IT Security Internship Assignment questions/answers by cleantech solar(may 2025)

1. Explain the key components of an effective IT security policy. Draft a basic IT security policy for a small organization

Ans- # it's strategic plans

it defines the scope of security and outlines the objective and frameworks

it outlines the goals

it defines the functional areas

assign the role and responsibilities to every employee of an organisation

#identify and manage risks levels

#policy related to identity and access management, which also includes access controls

#if policy exists then it must exist in types like issue-specific, system- specific and organisation specific policy

incident response plan

penalities & concequences for violating the policy

policy related to human error and emails handling(because most attack occurs because of email phishing.)

- Basic IT security policy for small organization

Goal –to safeguard company asset and defend against cyberattack

Scope- applies to all employee and third party users

Policy highlights

- No use of keyboard and on-screen keyboard for writing passwords, instead use virtual keyboard to protect against keyloggers
- Policy for identity and access management
- Store sensitive data on cloud or isolate storage
- Report suspicious emails link and attachment
- Use of antivirus software and firewall is must
- Do not install unauthorized software

violation of these policy may lead to disaplanary action, including termination

2. How would you identify and assess security risks in an organization's IT infrastructure?

Provide a brief example

Ans - # most high chances for risk occur through network security so my first attempt will be to make network secure firewalls, IPS and IDS

emails and social media sharing –most attacks are initiated through phishing emails, links and attachment, social media can be used a tool for information gathering

#human-error – is one of the main reason for security related risks occur because of human errors like using outdated software and outdated firmware in hardware could be the main reason for attacks

#software and hardware based attacks – software based malware like spyware, adware,rootkit , logic bomb, backdoor, ransomware and for hardware use of outdated system or unpatch could be high vulnerable to attacks

#iot device threats – iot based attcks is common these days because, iot is nothing but embedded computer with internet access can adversary use these as an intermediate for initiating attacks

#lack of patches in security update and use of older versions of firmware

#guided media is much secure then unguided media so use of Ethernet more than wireless network security

Eg – if all employee us their own device, that could be the reason for security breach and data leak

Sol- if organization use their own device with access controls

3. List and explain three risk mitigation strategies that can be implemented to protect organizational data

Ans- #Lack of updation of security patches & use of older firmware –this is the current and main reason due to which attack occurs. Because no security patches will be in high vulnerability for attacks to occur and older firmware can be hacked easily with an attack to if these can be managed by regular updates and using latest hardware then most attacks will be reduced

#defense in depth and layered approach – by using multiple layer of security approach by increased security by data redundancy will protect the integrity of

the data with layers like- administrative controls, physical controls and at last technical controls

- Admininstrative controls –use of policies and procedures
- Physical controls –installing cameras and security guards
- Technical controls –use of software and hardware for security like antivirus software, firewall etc

#use of encryption & antimalware software with (signature based detection)encryption is a great way to make data unreadable to the users who doesn't contain the decrypting key and software that contains signature based detection will help detect malware easily

4. Describe the steps you would take if you detected a potential security breach in the organization.

Ans – step-1 my first step will be towards ensuring the data protection because information protection is priority

Step-2 second step towards not letting it spread through networks and other systems as it can cause more damage

Step-3 quickly I will report the breach and aware employee about the breach and the damage it can cause

Step-4 give strict instruction to employee,what they need to do

Step -5 backup and storage, what if we ain't able to stop the security breach, so it's imp to ensure we must have a copy of data

Step-6 review and make sure breach less likely to happen in future

5. What are the top 3 emerging cybersecurity threats in 2025, and how should an organization prepare for them?

Ans - # deepfakes & voice clone mechanism with AI

Preparations-least posting of information on social media and allow only known uses, and keep information of company and person confidential

#phishing through mails, calls, text and other means with integration of AI

Preparations-auto detecting tools for phishing and education employee about the danger of phishing links and attachments

#supply chain threats of third party vendors

Preparations- vendors risk assessment

6. How would you use Microsoft Intune to enforce security policies on employee devices?

ans- # device compliance policy –access control and block suspicious devices or jailbreak device

#monitor of user activity through device

#automatic deletion of company data if device gets stolen or lost

#conditional allowance –block access of non-complaint devices

7 What security features in Microsoft 365 can help protect sensitive business data? Provide examples.

Ans –#data loss prevention –it prevent data loss and prevent data from leaving the organization

#email protection from phishing and malware

#automatically saving important documents

#secure score, a dashboard that recommends actions to improve security

8. Outline a plan for conducting a basic security audit for a mid-sized company

Ans –checking vulnerability of system, software, hardware and network

#assessment of physical security and network security like firewall, ips and ids

define audit scope and objective

#gather information –network topology, software, password

#identity and access management controls

#identify and mitigate risks and provides solution

#checking updates and patches, if applied to security

9. What tools would you use to perform a vulnerability assessment, and what key factors would you report on?

Ans –Nessus –for network velnerablilty scanner

Openvass-opensource scanner

10. What is an IDS (Intrusion Detection System)? How is it different from an IPS (Intrusion Prevention System)?

Ans –intrusion detection system (ids)-is a network threat detection tool, which is used for network security with firewall, IDS has it's two types host based ids and network based IDS

#it's different from IPS because IPS blocks and prevents threats in real time and on the other hand IDS monitors and alerts threat but but dosen't block or prevent them

11. Describe how firewalls contribute to IT security. What are the common firewall rules you would configure?

Ans-firewalls are tools, in a form of software or hardware,which is used for network security

#main purpose

- Monitor and controls incoming and outgoing network traffic
- Prevents unauthorised access

Common rules for firwewalls

1-allow incoming traffic from HTTP/HTTPS to port 80/443 for web service

2-block all incoming except secure shell from port 22

3-allow dns for name resolution

12. Compare two security software solutions and recommend one for an organization. Justify your choice.

Ans-# bit-defender gravityzone – AI powered detection, patch management,end-point security

#Mc Afree total protection-web-security,cloud security

Recommendation-bitdefender gravityzone because of enterprise level, it's good AI based detection, end-point security and uses signature based detection

13. Design a short security awareness training module outline for employees. What topics will you cover?

Ans –topics

#introduction to IT security

#basic human errors and phishing emails

#all do's and don't for security topics

#problems with too much sharing on social media

#no clicking on suspicious link and harmful attachment that may cause harmful hardware

#don't pick up unknown number or random vedio call from unknown people

#no use of public wifi and public computer

#do safe browsing by only surfing https on port 443 with padlock, and use of private browser and proxy to be safe from cookies.

#be aware of common malware like –spyware and adware

#common social engeneering tactics attackers use to deceive people

USES- vedios, quiz and real- life case studies

14. Give an example of how you would collaborate with the IT or HR department to ensure security compliance.

Ans-work with HR

to ensure That all employee sign the policy assignment while onboarding

#regular training with IT is shedhuled

15. Create a basic incident report template that could be used when a security event occurs.

Ans-

Date of incident- Time of incident - Reported by – System affected- Description of incident -

Initial impact -

Damaged cost-

Action taken -

Root caused identified-

Preventive measures implemented

Lesson learned

Summit by-

Date-