ITNSA Assignment

Noah Lewis
13/09/2021

1.1.

The CIA triad or Confidentiality, Integrity, Availability triad is a security model that's function is to help protect information and security. The three components of the triad act as rules which should be followed in order to ensure that security and privacy are upheld.

When a business is running, using and storing sensitive information such as user data, it is imperative that said information is kept secure so that nobody with unauthorized access can get their hands on it. If this were to happen, the attacker may be able to steal information and use it for personal gain whilst also negatively affecting the people whose information has been stolen. This can then cause the customers of the business to distance themselves from the company as they feel that their information is not in good hands, breaking trust and giving the company a bad reputation.

With this in mind, it is clear to see why the CIA triad is so relevant in ensuring the continual running of a business, especially when businesses store payment information and the like. Each piece of the triad covers different methods for ensuring safety of data and all of them should be upheld for a piece of information to be considered secure.

Confidentiality:

This refers to the business restricting access of information to only those who should have access to it. This helps to prevent unauthorized access to that information and thus keep it private. This rule can be violated by means of cyber attacks which aim to gain unauthorized access to steal or tamper with information.

Integrity:

Integrity refers to the quality and completeness of information. Upholding the integrity of information means ensuring that the data isn’t being tampered with and thus verifying that it is correct, authentic and reliable. Integrity is violated when data is intercepted and changed.

Availability:

Availability of information is the ability to get information when needed. If information is needed but it can't be obtained then there's not much of a point in having the information in the first place. It ensures that everything that needs information gets information, essentially allowing the business to run. Threats to this are things such as DDOS attacks which spam requests to a server, slowing it down and interfering with the process of making data available.

As seen by the examples above, each triad member is essential in thinking about IT security. If any one of these are not upheld, it could cause a threat to the functioning of the business or even cause the business to cease functioning altogether.

1.2.

The AAA model, standing for authentication, authorization, and accounting is a framework for controlling and managing access to computer resources as well as providing billing information when necessary. It is a security service which is usually used to set up access control to the router or access server. This lets things such as what users are authorized to do and what they are accessing to be more easily controlled. This in turn helps to better secure the network and keep the business' network running. This is done by an AAA server which handles user requests for access to

Authentication:

Authentication is the method used to identify users on the network. This can be things such as usernames and passwords for accounts which will provide identified access to the network. The AAA server will check the entered credentials to those stored in the database's active directory and grant access if the user's login details match.

Authorization:

Once the user has been authenticated, they will then need authorization to do certain tasks. If the user issues a command, it is first checked to see if the user has permission to use said command. This can be violated by attackers who gain unauthorized access and are able to do things that they are not authorized to do. This could cause the business to cease functioning until the damage from the attacks has been resolved.

Accounting:

Accounting refers to the resources that a user is consuming while accessing the network, including the amount of time that they spend using the network and the amount of data sent and received. This monitoring of resources is used for billing, resource utilization and trend analysis, all of which are required for business functions.

Each aspect of the framework allows step by step access control and monitoring to ensure that no unauthorized entry is gained. Along with the billing information and analysis functionality, AAA is vital in the secure running of the company's systems. Without these systems in place, the network would be very vulnerable and cause many privacy issues.

2.1.

Defense in depth is a security concept with multiple layers of security controls which are used within an IT system or network. The aim of this strategy is to create many protective layers to create a reliable system rather than counting on a single layer to be 100% reliable.

An example of this would be installing anti-virus software on the computers on the network when there is already virus protection on the servers and firewall. This is called a layered approach because anything getting through a layer will be caught by the next layer rather than getting through only one layer and that issue becoming a wider problem. In this way depth in defence can be considered a countermeasure as it provides redundancy in the event that a security protocol or control fails.

Depth in defense can be subdivided into three distinct aspects, these being physical, technical and administrative. Each of these governs its own ‘layer’ and provides a different approach to securing data.

Physical controls:

These are any physical limitations that prevent access to the network such as guards, fences and security cameras. This means that intruders will need to get past these before attempting to gain access to the system. This acts as a countermeasure for the next security layer that will need to be bypassed in order to gain access.

Technical controls:

These controls are pieces of hardware or software that protect the system's resources. They include things such as encryption, authentication and file integrity software. Hardware controls add features that prevent the access of a system's contents but don't protect access to the physical systems. This makes gaining access to the sensitive data more difficult and acts as a way to safeguard the integrity of the data.

