**Student Assessment Submission and Declaration**

When submitting evidence for assessment, each student must sign a declaration confirming that the work is their own.

|  |  |  |  |
| --- | --- | --- | --- |
| Student name: **Rashed Hasan.** | | Assessor name: | |
| Issue date (1St Submission): | Submission date (1St Submission): | | Submitted on: |
| In case of resubmission | | | |
| Issue date (1St Submission): | Submission date (1St Submission): | | Submitted on: 30/4/2023 |
| Programme: Higher National Diploma – Cyber Security | | | |
|  | | | |
| Assignment number and title: 1. **Managing Organizational Security** | | | |

* TASK A: Risk Assessment and identification  
  Your company has tasked you with your team to evaluating the level of dedication to information security processes. It is necessary to understand the potential risks to the company's IT security to maintain a secure system. As a result, the team is required to present their findings to senior management.

1. Name a risk table outlining the different kinds of security threats and vulnerability for each risk that can impact businesses.

Answer:

If, Risk Table for Information Security Threats and Vulnerabilities:

|  |  |  |  |
| --- | --- | --- | --- |
| Risk | Threats | Vulnerabilities | Impacts |
| Compliance Violation: Wireless attacks that result in data and information breaches or unauthorized access may result in non-compliance with industry regulations or data protection laws, resulting in fines, penalties and legal liabilities. | Malicious Insiders Employees or contractors with authorized access to the wireless network may deliberately misuse their privileges to launch wireless attacks for personal gain or malicious purposes. | Attackers with malicious intent can exploit SQL Injection vulnerabilities to gain unauthorized access, steal data, or disrupt system operations. | Attackers with malicious intent can exploit SQL Injection vulnerabilities to gain unauthorized access, steal data, or disrupt system operations. |

|  |  |  |  |
| --- | --- | --- | --- |
| Risk | Threats | Vulnerabilities | Impacts |
| Insider Data Leakage | Employees, contractors, partners with unintentional data leaks. | Lack of data loss prevention (DLP) measures, inadequate user training and awareness, improper handling of sensitive data | Unintentional exposure of sensitive data, reputational damage, legal and regulatory penalties, loss of customer trust |
| Unauthorized access | Malicious insider’s human, hackers, social engineering attacks. | Weak or cracked passwords, unpatched and anonymous software, lack of access controls. | Unauthorized access to sensitive and important data, data theft, data manipulation, damage to reputation and the occurrence of losses, legal liabilities. |
| Encryption Weaknesses | Weak encryption algorithms, improper encryption implementation, unsecured transmission of encrypted data. | Use of weak encryption algorithms, improper encryption key management, failure to encrypt sensitive data in transit | Loss of Confidentiality: Encryption weaknesses can result in the loss of confidentiality of sensitive data, exposing it to unauthorized access and compromise. |

|  |  |  |  |
| --- | --- | --- | --- |
| Risk | Threats | Vulnerabilities | Impacts |
| Ransomware attacks can result in significant financial loss due to the costs associated with ransom payments, data recovery, and potential legal liabilities. | Malicious actors and organized cybercriminal groups are the primary threat actors behind ransomware attacks, seeking financial gain by encrypting data and demanding ransom payments. | Unpatched Software and Systems: Outdated or unpatched software and systems can have vulnerabilities that can be exploited by ransomware attacks. | Financial Costs: Ransom payments, costs associated with data recovery and system remediation, potential legal liabilities, and regulatory fines can result in significant financial impacts. |
| Data tampering, in which the attacker can use SQL Injection to modify the data in the databases, which can be deleted or processed, which leads to major problems in data integrity, which may lead to loss of trust from customers, the public, or stakeholders. | Introducing malicious programs and applications Attackers may inject malicious programs and applications into the software supply chain, which may compromise the integrity and validity of the software and lead to unauthorized access or data breaches. | Vulnerable or vulnerable SDKs or repositories: Vulnerable or compromised SDKs or repositories may be exploited by attackers to inject malware or tamper with software components. | Compromised Software Integrity: Software supply chain attacks can compromise the integrity of software and data, leading to unauthorized access, data breaches, tampering, or other malicious activities. |

2. Summarise The security controls that your organization needs to adhere to the risk that been provided in the previous task in order to safeguard its systems against potential risk in the future.

