Preet Dabhi 10459151

Assignment 1

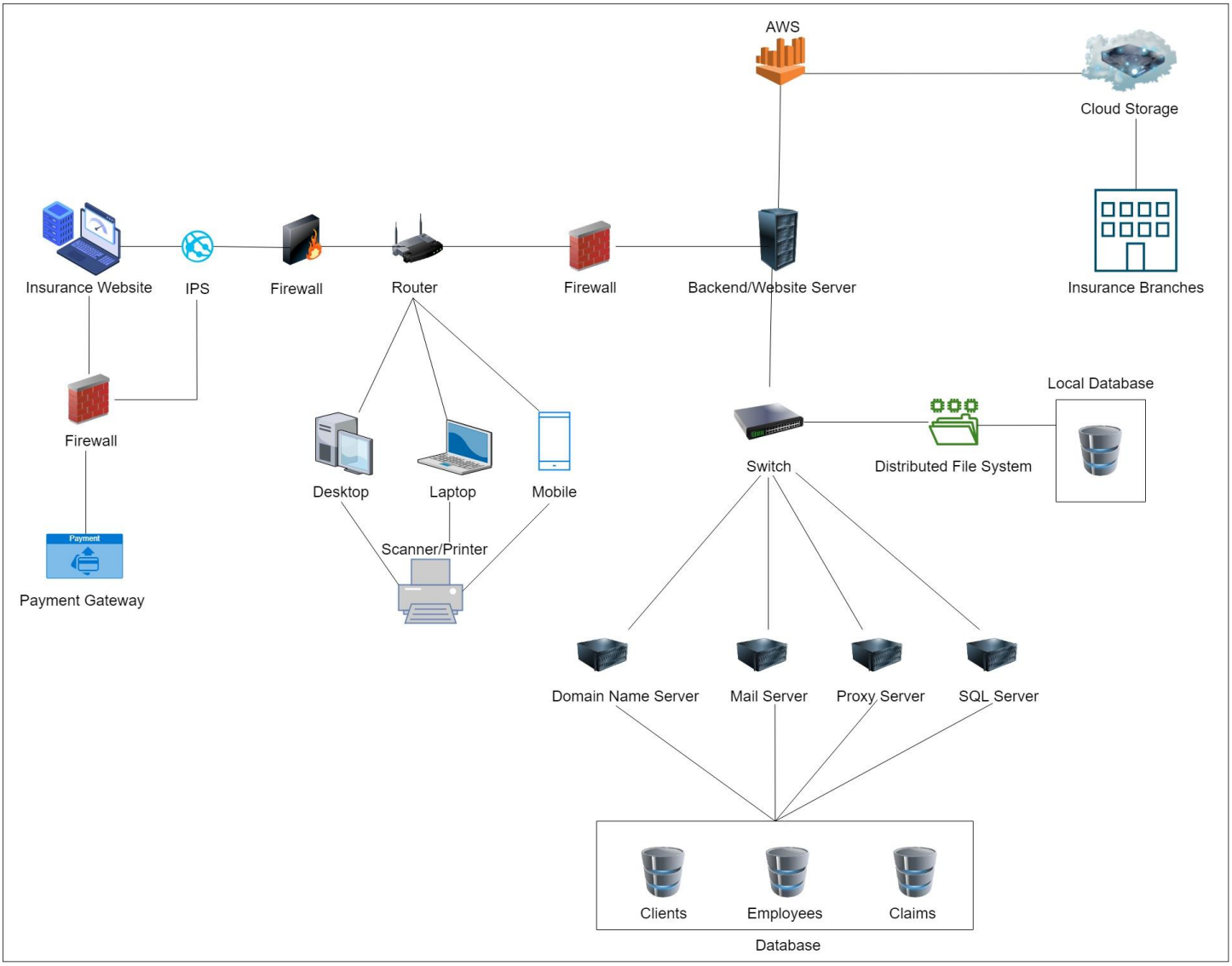
Identify And Describe a Fictitious Enterprise Network (You Can Draw or Describe) And Carefully List the Valued Assets for This Network. (It Would Be Recommended to Keep the Number of Assets More Than 10 But Less Than 25.) Then, Create A Threat-asset Matrix for Your Fictitious Example and Estimate the Security Risk for Each Individual Cell in The Matrix. Write A 1-2 Sentence Justification for Each Risk Estimate. You Are Welcome to Draw the Matrix by Hand (Scan and Cut the Image into Your Paper) Or You Can Use A Tool Such As Excel Or PowerPoint.

