference Material

1. Rodney Heisterberg and Alakh Verma (April 2022). "Creating Business Agility: How Convergence of Cloud, Social, Mobile, Video and Big Data Enables Competitive Advantage," Narrated by Stephen Graybill.
2. Jonathan S Walker (2021). Social Media Marketing For Beginners - How To Make Money Online: Guaranteed Strategies To Monetizing, Mastering, & Dominating Any Platform For Your Brand, JW Choices.
3. Barry Connolly (2020). Digital Trust: Social Media Strategies to Increase Trust and Engage Customers, Bloomsbury Business.
4. Seema Gupta (6 August 2020). Digital Marketing McGraw Hill; Second edition.
5. Tracy L. Tuten, Michael R (15 June 2020). Solomon et al, Social Media Marketing, SAGE Publications Pvt. Ltd; Third edition.
6. Paul Martin Thomas Erickson (2019). Social Media: Usage and Impact, Global Vision Publishing House, 2 edition.
7. Steve Randazzo (2019). Brand Experiences: Building Connections in a Digitally Cluttered World, Paipen publishing.

18.13 Answers to Check Your Progress Questions

1. (d) **Defining IT security principles, Accountability and action, responsibility of the Board of Directors**

   Information security governance includes defining core IT security principles, accountability rules approved by the board of directors.

2. (a) **Authentication**

   It is the process of verifying the user credentials such as User Id and Password.

3. (d) **Asset Protection**

   It is the protection of information assets from loss or unintended disclosure, and resources from unauthorized and unintended use.

4. (a) **Information security policy**

   IS policy is a high-level document, which includes principles and rules.

5. (b) **Malicious code**

   Trojans, virus, internet worms and spy programs are examples of malicious code.

6. (e) **Implement the policy with measures**

   While all the other four options are called security policies, implementation with measures is not defined in that stream.

7. (b) **ISO:27004**

   It specifies monitoring and measuring of Information Security Measurement model.

8. (c) **Information Security Management System**

   ISMS stands for Information Security Management System.

9. (d) **Following are the steps involved in building information security in clouds**

   Auditing all the operational and business process, Identifying the roles and responsibilities and managing people, Enforcement of privacy policy and understand the fine print and the requirements from a company perspective to exit the process.

10. (a) **Service Level Agreement** (SLA)

    SLA is a set of rules and guidelines for service conditions and termination rules to be followed by the participating partners.

SMACS (Social, Mobile, Analytics, Cloud, and Security) Technologies for Business

Course Structure

Block 1: Introduction to Digitization	
Unit 1	Introduction to SMACS (Social, Mobile, Analytics, Cloud, and Security) Technologies for Entrepreneurship Development
Unit 2	Social Networking Platforms and Stakeholders
Unit 3	Product Development Using Social Media
Unit 4	Customer Relationships through Social Media
Block 2: Mobile Technologies for Business	
Unit 5	Mobile Devices and Platforms
Unit 6	Mobile Operating Systems
Unit 7	Mobile Apps for Business Organizations
Unit 8	Mobile Business Process Management
Block 3: Business Analytics	
Unit 9	Decision Making Using Big Data
Unit 10	Handling Unstructured Data
Unit 11	Data Analytics for Top Management Decision Making
Unit 12	Business and Marketing Intelligence Using Analytics
Block 4: Cloud for Business	
Unit 13	Cloud Architectures and Services
Unit 14	Enterprise Systems Development Using Cloud Technologies
Unit 15	Clouds for Social Marketing
Block 5: Security Technologies for Business	
Unit 16	Data Security in Organizations
Unit 17	Network Security in Organizations
Unit 18	Information Security in Cloud Environment
Block 6: Applications of SMACS	
Unit 19	SMACS Applications to Top Management
Unit 20	SMACS for Marketing
Unit 21	SMACS for Operations