Administrative controls:

Administrative tools are controls which have certain rules and procedures which are followed in order to prevent access to the system. Their job is to ensure that all security regulations are met and include things such as hiring practices, security requirements and data handling procedures. The hiring practices and training of staff also acts as a countermeasure as it ensures that all sensitive data will be properly and securely stored.

With these in place, ity is ensured that the data which is being protected is being done so as effectively as possible. By using layers, the risk of a single point failure is massively reduced.

It also requires a larger variety of tools and skills when gaining access to each layer, making itm much more difficult to do than just getting through one layer with a singular set of tools.

In essence, these layers of defence act to uphold the CIA triad and therefore protect all aspects of the sensitive data. This is done through website protection, auditing systems, network security, behavioural analytics and data isolation to name a few. All of which provide their own unique hurdles to overcome when trying to gain access to restricted data. As such, defense in depth can be considered both a countermeasure and a safeguard for said data.

2.3

Technical documentation of Cisco firewall configuration

Making the topology:

- Place down a firewall, 2 pcs, a laptop, a switch, a router and a DNS server within the Cisco packet tracer.
- The firewall is connected to the router and the router to the DNS server.
- Another connection is made between the firewall and the switch, and from the switch are two other connections, each going to a pc.
- Lastly the laptop is linked to the firewall via the console cable to act as a way to interface and manage the firewall settings.

Assigning IP:

- Click on the laptop, navigate to the desktop and click on the terminal.
- Type “sh runn” to view the default information.
- Then type “conf t” to direct to the config.
- In the terminal type “no dhcp address 192.168.1.5-192.168.1.35 inside”
- This will remove the preconfigured dhcp address.
- Type “conf t” to go to configuration.
- Once in config type “int vlan 1”.
- Then “Ip add 10.1.1.1 255.0.0.0” to replace the default ip.
- ‘No shutdown’ ensures that the component keep running.

Set Internal and External Security Levels on Firewall:

- Security level relates to the inside and outside facing connections.
- A security level of 100 indicates an inside facing connection while a security level of 0 indicates an outside facing connection.
- On the laptop, open the terminal and type “security-level 100” to set the security level to an inside connection.
- Type ”exit”
- “Switchport access vlan 1” to connect to the firewall internally.
- “Exit”
- “Int vlan 2”

- “Ip add 50.1.1.2 255.0.0.0” to add an ip.
- “Security-level 0”
- “Exit”
- “Int e0/0”
- “Switchport access vlan 2” to link the two.

Configure DHCP and DNS ip:

- Click on router and go to CLI.
- Type “n”
- Type “conf t”
- Type “int f0/0”
- Type “ip add 50.1.1.1 255.0.0.0”
- Type “int f0/1”
- Type “ip add 8.8.8.1 255.0.0.0”
- “No shutdown”

- Navigate to the dns server, then to desktop and from there to ip configuration.
- In the IP textbox type “8.8.8.8”
- In the subnet mask box type “255.0.0.0”
- In default gateway type “8.8.8.1”

- Click on the pcs and select DHCP to enable automatic ip assignment by the firewall.
- Then click of the laptop and go to the terminal.
- Type “dhcpd address 10.1.1.10-10.1.1.30 inside” to assign a range of ips.
- Type “dhcpd dns 8.8.8.8 interface inside” to assign the ip for the DNS server.
- The dhcp on the pcs should now automatically receive the ips.

Configuring the default routing:

- Click on the laptop and open terminal.
- “Route outside 0.0.0.0 0.0.0.0 50.1.1.1”

Configure OSPF:

- Click on the router and open the CLI.
- “Router ospf 1”
- “Net 50.0.0.0 0.255.255.255 area 0”
- “Net 8.0.0.0 0.255.255.255 area 0”

Create Object network and enable NAT:

- Go to the laptop and open the terminal.
- Type “object network LanNet”
- “Subnet 10.0.0.0 255.0.0.0”
- This will create the object.
- To configure the NAT type “nat (inside,Outside) dynamic interface”

Create ACL:

- Access the laptops terminal.
- Type “access-list LanToNet extended permit tcp any any”
- Type “access-list LanToNet extended permit icmp any any”
- “Access-group LanToNet in interface outside” which will activate the ACL.

