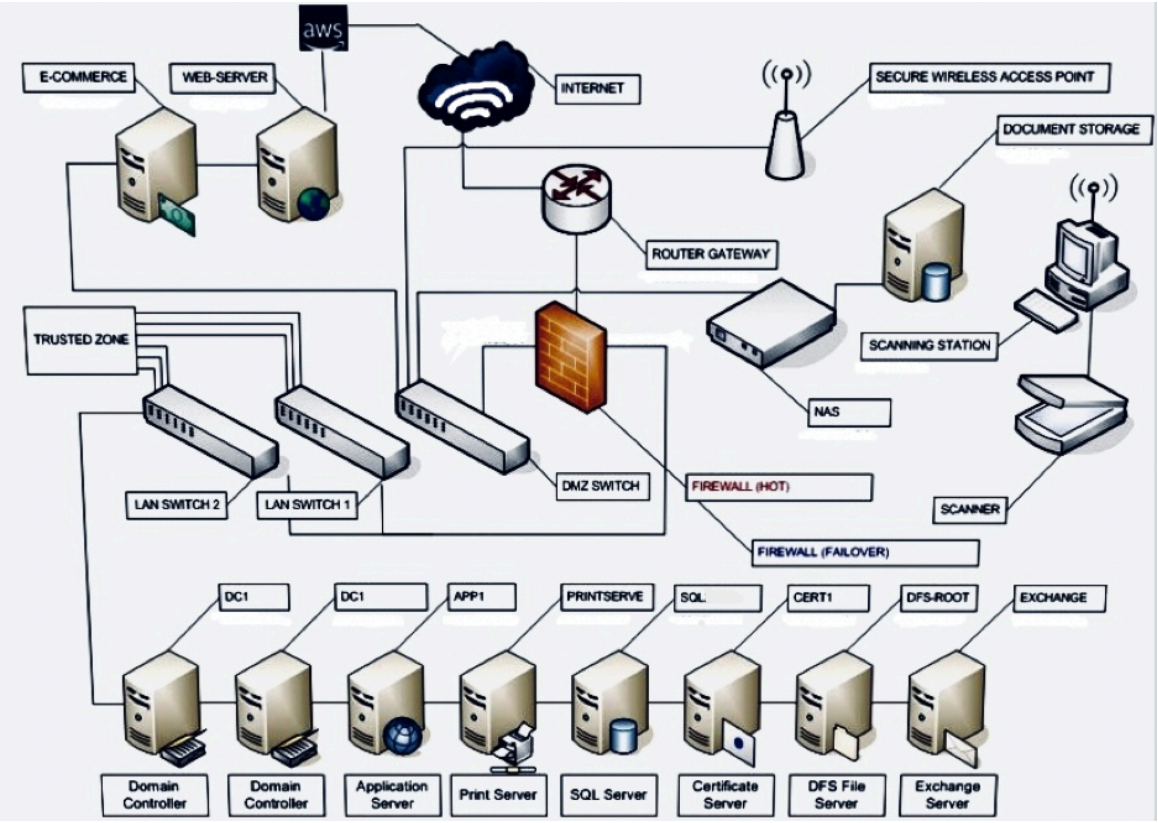
Assignment 1

CS 573 A - Introduction to Cyber Security

Devila Bakrania
CWID: 10457590
Department Computer Science
Stevens Institute of Technology

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.

Fictitious Enterprise Network for E-Commerce Website



Threat - Asset Matrix for E-commerce Website

Assets / Threats	Confidentiality	Integrity	Availability	Theft / Fraud
AWS Cloud	P = 3 C = 3 | R = 9	P = 2 C = 3 | R = 6	P = 1 C = 2 | R = 2	P = 2 C = 2 | R = 4