P – Probability

C – Consequence

R – Risk (P*C)

Range: 3 - High 2- Medium 1- Low



Fictitious Enterprise Network for Insurance Company

Preet Dabhi 10459151

Threat-Asset Matrix for Insurance Company

Assets/Threats	Confidentiality	Integrity	Availability	Theft/Fraud
Website	P = 3 C = 3 R = 9	P = 2 C = 3 R = 6	P = 1 C = 2 R = 2	P = 3 C = 3 R = 9
Firewall	P = 3 C = 3 R = 9	P = 3 C = 2 R = 6	P = 2 C = 2 R = 4	P = 1 C = 1 R = 1
Switch	P = 1 C = 1 R= 1	P = 2 C = 1 R = 2	P = 2 C = 1 R = 2	P = 1 C = 1 R =1
Website Server	P = 3 C = 3 R = 9	P = 3 C = 2 R = 6	P = 3 C =3 R = 9	P = 1 C = 1 R = 1
Payment Gateway	P = 3 C = 2 R = 6	P = 3 C = 2 R = 6	P = 2 C = 2 R = 4	P = 3 C = 3 R = 9
AWS Cloud Storage	P = 3 C = 3 R =9	P = 3 C = 2 R = 6	P = 2 C = 2 R = 4	P = 3 C = 3 R = 9
DFS	P = 3 C = 3 R = 9	P = 2 C = 2 R =4	P = 1 C = 1 R = 1	P = 1 C = 3 R = 3
Proxy Server	P = 2 C = 3 R = 6	P = 1 C = 1 R = 1	P = 2 C = 3 R = 6	P = 2 C = 2 R = 4
Router	P = 2 C = 2 R = 4	P = 1 C = 1 R = 1	P = 3 C = 2 R = 6	P = 1 C = 1 R = 1
SQL Server	P = 3 C = 3 R = 9	P = 3 C = 2 R = 6	P = 3 C = 2 R = 6	P = 1 C = 1 R = 1
Desktop	P =1 C = 1 R =1	P =1 C = 1 R =1	P = 1 C = 1 R = 1	P = 1 C = 1 R = 1

Explanation

Confidentiality: Protecting the data and various resources from unauthorized viewing and access

Integrity: Making sure that the data is reliable and correct and protecting it from unauthorized access

Availability: Authorized users have access to the systems and the resources they need.

Theft/Fraud: To protect data and services from being accessed illegally.

1. Website

Confidentiality: Banking applications are always the first thing a attacker tries to attack, by using brute force which help them stealing the users information and which gives them unauthorized access to users information.

Integrity: Attacker can make changes to the information which they have achieved and make various transaction to their desired account.

Availability: Most of the web applications are accessed through the cloud and there is a very low chance of the website not being available, even if the website goes down, one can easily create a new instance and the website is back up again.

Theft/Fraud: Insurance company systems are often prone to stealing information to steal money from bank accounts.

2. Firewall

Confidentiality: Firewalls are the first line of defense, they monitor all the traffic of the website and checks for all the requests that are made, if there are any suspicious activities firewall blocks it before making the request, firewalls are most affected during a cyber-attack.

Integrity: There is a high possibility that the attacker might just fake a data packet and a high chance that it will pass through the firewall making the system vulnerable to attacks.

Availability: If there is a cyber-attack or if there is a failure most of the systems have a backup firewall which can be replace with the existing one

Theft/Fraud: Low probability of theft of firewall.