Answer:

|  |  |  |
| --- | --- | --- |
| Threats | Treatment | Solution |
| Employees, contractors, partners with unintentional data leaks. | We develop procedures and methods to respond to incidents that can be implemented quickly in the event of data leakage, in order to minimize damage and prevent further losses. | We put in place access controls to ensure that employees, contractors, stakeholders, and partners who have access to the information, data, or systems necessary to perform their functions and tasks are required to implement them and enforce strong password policies, multi-factor authentication, and regular access reviews to prevent unauthorized. |
| Malicious insider’s human, hackers, social engineering attacks. | Multi-factor authentication MFA requires users to provide two or more types of authentications to enter the system, making it more difficult for hackers to compromise user and employee accounts. | We conduct regular and extensive security awareness training to educate and know employees on how to detect and respond to social engineering attacks, handle them and respond to them. Also, training should include how to identify phishing emails, how to create strong passwords, and how to report any suspicious activity. |

|  |  |  |
| --- | --- | --- |
| Threats | Treatment | Solution |
| Weak encryption algorithms, improper encryption implementation, unsecured transmission of encrypted data. | To update encryption software, applications, and devices regularly and continuously, in order to keep encryption software and hardware updated with the latest security patches and strengthening, as well as updates to address any security vulnerabilities. | Also, to make sure that your company or organization uses strong algorithms, such as RSA, which are strong and secure on a large scale. |
| Malicious Insiders Employees or contractors with authorized access to the wireless network may deliberately misuse their privileges to launch wireless attacks for personal gain or malicious purposes. | We develop a strategic incident response plan that outlines the steps to be taken in the event of a wireless attack. This should include procedures to isolate and immobilize affected devices or networks, identify the source of the attack, and mitigate the damage caused. | Role-Based Access Controls: We use Role-Based Access Controls and instructions to assign different levels of access based on job responsibilities and functions. This will also ensure that employees or contractors have access to the information and resources they need to perform their job duties. |

|  |  |  |
| --- | --- | --- |
| Threats | Treatment | Solution |
| Malicious actors and organized cybercriminal groups are the primary threat actors behind ransomware attacks, seeking financial gain by encrypting data and demanding ransom payments. | To develop an Incident Response Plan by developing an Incident Response Plan that identifies and evaluates the steps to be taken in the event of a ransomware attack. This includes procedures and instructions for isolating and blocking affected devices or networks, identifying the source of the attack, and mitigating the damage and problem caused. | To make backup copies of all important and sensitive data and information on a regular basis, and make sure that backup copies are stored in a safe place so that it cannot be accessed from the main network. |
| Introducing malicious programs and applications Attackers may inject malicious programs and applications into the software supply chain, which may compromise the integrity and validity of the software and lead to unauthorized access or data breaches. | To identify and isolate infected and compromised systems by identifying and isolating any systems that may have been compromised by malicious programs and applications. Which can prevent this malicious program from spreading to other systems and reduce the damage caused by the attack. | SDLC Security: We integrate security into the entire SDLC, from design and planning to testing and implementation. This includes security testing and code analysis tools as well as secure encryption practices and security requirements for third-party software components. |

3. Then set a strategy for evaluating and addressing IT security threats.

Answer:

So, in order to assess the level of dedication and address threats in IT security operations within the company, we must take the following actions:

* That we identify, evaluate and review the current security policies and procedures, and this requires evaluating and reviewing the policies and procedures for network security in order to ensure that they are modern, updated, comprehensive and effective as well, so the effectiveness of these rules and procedures that are followed must also be evaluated as part of this evaluation.
* That we conduct a risk analysis and assessment in order to conduct a comprehensive and complete risk assessment and analysis of the information technology environment and the system in order to discover all potential threats, risks and vulnerabilities, and also a comprehensive examination of the information technology infrastructure, policies and practices of the business must be part of this to ensure the degree of exposure to various risks.
* To conduct staff training and security awareness of the best safety practices, by training and educating employees and conducting regular security awareness trainings for all employees, contractors and partners to ensure that they are aware of potential risks and how to mitigate them. This should include instructions on social engineering, password management, and other relevant security topics.
* That we implement technical security measures, which must protect the company's information technology systems and networks, through technical security measures and matters, including firewalls, intrusion detection and prevention systems, anti-virus programs, malware and encryption.
* We implement a mechanism to monitor and track the information technology environment in order to detect any security incidents or problems in order to respond to them, and improvements must be made based on the changing threats and risks, and this must include monitoring system logs, network traffic, data sources and other relevant information.
* We implement and conduct penetration testing, which entails simulating a real attack on the organization's IT infrastructure to find any vulnerabilities that attackers may exploit, and social engineering methods and techniques must also be used in this test to measure employee knowledge of security risks.
* To conduct and implement continuous review and improvement, and that the information technology security situation in the company and the system must be reviewed and strengthened, so to ensure that security measures are effective and up-to-date, frequent and regular penetration tests, vulnerabilities assessments, vulnerabilities and other security assessments must be included.

Therefore, in a nutshell, to effectively assess and address IT security threats, it is crucial to have a comprehensive and continuous approach and strategy that includes all stakeholders in the company. The strategy should focus on proactive risk management, continuous improvement and updating of systems and IT infrastructure, and a strong culture of security awareness and compliance.

* Task B: Studying issues to find solutions

As mentioned before the organization uses a firewall system, and an anti-virus system, in addition to relying on manual backup services for major databases. Describing the IT security solutions for security issues is one of your main duties related to your position, so you must provide the company with a study about all types of solutions that can be applied to the business to assure the highest security for their systems. In your study you must complete the following:

1. Show how IT security could be compromised by incorrectly set up firewall policies and third-party VPNs.

Answer:

So, by restricting access to and from the network, firewalls are a very important part of network protection and security. However, incorrect and incorrect configuration and setup of firewall rules may lead to security gaps, violations, and breaches. Therefore, below are some of the ways through which policies can lead Improperly configured and configured firewall endangers IT security:

* First, improperly implemented or set firewall rules and principles may expose or allow incorrectly configured firewall rules to access unauthorized third parties to the network, for example, if a rule is created or configured to accept any connection from any address. That can leave the network vulnerable to attacks and breaches so configure firewall rules incorrectly, leaving a vulnerability in the system that allows unauthorized access to the network.

Another example, firewall rules may allow traffic from a specific IP address or port that should have been blocked, or they may have mistakenly blocked traffic that should have been allowed. As a result, cybercriminals can take advantage of this vulnerability to gain access to the corporate network, steal sensitive information, or initiate attacks on the organization's system.

* Secondly, the lack of updates to the firewall, in order to be effective, the firewall needs and requires regular and frequent updates, so the network may become open to attacks and new violations if the firewall is not updated routinely and regularly, for example, hackers can exploit vulnerabilities and that to obtain unauthorized access to the company's network and data, bypassing the old and not updated firewall, and this may lead to data breaches, system crashes, and financial losses. Therefore, to ensure that the firewall can successfully defend and protect the network against new and existing threats, regular upgrades are essential. These updates may include software patches, firmware updates, and rule modifications that take into account the latest security practices. Organizations may improve network security and reduce the risk of cyberattacks by maintaining an updated firewall.
* Third, insecure protocols, so some VPN networks use insecure protocols that are easy to hack and exploit, so for example the PPTP protocol is known as the point-to-point tunneling protocol, and it is well known for being insecure, vulnerable and easily hacked, PPTP protocol contains which was once commonly used contains a number of vulnerabilities that hackers could take advantage of. Attackers can obtain sensitive data, including usernames, passwords, and confidential information, by intercepting and decrypting the PPTP connection.
* Fourth, data leakage, if the third-party VPN is not properly set up and configured, this may lead to sensitive and important data leakage, which may expose sensitive and important data to the company at risk and lead to great losses, for example if the third-party VPN is not properly set up and configured to Restricting access to certain areas of the network, so that an attacker may be able to access sensitive and important information and use it for malicious purposes. Therefore, it is important to ensure that the external VPN is configured and set up correctly by conducting regular and frequent security audits to identify any vulnerabilities or any potential security threats.