Assets / Threats	Confidentiality	Integrity	Availability	Theft / Fraud
E-commerce Website	P = 2 C = 3 | R = 6	P = 2 C = 3 | R = 6	P = 1 C = 2 | R = 2	P = 3 C = 2 | R = 6
Web Server	P = 3 C = 2 | R = 6	P = 2 C = 2 | R = 4	P = 1 C = 1 | R = 1	P = 1 C = 1 | R = 1
Firewall (HOT-FAILOVER)	P = 3 C = 3 | R = 9	P = 3 C = 3 | R = 9	P = 1 C = 3 | R = 3	P = 1 C = 1 | R = 1
DMZ Switch	P = 1 C = 1 | R = 1	P = 1 C = 1 | R = 1	P = 1 C = 1 | R = 1	P = 1 C = 1 | R = 1
LAN SWITCH 1	P = 1 C = 1 | R = 1	P = 1 C = 1 | R = 1	P = 1 C = 1 | R = 1	P = 1 C = 1 | R = 1
LAN SWITCH 2	P = 1 C = 1 | R = 1	P = 1 C = 1 | R = 1	P = 1 C = 1 | R = 1	P = 1 C = 1 | R = 1
Router	P = 2 C = 3 | R = 6	P = 1 C = 1 | R = 1	P = 1 C = 1 | R = 1	P = 1 C = 1 | R = 1
Printer	P = 1 C = 1 | R = 1	P = 1 C = 1 | R = 1	P = 1 C = 1 | R = 1	P = 2 C = 2 | R = 4
Scanner	P = 1 C = 1 | R = 1	P = 1 C = 1 | R = 1	P = 1 C = 1 | R = 1	P = 2 C = 2 | R = 4
NAS	P = 1 C = 1 | R = 1	P = 1 C = 1 | R = 1	P = 1 C = 2 | R = 2	P = 1 C = 1 | R = 1
Domain Controller	P = 3 C = 3 | R = 9	P = 3 C = 3 | R = 9	P = 1 C = 1 | R = 2	P = 1 C = 1 | R = 1
Application Server	P = 3 C = 2 | R = 6	P = 2 C = 2 | R = 4	P = 1 C = 1 | R = 1	P = 1 C = 1 | R = 1
File Server	P = 1 C = 3 | R = 3	P = 1 C = 3 | R = 3	P = 1 C = 2 | R = 2	P = 1 C = 1 | R = 1
SQL Server	P = 1 C = 3 | R = 3	P = 1 C = 3 | R = 3	P = 1 C = 2 | R = 2	P = 1 C = 1 | R = 1
Certificate Server	P = 3 C = 3 | R = 9	P = 3 C = 3 | R = 9	P = 1 C = 1 | R = 1	P = 1 C = 1 | R = 1
DFS File Server	P = 3 C = 3 | R = 9	P = 3 C = 3 | R = 9	P = 1 C = 1 | R = 1	P = 1 C = 1 | R = 1
Exchange Server	P = 3 C = 3 | R = 9	P = 3 C = 3 | R = 9	P = 1 C = 1 | R = 1	P = 1 C = 1 | R = 1
Document Storage	P = 2 C = 3 | R = 6	P = 2 C = 3 | R = 6	P = 1 C = 1 | R = 1	P = 2 C = 2 | R = 4
Payment Gateway	P = 2 C = 3 | R = 6	P = 1 C = 2 | R = 2	P = 1 C = 1 | R = 1	P = 1 C = 1 | R = 1
Google Payroll	P = 1 C = 2 | R = 2	P = 1 C = 2 | R = 2	P = 1 C = 1 | R = 1	P = 1 C = 1 | R = 1
Salesforce	P = 2 C = 2 | R = 4	P = 2 C = 2 | R = 4	P = 1 C = 2 | R = 2	P = 1 C = 1 | R = 1
Bank of America	P = 2 C = 3 | R = 6	P = 2 C = 2 | R = 4	P = 1 C = 1 | R = 1	P = 2 C = 2 | R = 4

P = Probability, C = Consequences, R = Risk (P *C)

Range: 3 = High, 2 = Medium, 1 = Low

Four Major Threat Types:

