IT409- IT Security and Policies

Assignment No. 3 includes chapter 7,8 and 9

Due Date: 6th April, 2016 (Wednesday, 11:59 pm)

Total Marks: 10

Important Instructions:

1. *This is an individual work, so make sure it is your own: express yourself in your own words in a precise and concise manner*
2. *Search the book or other resources to have a better understanding of the questions.*
3. *Use 'Word Processor' to answer the questions.*
4. *Submission must be through the submission folder set by your instructor on Blackboard, no email submissions will be accepted.*
5. *Late submission or plagiarism will result in ZERO mark.*
6. *This assignment worth 5 marks of the total course mark.*

Question No. 1

Explain how clear desk and clear screen policy is important to protect the confidentiality of company-owned data. **[2 mark]**

Answer

Documents containing protected and confidential information are subject to intentional or accidental unauthorized disclosure unless secured from viewing by unauthorized personnel when not in use. The same holds true for computer screens. Companies have a responsibility to protect physical and digital information both during the workday and during non-business hours. All too often, organizations make it *easy* for unauthorized users to view information. Unauthorized access can be the result of viewing a document left unattended or in plain sight, removing (or reprinting) a document from a printer, copier, or fax machine, stealing digital media such as a DVD or USB drive, and even ***shoulder surfing***, which is the act of looking over someone's shoulder to see what is displayed on a monitor or device.

Protected or confidential documents should never be viewable by unauthorized personnel. When not in use, documents should be locked in file rooms, cabinets, or desk drawers. Copiers, scanners, and fax machines should be located in non-public areas and require use codes. Printers should be assigned to users with similar access rights and permissions and located close to the designated users. Users should be trained to retrieve printed documents immediately. Monitors and device screens should be situated to ensure privacy. Password-protected screen savers should be automated to engage automatically.

Users should be trained to lock their screens when leaving devices unattended. Physical security expectations and requirements should be included in organizational acceptable use agreements.

Question No. 2

What is the difference between Data Replication and Data Backup? Where Backed-up or replicated data should be stored? **[2 mark]**

Answer

The impact of malware, computer hardware failure, accidental deletion of data by users, and other eventualities is reduced with an effective data backup or replication process that includes periodic testing to ensure the integrity of the data as well as the efficiency of the procedures to restore that data in the production environment. Having multiple copies of data is essential for both data integrity and availability.
Data replication is the process of copying data to a second location that is available for immediate or near-time use. ***Data backup*** is the process of copying and storing data that can be restored to its original location. A company that exists without a tested backup-and-restore or data replication solution is like a flying acrobat working without a net.

Backed-up or replicated data should be stored at an off-site location, in an environment where it is secure from theft, the elements, and natural disasters such as floods and fires. The backup strategy and associated procedures must be documented.

Question No. 3

What are the advantages and disadvantages of default deny model and default allow model? Give at least 3 properties of each model. **[3 mark]**

Answer

Model	Default allow	Default deny
Advantage	Easier to deploy	Secure
disadvantage	No security	Difficult to deploy
Properties	1. Access, not explicitly forbidden, is permitted 2. Easier to deploy, 3. works out-of-the-box, 4. No security	1. Access, not explicitly permitted, is forbidden 2. Difficult to deploy, 3. Access is unavailable by default until the appropriate control is altered to allow access 4. Secure

Question No. 4

Firewall rule sets use source IP addresses, destination addresses, ports, and protocols.

1. Describe the function of each.

2. What is the purpose of the following rule?

Allow Src=10.1.23.54 dest=85.75.32.200 Proto=tcp 21

3. What is the purpose of the following rule?

Deny Src=ANY dest=ANY Proto=tcp 23 **[3 mark]**

Answer

1. Source IP addresses: Specify a Source IPv4 address to apply for this rule,

Destination addresses: Specify a Destination IPv4 address to apply for this rule,
Ports: Specify a Port number used in this rule such as 21, 80 and 1025, there is two kinds of port number, privilege number less than 1024 and non privilege greater than 1024.
Protocols: Specify the name of the used protocol or service such as FTP, TCP, UDP etc.

2. Allow Src=10.1.23.54 dest=85.75.32.200 Proto=tcp 21

Allow the permission of the protocol TCP using the port number 21 between source IP address equal to 10.1.23.54 and IP source destination equal to 85.75.32.200.

3. Deny Src=ANY dest=ANY Proto=tcp 23

Deny the permission of the protocol TCP using the port number 23 between any source IP address and any IP source destination.