Lab #4: Assessment Worksheet

Part A – Perform a Qualitative Risk Assessment for an IT Infrastructure

Course Name: IAA202

Student Name: Dang Hoang Nguyen

Lab Due Date: 30 May 2023

Overview

The following risks, threats, and vulnerabilities were found in an IT infrastructure.

Scenario / industry vertical given: **Healthcare provider under HIPPA compliance law**

1. Given the list, perform a qualitative risk assessment by assigning a risk impact/risk factor to each of identified risks, threats, and vulnerabilities throughout the seven domains of a typical IT infrastructure that the risk, threat, or vulnerability resides.

1	Unauthorized access from public Internet	Lan-to-wan Domain	Critical
2	User destroys data in application and deletes all files	System/Application Domain	Critical
3	Hacker penetrates your IT infrastructure and gains access to your internal network	Lan-to-wan Domain	Critical
4	Intra-office **employee romance gone bad**	User Domain	Minor
5	Fire destroys primary data center	System/Application Domain	Critical
6	Service provider SLA is not achieved	WAN Domain	Minor
7	Workstation OS has a known software vulnerability	System/Application Domain	Major
8	Unauthorized access to organization owned workstations	Workstation Domain	Major
9	Loss of production data	System/Application Domain	Critical
10	Denial of service attack on organization DMZ and e-mail server	Lan-to-wan Domain	Major
11	Remote communications from home office	Remote Access Domain	Major
12	LAN server OS has a known software vulnerability	Lan Domain	Critical
13	User downloads and clicks on an unknown workstation browser has software vulnerability	User Domain	Major
14	Mobile employee needs secure browser access to sales order entry system	User Domain	Minor
15	Service provider has a major network outage	Lan Domain	Critical
16	Weak ingress/egress traffic filtering degrades performance	Lan-to-wan Domain	Critical
17	User inserts CDs and USB hard drives with personal photos, music, and videos on organization owned computers	User Domain	Minor
18	VPN tunneling between remote computer and ingress/egress router is needed	Remote Access Domain	Major
19	WLAN access points are needed for LAN connectivity within a warehouse	Lan Domain	Minor
20	Need to prevent eavesdropping on WLAN due to customer privacy data access	Lan Domain	Major
21	DoS/DDoS attack from the WAN/Internet	WAN Domain	Major

2. For each of the identified risks, threats, and vulnerabilities, prioritize them by listing a “1”, “2”, and “3” next to each risk, threat, vulnerability found within each of the seven domains of a typical IT infrastructure. “1” = Critical, “2” = Major, “3” = Minor. Define the following qualitative risk impact/risk factor metrics:

“1” Critical – a risk, threat, or vulnerability that impacts compliance (i.e., privacy law requirement for securing privacy data and implementing proper security controls, etc.) and places the organization in a position of increased liability.

“2” Major – a risk, threat, or vulnerability that impacts the C-I-A of an organization’s intellectual property assets and IT infrastructure.

“3”Minor – a risk, threat, or vulnerability that can impact user or employee productivity or availability of the IT infrastructure.

User Domain Risk Impacts:

- Risk: Weak Passwords
  - Impact: 3 (Minor)
- Threat: Social Engineering
  - Impact: 1 (Critical)
- Vulnerability: Untrained Staff
  - Impact: 2 (Major)

Workstation Domain Risk Impacts:

- Risk: Unauthorized Access to Workstations
  - Impact: 1 (Critical)
- Threat: Malware
  - Impact: 2 (Major)
- Vulnerability: Outdated/Unpatched Software
  - Impact: 2 (Major)

LAN Domain Risk Impacts:

- Risk: Insider Threats

    - Impact: 2 (Major)
- Threat: Hacking
    - Impact: 1 (Critical)
- Vulnerability: Misconfigured Firewall
    - Impact: 2 (Major)

LAN-to-WAN Domain Risk Impacts:

- Unauthorized access from public Internet:
    - Critical
- Hacker penetrates your IT infrastructure and gains access to your internal network:
    - Critical
- Denial of service attack on organization DMZ and e-mail server:
    - Major

WAN Domain Risk Impacts:

- Risk: Data Breach During Transmission
    - Impact: 1 (Critical)
- Threat: DDoS Attacks
    - Impact: 2 (Major)
- Vulnerability: Lack of Encryption
    - Impact: 2 (Major)

Remote Access Domain Risk Impacts:

- Risk: Insecure Remote Access
    - Impact: 1 (Critical)
- Threat: Unauthorized Access

    - Impact: 2 (Major)
- Vulnerability: Weak Authentication Methods
    - Impact: 2 (Major)

Systems/Applications Domain Risk Impacts:

- Risk: Data Loss
    - Impact: 1 (Critical)
- Threat: Ransomware
    - Impact: 2 (Major)
- Vulnerability: Lack of Access Controls
    - Impact: 2 (Major)

Lab Assessment Questions

1. What is the goal or objective of an IT risk assessment?

- The objective of risk assessment is to prevent, analyze evaluate the potential risk that can be harm to the CIA triad and define how the risk should be managed, mitigated, controlled when confronting

2. Why is it difficult to conduct a qualitative risk assessment for an IT infrastructure?

- The risk assessment base on qualitative is used when it takes less time and money by hiring experts from this field to analyze in order to get the result fast. But it has one drawback is that, these analyze all base on the expert's experience. Although quantitive risk assessment take more time, but it has conduct the number, more easy to analyze

3. Identify a risk mitigation solution for each of the following risk factors:

User downloads and clicks on an unknown e-mail attachment – Restrict user from downloading, if user has permission to download email attachment, if it's a office file, check for VBA macros, or simply check it hash

Workstation OS has a known software vulnerability – Keep the OS up-to-date

Need to prevent eavesdropping on WLAN due to customer privacy data access – Using some encryption such as AES, using WPA2 instead of WPA

Weak ingress/egress traffic filtering degrades performance – Using firewall, enhance it filtering section

DoS/DDoS attack from the WAN/Internet – Using firewall, IDS/IPS such as barracuda

Remote access from home office – Secure VPNs

Production server corrupts database – have a backup database, if the server corrupts database, we will turn on or typically run two databases parallel