1. **Confidentiality**: Access to sensitive information by attacker
2. **Integrity**: maintaining the consistency, accuracy, and trustworthiness of data
3. **Availability**: Ensuring Services and Data is available and working correctly
4. **Theft/Fraud**: Acquiring Data or Services illegally

AWS:

AWS Cloud solution provides computational platform for system operation

i. **Confidentiality:** The cloud acts like the heart of the entire web application and is always under constant attack, attacks which can have access to a lot of sensitive information causing a lot of damage to the system

ii. **Integrity:** Cloud systems are now advanced to store multiple copies of the same data across the system to make sure the data loss or change can be prevented. They use multiple layers of cryptography to ensure integrity. Although on the off chance when it does happen it can cause a lot of damage to the core of the system.

iii. **Availability:** Cloud systems have the capacity and hardware to store large values of data for longer times and are of low risk for data unavailability.

iv. **Theft / Fraud:** Stealing of AWS services and data from the cloud for illegal use

E-commerce Website:

Actual Website built using Web Technologies like Node, React, etc.

i. **Confidentiality:** Popular E-commerce websites are always under the raider for attacks to steal username and passwords of users and which results in identity theft and false orders.

ii. **Integrity:** E-commerce websites face a lot of Counterfeit products and products with inaccurate information, also fake reviews and prices to scam the legit user.

iii. **Availability:** Since the website and its services are mostly accessed through the cloud the probability of the website being down is quite low and the consequences of it are also moderate because it is very easy to switch the website to a different server and isolate the issue.

iv. **Theft / Fraud:** E-commerce websites often prone to stealing of products without paying

Web Server:

Server used to host the website and to manage the Domain

i. **Confidentiality:** Web servers are the ones which are constantly hit by cyberattacks in order to get in the information and gain access but they do not hold a lot of sensitive information and includes data for the website and other front end services and acts as a gateway to interface with the backend APIs

ii. **Integrity:** Web servers are responsible to fetch and send accurate data to the APIs in-order to display accurate information to the user. An anomaly in this process can directly affects what the user will see on the website.

iii. **Availability:** Web servers are abundantly available by the domain hosts and are constantly switched between to balance load and maintenance.

LAN/DMZ Switch: LAN and DMZ Switch are used to route different servers to different zones and networks and do not necessarily affect the CIA of the overall system

Router / Wireless Access Point:

Routers / WAP work together to transfer data from modems to wireless points and provide internet to different services

i. **Confidentiality:** Routers and WAPs frequently go through ddos and wireless attacks in-order to gain access to the internal network. While all internal servers are connected through LAN and not WAP local users and system can be damaged by such attacks.

ii. **Integrity & Availability:** Routers and WAP are primarily used for packet transfer and routers between wireless systems and do not affect the duty of actually transferring data and receiving it.

Printer / Scanner: Printers and Scanners do not link with the core functionalities of the system and thus are of very low CIA risk. They can however be prone to theft and non-company usage

NAS:

NAS system is a storage device connected to a network that allows storage and retrieval of data from a centralized location for authorized network users

i. **Confidentiality:** Whatever data that is being stored in NAS is local and hence very hard to attack

ii. **Integrity:** Chances of altering data is very low because since it is an isolated device makes changes in the NAS would not affect the online system

iii. **Availability:** NAS may run out of available storage and might need replacement

Domain Controller:

Domain Controllers are responsible for authenticating server requests

i. **Confidentiality:** They are also under constant attack and of high risk because if the DC is compromised the system loses its secure authentication and is vulnerable to attacks

ii. **Integrity:** Domain Controllers require trustworthiness of data and requests and is highly likely to be compromised by cyber attacks.

iii. **Availability:** Domain Controllers are build to handle a lot of requests at a given instance and so their hardware is build accordingly.