**2. Exhibit an illustration of how a DMZ, static IP, and NAT can enhance network security by giving an instance for each.**

Answer:

**Demilitarized Zone (DMZ):** It is a section or part of the network that is used to separate or isolate the servers that can be accessed from the Internet from the rest of the internal network, and often the DMZ is placed between the internal network firewall and the external firewall, so the company may make sure that any Potential security breaches are limited within the DMZ and do not spread to the internal network by placing servers that can be accessed from the Internet, for example such as web servers or email servers. These servers can be accessed via the Internet, but a DMZ is used to separate them. on the company's intranet. As a result, if one of these public-facing servers were compromised, the attacker would only have access to the DMZ's network section rather than the entire internal network of the organization.

**Static IP:** A static IP address is an IP address that is manually assigned to a device permanently or statically as an address on the Internet. It acts as a unique identifier for the device connected to the Internet, since it is easier to monitor network activity and identify potential threats and risks when using a static IP address, and this can be done by further improving network security. For example, if a company sets up or implements a VPN in order to enable remote access to its internal network, the VPN server will also be assigned an IP address to ensure it is easily identified on the network, making it easier to monitor and protect it from potential breaches and attacks. Assign a static IP address to a server that hosts websites and also provides email and database services.

**NAT (Network Address Translation):** It is a process that enables and allows an IP address to represent a group or a number of devices connected to the network in one IP address, and that NAT can enhance and improve network security by hiding the IP addresses of the internal network from the Internet, so it makes it difficult for Attackers target specific machines The primary purpose of NAT is to maintain the number of public IP addresses used, for security and economic purposes. For example, corporate NAT may be used to allow multiple machines on the internal network to share a single public IP address. By making it more difficult for attackers to locate IP addresses for specific devices, it can help improve the defences of the internal network against targeted attacks and abuses.

In general, and briefly, DMZ, static IP, and NAT are very important parts that can be used to improve network security, and also through the implementation of these solutions, companies or organizations can protect their networks better and better, and also to reduce risks and security breaches.

**3. Negotiate three advantages of integrating network monitoring systems and support your points with justifications.**

Answer:

Network monitoring systems provide and enjoy things and many important and necessary advantages for companies in order to manage networks and institutions effectively and with high efficiency. Therefore, there are some advantages, including:

* The network monitoring systems work and monitor and check the network in search of any problems and alert the information technology staff as soon as possible and immediately with any concerns or threats, and this helps and facilitates the information technology staff to search and find problems and fix them as soon as possible, which can save the simple problem From becoming a bigger problem that may affect the company's operations, for example, the failure of the equipment in the company is costly, dangerous and takes a long time, which may disrupt the company's operations and lead to large financial losses. Therefore, by using network monitoring systems, time may be reduced for work resulting from malfunctions Devices, and in the event of a problem, you can identify the main problem and its root cause as soon as possible, in a jiffy, solve it, and resume operations as soon as possible.
* Also, network monitoring systems work to improve efficiency and effective productivity by providing visibility and nature of operations at work. Information technology staff can easily find out where resources are being used more efficiently and efficiently through detailed reports, as well as identifying areas where resources are wasted and misused. Therefore, IT staff can monitor the network for months, hours, days and weeks without manually checking each device. For example, the network monitoring system can identify network devices that use excessive bandwidth, such as video streaming, etc., which alert information technology staff, which helps reduce network congestion and helps improve the overall performance of the network with high efficiency, in order to ensure that employees have access to network resources. They need to do and perform their jobs efficiently, and also network monitoring systems can automate many and many routine network management tasks, which frees and gives time for IT staff to focus on issues and carry out important tasks that are more complex and require their expertise, and this helps improve efficiency and productivity with high effectiveness Finally, it may allow IT staff to spend more time brainstorming and achieving goals in strategic initiatives that promise and contribute to the company's achievement of its goals and new ideas.
* Network monitoring systems work and reduce operational costs by helping IT staff notify and detect problems and threats before they occur, and by monitoring network traffic, IT staff can identify potential problems before they become major problems, which helps network monitoring systems prevent Stop and reduce the need for costly and time-consuming repairs. Network monitoring tools may also help IT teams plan network capacity and allocate resources by giving real-time visibility into network activities, which can save expenses in the long run. Network monitoring technologies can help companies save money overall and stay competitive in an increasingly interconnected and complex business environment. For example, if an employee modifies or deletes files by mistake, the IT staff can find out who did it by taking action to prevent further damage.

**4. Assess at least three physical and virtual security measures that aim to maintain the CIA triad standards of information systems, with a particular focus on "Integrity," and provide critical feedback. (Note: your answer must be detailed research).**

Answer:

CIA stands for Confidentiality, Integrity, and Availability. These three principles make up the CIA's Trinity the CIA's Trinity provides a framework for evaluating its application and implementation of information security procedures to protect the availability, confidentiality, and integrity of information assets.

**Availability** means and indicates that information and systems are always available and effective for authorized users, when they need it, without interference, interruption, or downtime, which is important for companies and organizations that rely on technology to conduct their operations. Which is one of the basic and important principles of the three for information security, along with confidentiality and integrity.

**Physical methods:**

Environmental controls: They are physical procedures and instructions that give devices and systems a stable environment and a stable and secure infrastructure. They are physical methods that guarantee the availability of the system, and this requires taking measures and steps to protect devices and systems from environmental damage, such as controlling humidity and temperature and filtering the air.

**Technical methods:**

Load balancing: It is a method through which workloads are divided among several servers or systems. Load balancing is a technological technique that guarantees availability, which prevents any system from working beyond its capacity, allowing others to take over if one of them fails or breaks down. For example, incoming web traffic can be split across many web servers.

It refers and means **confidentiality** in information security, which is preventing unauthorized access to or disclosure of sensitive information, which means that only authorized individuals or systems can access, view or use the information.

**Physical methods:**

Locks and Access Controls: Physical locks and access controls can be used for you to restrict access to physical areas that store sensitive data for example, a secure data centre can have only a select few doors that can be opened with a smart card or biometric verification.

**Technical methods:**

Firewalls: through which it can be used to restrict access to networks as well as systems, thus ensuring the protection of sensitive and important information and data from unauthorized access, in order to prevent unauthorized access attempts, which checks firewalls for incoming and outgoing network traffic. A network firewall can also be used, for example, to protect a corporate network from external threats or breaches of the company or organization.

**Integrity** indicates that it means preserving and protecting data and information from deletion, modification or change from unauthorized third parties, which ensures that the data remains accurate, complete and consistent over time, and that it is also not subject to manipulation, corruption or changes from unauthorized third parties.

**First, preventing unauthorized modification of data:** which means and refers to the process of preserving and ensuring that data and information remain unaltered or altered by unauthorized persons, individuals, or processes.

**Physical methods:**

Restricted access to physical storage media that contain data and information: This method or physical approach includes restricting people or individuals from accessing storage media that contain sensitive and important information and data, which can limit and restrict the company from accessing the area where it wants devices. Physical storage, server rooms, or data centers, to which access is limited to authorized persons only, including information technology staff or security officers.

