Table of Contents

[Introduction 2](#_Toc7091574)

[TASK 1 2](#_Toc7091575)

[TASK 2 4](#_Toc7091576)

[TASK 3 6](#_Toc7091577)

[TASK 4 8](#_Toc7091578)

[TASK 5 8](#_Toc7091579)

[Conclusion 8](#_Toc7091580)

# Introduction

Escape is a privately-owned Holistic retreat established in 2002 and is currently booming with significant amount of increase in workforce. The manager is pleased with the growth but feels uncomfortable about security. Due to increase in cyberattacks, the company now needs a redesign with good security measures taken.

# TASK 1

a) It is crucial to preserve and secure the data inside a company. Whether it is digital or not, the data needs to be rightfully protected. Below are some of the digital data that needs special attention.

i) Financial System Information

Customers very important financial data are stored in the server. It could be credit card details, transactions, contact information and other volatile data that are sensitive and should be kept absolute confidential.

ii) Network Folders

Network folders contain committee minutes, business policies, procedures and much more. These information are very critical and should be secured carefully.

iii) Customer Record Data

It holds critical data about customer. Standard data such as name, order data, billing information and interaction information being an integral part of them.

iv) Human Resource Information

These data are often used to improve decisions, optimize business and make employees happier. It is something that adds value to the company. If breached by competitor company, the may use it for their own advantage.

v) Learning Management System (LMS) and marketing website

In a market surviving the competition is hard. LMS comprises of information for making the employees be competitive and professional. With this information in competitors’ hand can lead to the downfall of the company. Such applies with the marketing website as well.

b) Below are the security threats that can be addressed for the following assets.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Asset | Threat | CIA | Likelihood | Impact | Risk |
| Financial System Information | Employee Theft | CI | Low | High | Medium |
| Scanning Vulnerabilities and exploiting | CIA | Low | High | Medium |
|  | SQL Injection | CIA | Medium | High | Medium |
| Network Folders | Man in the middle attack | CI | Medium | High | Medium |
| Employee Theft | CI | Medium | High | Medium |
| Distributed Denial of Service | A | Low | Medium | Low |
| Customer Record Data | Employee Theft | CI | High | Medium | Medium |
| Scanning Vulnerabilities and exploiting | CIA | Low | High | Medium |
| Human Resource Information | Employee Theft | CI | Medium | High | Medium |
| Marketing website & LMS | Distributed Denial of Service | A | Low | Medium | Low |
| Server Failure | A | Low | Medium | Low |

# TASK 2

a) The presented threat to the assets can be avoided using the following measures.

**External**

One of the toughest threats to avoid is DDOS attack. Acronym for Distributed Denial of Service, here the attacker produces an immense amount of requests from multiple sources; more than enough request that the server cannot process, consequently, shutting down the server. Marketing website is vulnerable to it as it globally accessible.

The financial data that are stored is susceptible to SQL injection. SQL injection is a type of attack that plays with the database queries, modifies it and cracks it. Confidential financial data can be fetched through this attack.

With the growing age of internet, spywares and spams are a common thing now. With the vast internet, employees are unaware of many software, plugins, extensions and others that may cause threat to the system.

**Resolution**

Marketing website should use free ‘proxy servers’ like *Cloudflare* to prevent against DDOS attacks. Proxy server absorb all the heat generated saving the main server hosting the website. Cloudflare does the job with *zero charges.* Talking about the financial system, one way to protect it is by making the fundamentals strong i.e. using strong statements in the software. But of course, that is not enough. An additional firewall is a must add. Upon purchasing appropriate licenses, it can work as proxy, IPS, anti-spyware, anti-virus and much more. Access list in the firewall can be written to prevent unauthorized access. Proxy server in the firewall is handy to prevent against SQL attacks.

Spams can be eliminated to certain extent by raising the *DMARC*, *DKIM* and *SPF* values in the values. Also, a brief training should also be given to the staffs.

**System**

All the information are stored in server. Once it goes down, the availability is absent. Due to it the productivity of the company can significantly reduce.

**Resolution**

In the server, all the information are stored in drives; *hard drives*, *tape drives*, *solid state drive* or other. Once the drive fails, all the information is gone. So, it is important to have another drive as a redundant drive for redundancy. RAID is a fantastic invention made for it. Talking about redundancy, it applies for the whole server, fans and power as well. A regular check up should be done for the lights of the server. Lights indicate the condition of the hardware. Back Up of data also can be done in case of any data loss.

UPS system can also be added to protect against power surges and black out.

**Internal**

According to a report carried out by JYC university, about 75% of the breaches come from inside. A malware is installed by rogue employees in order to steal information. The devices can be freely accessed by the rogue employees. Customer record data, financial data and other data can be stolen.

**Resolution**

Physical access to the network devices should be blocked by implementing the use of racks and biometric security. Firewall ACLs is a must implement to block unauthorized user to access the unintended network. As the PCs of the employees are next to each other, a strong password should be configured.

B and C)

In today’s days and age, security is a major concern. For the purpose of maintaining integrity and confidentiality, it is mandatory to encrypt data. Encryption ciphers the data into non- understandable which can later be deciphered back into readable text when necessary.