3. Switch

Confidentiality: Switches are used to route different servers to different zones and networks. Switches are do not affect the overall system. It has a low risk

Integrity: Switches just route the requests to different serves, no major effect on the overall system if it is attacked

Availability: There is a low risk of the switch not being available, if it goes down one can use a backup switch or just replace it with a new one

Theft/Fraud: There is a low risk of the theft of switch

4. Website Server

Confidentiality: Website server is where all the requests are sent, and website servers are the ones that get hit the most by the attackers. Web servers monitor all the traffic therefore there is a probability and consequences of attacks are high.

Integrity: Web servers are responsible for accessing the data from the API's and constantly fetching and sending data at the same time it has the data of the user who is using the website

Availability: If a web server is attacked, then the attacker might just shut down the service and this might cause the whole application to do down. This is of high risk

Theft/Fraud: Servers have low risk from information being stolen.

5. Payment Gateway

Confidentiality: Payment gateways are always under the radar of attackers as there are a lot of transactions happening thorough it. It requires a lot of authentication and access to the bank account. Attackers can steal users' payment

Integrity: Payment Gateways require users to enter their own credit/debit card information and it goes through a lot of authentications. Risk is medium

Availability: Payment Gateways are built to handle various payments and services at the same time, it has its own authentication system.

Theft/Fraud: There is a low possibility of it being stolen.

6. AWS Cloud

Confidentiality: AWS cloud is where probably where the application is and a place where the backend server runs, there is a high risk of it being under attack most of the time. If the attacker gets access to it, this can cause a lot of damage

Integrity: Cloud stores multiple copies of data across various places to make sure the data loss or change can be prevented. AWS cloud uses various layers of authentication from accessing that data, however if it goes under attack and the attackers gets access to that data it can cause a lot of damage

Availability: Cloud have the ability to store a large amount of data and one can easily create a new instance if a service goes down

Theft/Fraud: Stealing data from AWS cloud will be difficult as it has its own various levels of authentication

7. DFS

Confidentiality: Data which is used on a temporary basis is stored in the Distributed file system which is local data storage and is difficult to attack

Integrity: Making changes to this is very low because it a temporary storage and will not result in big changes, it is isolated which makes it difficult to get access.

Availability: DFS might run out of storage as it is a temporary storage and might need replacement

Theft/Fraud: There is low risk of it being stolen and medium risk of identity theft

8. Proxy Server

Confidentiality: Proxy servers are used to mask the connection and make the request hidden which is not visible to the ISP, with this we can minimize the chances of getting attacked, but the problem with this is that the request has to be sent to third parties and if they go under attack there is possibility that the user's information can be revealed

Integrity: Attack on the proxy sever could be used to gain unauthorized access to the user's information, however there are low risk of that happening.

Availability: Proxy servers are prone to DoS attack where an attacker tries to send more network traffic to the proxy software than the system can process

Theft/Fraud: There is a low possibility of the server being stolen and medium risk of identity theft

9. Router

Confidentiality: Routers are primarily used for packet transfer and are prone to packet mistreating attack which injects packets with malicious codes designed to confuse and disrupt the router and network.

Integrity: There are chances of unauthorized changes to data, but the risk is low.

Availability: As the routers can go into DDOS attacks there can be a problem in the availability of the router

Theft/Fraud: There are low chances of theft of routers

10. SQL Server

Confidentiality: SQL servers are used to make various operations to the database such as CRUD operations, these servers are hard to reach since they are deep into the system and a lot of authentications is needed to gain its access, however if it is attacked it can cause a lot of damage

Integrity: Once the attacker has access to the database server, they can easily manipulate the data however to gain such access one has to go through a lot of authentications

Availability: Since there are a lot of new users being added to the database there is a need of larger storage more frequently and the server needs to maintained daily and constantly updated and upgraded

Theft/Fraud: Low risk of SQL servers being stolen by attackers

11. Desktop

Confidentiality: Desktop have minimal risk of confidentiality treats as these risks can be because of virus, worm or trojan, it can sometimes give access to user's personal information

Integrity: Medium risk as changes to the Desktop system can have serious consequences

Availability: Probability, Consequences and risk of Desktop unavailability is low.

Theft/Fraud: There is less probability of Desktop being subject to theft.