**Technical methods:**

Encryption of data to prevent unauthorized modification during movement or rest: Encryption can be used to protect data and information from change and modification from unauthorized parties, whether in transmission or at rest, and also includes encryption of data using encryption techniques and algorithms by converting plain text data into a format It is unreadable and can only be decrypted by individuals or persons who have the correct decryption keys. Also, this can prevent and block unauthorized persons or individuals from modifying, changing or manipulating data while it is being sent or transmitted over the network or while it is stored on a device, even if the unauthorized person has access to the data or information, he will not be able to read it Without decoder available.

**Secondly, the matter of discovering the unauthorized modification or change of data and information** is extremely important in order to maintain the integrity of the data and the security of the information, so let us clarify that we have developed physical and technical methods in order to discover the unauthorized modifications:

**Physical methods:**

Installing physical security measures such as security cameras, alarms, or motion detectors in data and information storage facilities can help detect unauthorized modification of data. So these procedures act as a deterrent which gives and provides evidence in the event of a breach which also enables security cameras to take snapshots of anyone tampering or tampering with data while alarms can notify and alert security personnel or police authorities in the event of a breach. In addition, physical access controls can also be used to prevent unauthorized access. For example, the use of debit cards, biometric authentication, or other access mechanisms that restrict access to data storage areas can help prevent unauthorized modification

**Technical methods:**

Digital signatures and checksums that are among the technical methods through which they can be used to ensure the integrity of data and information in order to discover unauthorized modifications, so digital signatures are electronic signs that are used to verify the validity of data and information and to ensure that they are not Tampering with or manipulating it, the data is encrypted and a unique signature is produced that is difficult to forge through digital signatures using encryption methods. If any changes are made to the data, the digital signature will be changed, indicating that it has been modified.

And by creating a distinctive value that matches the contents of the data, the checksums are a phrase or refer to mathematical or mathematical operations that are used to confirm the validation of the data, and algorithms are used that take into account the size and content of the data in order to calculate the checksums that will change the value of the checksum if any is made Modifications or manipulation of data This indicates that the data has been changed.

It is also one of the technological methods and methods that identify and stop unauthorized modification attempts and prevent them, using intrusion detection and prevention systems (IDPS). IDPS systems also operate and use a variety of technologies, such as analyzing network traffic, monitoring user activity, and detecting anomalies in system behavior in order to identify potential threats and prevent any unauthorized modifications before they occur.

**Thirdly, recovery from unauthorized data change or modification** is an important aspect in order to maintain data integrity and availability. Therefore, there are some physical and technical ways to recover from unauthorized modifications:

**Physical methods:**

Regular data backups to storage locations that are offline or off-site, such as servers, can help to ensure that data is not lost or lost in the event of an unauthorized modification. Backups can also be used to restore data to its original state in In the event that the breach causes data loss or exposure to danger, so to protect it from being affected by the same breach that led to the loss of primary data, backup copies can be made regularly and kept in secure locations outside the site.

**Technical methods:**

The implementation of disaster recovery plans also helps to ensure that data can be recovered in the event of any unauthorized modification or breach. Disaster recovery plans specify the necessary actions to be taken in the event of data loss or breach, which includes this strategy. Or the plans are to determine the cause of the breach or threats in order to isolate the affected systems and restore data from backups such as cloud computing.

**Plagiarism**

Plagiarism is a particular form of cheating. Plagiarism must be avoided at all costs and students who break the rules, however innocently, may be penalised. It is your responsibility to ensure that you understand correct referencing practices. As a university level student, you are expected to use appropriate references throughout and keep carefully detailed notes of all your sources of materials for material you have used in your work, including any material downloaded from the Internet. Please consult the relevant unit lecturer or your course tutor if you need any further advice.

**Student Declaration**

|  |
| --- |
| **Student declaration**  I certify that the assignment submission is entirely my own work and I fully understand the consequences of plagiarism. I understand that making a false declaration is a form of malpractice.  Student signature: Rashed Hasan. Date: |