Linnéuniversitetet
Kalmar Växjö

1DV700 - Computer Security

Assignment 4

Task 1 individual Report

rq222ah@student.lnu.se

Author: Rashed QAZIZADA
Area: Computer Science
Supervisor: Ola Flygt
Course code: 1DV700
Semester: Autumn 2020

Abstract

This page was intentionally left unchanged.

Keywords

Place your keywords here

Contents

1 Information

This report summarize chapter 12, 13 and 14 of the IEC-ISO 27003 INTERNATIONAL STANDARD Second edition 2013-0-01.The ISO/IEC 27002 is an information security that provides best practice recommendations on information security controls. Internationally-recognized standard of good practice for information security.

2 Operations security

Procedures for the operating of equipment should be formally documented and made available as official document to those using the equipment. From the simple procedure of computer use to the use of more complicated equipment, everything should be mentioned in the documents. Any change in the management which effects information security, must be approved by management. These changes include a new system or change in an important business process. For audit purposes, a changelog should be kept. The capacity management actually covers a big part of an organization. It is vital to know how much capacity a system, human resources, offices, and facilities have. Overcapacity of any kind can result in unpleasant situations. Software and hardware exist in different stages on the work floor. Software and hardware can be in development (to make changes) or to improve the operational software/hardware or to create something entirely new. The soft and hardware needs to be tested before operation. To prevent accidental changes in operational environment, both the sections are separated.

Organizations should have controls in place to detect, prevent, and recover from malware attacks. It is important to make all employees aware of the dangers of malware and instructed how to work safely and keep malware out.

A backup policy is a well-known information security measure. A proper procedure for backing up information, software, and system images should be in place. The backups have high importance so they must be properly encrypted. The backups also need to be checked for completeness and whether they actually work.

Event logs are important to keep an eye on what happens in an organization. Most electronic devices can create logs of all user activity which captures any faults, or any security incidents. These logs can be inspected during regular checks and audits. As the logs contain secure information, so they should be properly protected against tampering and destruction. A good way to retain the integrity of logs is to automatically back them up to a location with extreme access controls and requirements. The privileged accounts have access to other logs and the crate their own logs as well. It is important to restrict their access to their own logs by another level of logging system, which cannot be accessed by privileged users. The synchronized clock should be used with all the systems. In this way the activity can be accurately tracked through multiple systems. Management should document how the reference time is chosen and how synchronization is done.

Installation of software on operational systems should be controlled. There should be a documented procedure of how software is checked before installation, and who installs/updates/deletes the software and how, otherwise it may have negative outcomes.

Since it is near impossible to have a system run without any technical vulnerabilities, there should be a proper procedure for discovering them and how to take measures.

Software installed by normal personnel cannot usually be easily controlled, is unsecured and should therefore be capture in a policy. A good way of preventing this is to restrict the access of users so they cannot install software themselves and have IT personnel install it after approval.

Audits might require deep access to a lot of information, which should not disrupt the day to day activities of personnel. To ensure a smooth audit, required access and scope should be approved by management beforehand, and auditors should be given read-only access.

3 Communications security

All networks in an organization should be controlled. To protect information in systems, there should be a proper overview of all networks and how they are protected. Networks could be separated, systems are authenticated and local access to systems, instead of whole network. Service agreements need to be established for all networks, no matter whether the service is provided in-house or from outside. These agreements should state what security mechanisms are in place, what the service levels are, and any requirements set up by management.

Information is shared inside and outside the organization. To lower the risk of information leak, there should be a protocol for all types of information sharing, including digital documents, physical documents, video. Information that is shared between the organization and external parties needs to be preceded by an information transfer agreement. This way, the source, content, confidentiality, transfer medium, and destination of the information transfer is known. There should be a clear and well documented policy for confidentiality or non-disclosure agreements. Different organizations might have different requirements for keeping information confidential, so it is important for organizations to identify, formalize, and update those requirements.

4 System acquisition, development and maintenance

Information systems have different security requirements attached to them, like legal requirements, and compliance with standards or regulations. The requirements should be documented and implemented in new information systems. The public Wi-Fi networks are not trusted, as they can be hacked, until a Virtual Private Network (VPN) software is used. The transactions are the ones which are targeted most. The information involved must be protected against unauthorized reception, re-routing, duplication, or alteration. This can be achieved with encrypted communication path, and electronic signatures of both sides.

Information security starts with safe systems. Rules for safe software and systems development should be documented by an organization and implemented during the development of new software and systems. When the systems are installed in development of organization, change in systems should be formally documented. Organizations should avoid automatic update to critical systems, which may fail the systems. After any change in the systems, their performance and security should be reviewed. Making this a company policy ensures the process is executed consistently and can prevent unnecessary work interruption and risks.

For all the outsource development a thorough agreement should be set up prior to the collaboration, the requirements should be crystal clear. The organization should be able to audit the development process, and deliverables tested before acceptance. During development, the security of the new/updated system should be thoroughly tested. Testing is done best by using realistic test-inputs to the system, and critically assessing the output. There should be a well-documented and strictly applied procedure for the acceptance testing of new/updated systems. The testing itself should be done independently of development and organizational security requirements.

testing should happen in a realistic situation with realistic test data. To mirror real world application and non-sensitive operational data should be used for testing and authenticated before use. Testing should be well documented and logged for auditing, and any operational test data has to be removed after the testing is complete[1].

5 Questions

5.1 The use of equipment is required to be well documented. How the documents are formatted and made available to the employees?

5.2 How well is the capacity management system working in your organization?

5.3 The malware attacks are the ones which are dangerous for any organization. What measures are taken to detect and prevent such attacks.

5.4 To overcome any potential hacker attacks, it is important to have system backups. How often the backups are made and what measures are being taken by your organization to protect the system backups.

5.5 To keep the systems safe, the installation and uninstallation of software should be controlled. What policy is being followed in your organization to control unauthenticated software installation?

5.6 Are all the systems in your organization run on same network?

5.7 In all organizations, the key area at risk is the information as it is being shared at all the time through several mediums. It may be within or outside the organization. What measures are being taken to make sure the information shared is secure and as per the policy?

5.8 The transactions in your organization can be at greater risk. How you are protecting them from any unauthorized attempt to alter them?

5.9 The systems are the important factor in any organization, and they are at greater risk of being malfunction or crash, while updating them. Which protocol is being followed to avoid this issue?

5.10 Do you have well documented agreements with the organizations, which are involved in the development process?

5.11 To test the systems, which testing protocols are being used in your organization?

References

[1] I. 27002:2013(E), “International standard iso/iec 27002,” *Second edition 2013-10-01*, 2013.