Encryptions can be used in different places such as drives, email, web browsing, wifi and storing passwords. Out of many encryption methods and protocols like AES, 3DES, Two fish, WPA, WPA-2, SMTP, IMAP and many others, AES-128 is a recommended encryption protocol for storing data into the drives whereas WPA-2 and SMTP, IMAP are suitable for wifi and email encryption respectively. Securing browsing of the website can be done through HTTPS protocol. Passwords can be stored using *hash function* such as SHA1. Also, wifi should be encypted with WPA-2 so that unauthorized user cannot access the internet.

Encrypting the data means the data cannot be fetched by an unauthorized or cannot be understood by them. AES-128 being a strong protocol is very hard to decrypt the data. Using the right port with the SMPT and IMAP protocols fully encrypts the email send between the *MTA* or *MUA.*

MTA- Mail transfer Agent 🡪 source server transferring the mail to destination server  
MUA- Mail User Agent 🡪 receives the mail from server/ MTA

# TASK 3

z

Fig: *Network Diagram*

As addressed above, proxy server ‘*CloudFlare*’ has been used to protect marketing website against DDOS attack. If a user/consumer sends request to ‘escape.com’ then the *domain registrar* will forward the request to cloudflare. Likewise, different features such as IPS, anti-bot, anti-virus and other blades has been enabled in the firewall. This will prevent against most of the attacks produced from the internet. For the purpose of redundancy, fault tolerance, load balancing and high availability, two of router, firewall and core switch has been added. These are the prime infrastructure of the company so two of each has been added. Networks has been separated for the staff and the visitors. Using ACLs, customers can be blocked to access the staff network or the network with the servers. Also, for the utmost security, only the 10.160.7.0 network can access the servers. DHCP server has been disabled for that network so the user has to manually set the IP to that network. Radius server has been set up for handling and controlling the access points used throughout the building.

If a remote user wishes to access the server, then the user can setup a VPN in their PC and access the network using the VPN.

Following rule/ACL can be added in the firewall for a good control over the network; prohibiting unauthorized access.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Rule | Name | Source | Destination | Action |
| 1 | Stealth Rule | 10.160.7.1/26 | 10.160.7.2/26 | Accept |
| 2 | Stealth Rule | 10.160.7.0/26 | 10.160.160.7.1/26  10.160.7.2/26 | Accept |
| 3 | Stealth Rule | Any | 10.160.7.1/26  10.160.7.2/26 | Drop |
| 4 | Internal Network | 10.160.7.0/26 | Any | Accept |
| 5 | Any to Internal Network | Any | 10.160.7.0/26 | Drop |
| 6 | Staff to others | 10.160.5.0/24 | Any | Accept |
| 7 | Visitors to Staff | 10.160.2.0/23 | 10.160.5.0/24 | Drop |
| 8 | Visitors to internet | 10.160.2.0/23 | Any | Accept |
| 9 | Clean Up rule | Any | Any | Drop |

ACL in this firewall tries to match the rule from top to down order. If a traffic is dropped in the first rule, it won’t live to tell the tale of what happened in another rule. The first rule ensures that the two firewalls can communicate between each other. The second rule ensures 10.160.7.0 network is allowed to access the firewall. The third rule ensures that no one is allowed to access the firewall. 10.160.7.0 is the most privileged network who is allowed to access any network. This is configured in the fourth rule. Fifth rule doesn’t allow visitors or internet to access the internal network. Sixth and eight rule allows staff and visitors to use the internet. Seventh rule drops any traffic generated from visitors to staff network. In case the traffic doesn’t match any rule, it is dropped.

This rule ensures that nobody except the intended personnel is allowed to access the firewall or servers. The visitors can only access the internet and not the all other internal networks. Security is made strict using these rules. Also access to news server can be done via Remote Desktop Connection or VPN.

# TASK 4

For maintaining security at the escape, following important practice can be implemented

1) Install network monitoring tools

Network monitoring tools such as ‘*Nagios’, ‘PRTG,’ ‘Zabbix’* can be used for monitoring traffic and resource utilization. Unusual traffic or CPU usage detection in early stage can save against potential breaches.

2) Checking firewall logs and events

What kind of attacking are often occurring? From what IP and from source is the attack often generated? These things can be viewed and analysed from the logs and event. This feature is usually found in the firewall. Solution steps can be taken accordingly.

3) Filling the entry logs before entering the server room

Users and staff should compulsorily fill some sort of entry form before entering the premises.

4) Update the host-based firewall regularly

New threats come in the market daily. The host-based firewall in every staff should be regularly updated.

5) The password in every staff pc, wi-fi and other devices should be set to strong and should be changed regularly.

# TASK 5

a) There were many devices that was important to use and using it in a intended way and in a best practice was quite a challenge. So, buying less devices but purchasing appropriate license in compatible devices is the decision made. There are complex firewall from vendors such as ‘checkpoint’, ‘sophos’ and other. They good an excellent job working as a IPS, anti-bot, anti-virus within a single device.

b) If the project could be done again, I would definitely search for the different devices that could meet the scenario. There could be cheaper alternatives for the SQL injection protection and a better cheap alternative for the alternative network design. Although the current network is very strong and meets all the security guidelines but the devices could further get merged leaning towards short yet strong network.

# Conclusion

In this way, a very strong and redundant network architecture has been designed for Escape. All the security guidelines has been met and the best practice has been implemented. This network architecture ensures no intruder can break the network and cannot steal any sort of information whatsoever.