Application Server:

Application Servers are used to maintain and manage the operation of different APIs used in the system

i. **Confidentiality:** Application servers are responsible to manage different APIs and to fetch and manipulate data on API calls and require specific authentication tokens and headers to process which can be prone to breaches and attacks

ii. **Integrity:** API calls made to the SQL Servers are at risk when there is data manipulation in the main data frame and can create an ambiguity on the overall consistency of the data.

iii. **Availability:** Application servers are build to sustain large amount of API calls and interfacing across different systems in the organization

File / SQL Server:

File / SQL Server are used to fetch and manage data stored in the Database

i. **Confidentiality:** File / SQL Servers are used to make CRUD operations to the database and although the chance of it to be attacked is low because of how deep rooted within the system it is, once the access is granted it can endure a lot of damage because it would give full data access to the imposter.

ii. **Integrity:** Altering data is fairly easy once the imposter gets access to the File Server but it is very hard to get access because it requires multiple levels of authentication

iii. **Availability:** File servers require more maintenance and constant upgrade and more and more data is added everyday

Exchange Server:

Used to manage various email clients for different users throughout the network

i. **Confidentiality:** Exchange servers are responsible to manage and maintain email and calendar services and requires a lot of privacy and is prone to a lot of attacks

ii. **Integrity:** It is very important to maintain consistency, accuracy, and trustworthiness of data over exchange servers and due to which they are often exploited

iii. **Availability:** Exchange Servers run through an Operating System and are easy to manage and maintain

Firewall:

Firewall is a network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules

i. **Confidentiality:** Firewalls act like the first line of defense and is used to tackle most of the cyber attacks. It is used to monitor all traffic and is also affected the most during a cyber attack

ii. **Integrity:** Data packets which impersonate actual packets are of high chance to pass through the firewall making the system very vulnerable to attacks

iii. **Availability:** At an event of firewall failures most systems also have backup firewalls installed to replace the damaged firewall

Document Storage:

Document storage system is used to receive, track, manage and store documents

i. **Confidentiality:** Document Storage or Data centers are highly secured facilities which store all the data of the system in physical disks. Attacks on such infrastructure usually happens through unauthorized virtual or physical access and can cause a lot of damage and privacy concerns to the whole system

ii. **Integrity:** Data Storage facilities do have checksums and encryption of data but unauthorized access can directly make CRUD operations to the main source of data and thus it is of high risk

iii. **Availability:** Data Storage rigorously maintain all hardware and are always at optimum operation with backups during failure

iv. **Theft / Fraud:** Theft of actual data by physical or virtual unauthorized access by the attacker in their system

Payment Gateway:

A payment gateway is a merchant service provided by an e-commerce application service provider that authorizes credit card or direct payments processing for e-businesses

i. **Confidentiality:** Payment gateways require a lot of authentication and access to the physical card or bank account. Access to these details however will result in payment abuse by the attacker

ii. **Integrity:** Payment Gateways require users to enter their card or bank details which goes through multiple level of authentication and hence is comparatively safe in terms of data integrity

iii. **Availability:** Payment Gateways are build to handle multiple payments at once because they are a whole system by themselves

Google Payroll:

Human Capital Management Software to maintain and manage employee payroll and services

i. **Confidentiality:** Payroll Systems do not directly affect the system and is handled by a different entity and hence are low risk

ii. **Integrity:** Data breach for Payroll will result in employee and company information loss and can be of risk if this data is accessed by the wrong people

iii. **Availability:** Fairly constant Payroll availability

Salesforce(CRM, Customer Data, etc.):

Merchant Software to manage Customer relationship management Data

i. **Confidentiality:** CRM data is very crucial as it includes user data and history and hence is prone to a lot of attacks

ii. **Integrity:** Attackers who have access to Salesforce data can access Website trends and sensitive user information

iii. **Availability:** CRM data is handled and managed by a separate entity and is available as long the company is in contract with the entity

Bank of America(Checking Account, etc.):

Bank service to manage transactions and store money securely

i. **Confidentiality:** Highly confidential and this is where the bank processing and transactions takes place. Bank systems are very secure but also very prone to attacks and are often used to do illegal money transfers when access is gained

ii. **Integrity:** Attackers can change bank information and transactions when if access is gained

iii. **Availability:** Data is always available since it has monetary value

iv. **Theft / Fraud:** Banks are prone to credit card and account frauds