Verify:

- Accessing the cmd on the pc will allow for connection checks to be made using the following command.
- “Ping -t 8.8.8.8”
- Another way to verify is to access the firewalls terminal and type “show nat”
- Finally you can check by typing “show xlate”
- This should give the information needed to ensure that everything is working.

3.2.

SSL stands for secure socket layer and is a way to keep a connection to the internet secure. It encrypts sensitive data that is being transferred between systems so that nobody can eavesdrop or tamper with the information being sent. This connection can be from the client to the server or even just a server to another server.

TLS or transport layer security is essentially an updated version of SSL which is more secure. The first public version of SSL was released in 1995 whereas the first version of TLS was released in 1999.

Both SSL and TLS are cryptographic protocols which authenticate the transfer of data between servers, users and other systems. Both protocols even use certificates to ensure endpoint encryption.

The differences between the two are quite minor besides the fact that one is newer than the other. SSL offers support for cipher suites while TLS does not. Instead TLS uses a standardization process to make defining cipher suites easier. Examples of these are RC4, AES and IDEA. These cipher suites are algorithms that help to keep a connection secure.

SSL has a “No certificate” alert message while TLS replaces this alert with several other alerts.

The record process is also different from SSL and TLS as SSL makes use of message authentication code or MAC when encrypting a message. On the other hand, TLS uses HMAC, a hash-based message authentication system which is used after each encryption.

The handshake process between SSL and TLS are also different in that SSLs hash calculation is made up of the master secret and pad whereas the hashes in TLS are calculated over the message handshake.

Lastly the message authentication is different as SSL message authentication takes key details and app data is ad-hoc while TLS makes use of hash message authentication.

3.3.

Social engineering is a term which covers a wide range of malicious activities, done by humans. These are things such as psychological manipulation which is then used to trick users into making mistakes or to accidentally give away sensitive information.

This can be dangerous to a company as giving away access or information to people who should not be authorized to have them can lead to security issues ranging from minor threats to major major ones. No matter how small a threat, it should be taken with the utmost seriousness as the issue may escalate and cause bigger ones down the line.

For the most part social engineering focuses on getting sensitive information. With this information they are able to do many things, all of which will end up affecting the business in a negative way. The most prominent social engineering tactics are:

- Phishing
- Vishing
- Pretexting
- Baiting
- Tailgating

These tactics allow the intruder to either gain access or information which can be used for malicious purposes. If information such as client banking details and the like are stolen, this poses a major threat to the security of the customers and their finances. This can cause clients to distrust the company as they feel as though their information is not being adequately protected. With this distrust, the clients may choose to distance themselves from the business or even stop associating with the company altogether. This in turn can cause the company to develop a bad reputation for not taking security seriously, hurting not only the functioning of the business but the entire brand as well.

In terms of access being gained by unauthorized personnel, these people may be able to steal information, tamper with systems and disrupt business functionality. Viruses can be installed on the businesses hardware and cause a lot of issues which can be difficult to fix. If access is gained and the business systems are taken offline for a day, the company is not only losing out on revenue but they are also losing customers who would have chosen to use that company to conduct their business.

With this in mind it is clear to see why social engineering poses such a big threat to the functioning of a company. People are not perfect and as such social engineering is a surprisingly effective technique for gathering information.

References:

F5 Labs. 2021. What Is The CIA Triad?. [online] Available at: <https://www.f5.com/labs/articles/education/what-is-the-cia-triad#:~:text=These%20three%20letters%20stand%20for,objectives%20for%20every%20security%20program.> [Accessed 17 September 2021].

Forcepoint. 2021. What is the CIA Triad?. [online] Available at: <https://www.forcepoint.com/cyber-edu/cia-triad> [Accessed 17 September 2021].

WhatIs.com. 2021. What is the CIA Triad? Definition, Explanation and Examples. [online] Available at: <https://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA> [Accessed 17 September 2021].

Arubanetworks.com. 2021. What Is AAA?. [online] Available at: <https://www.arubanetworks.com/techdocs/ClearPass/6.7/Aruba_DeployGd_HTML/Content/802.1X%20Authentication/About_AAA.htm#:~:text=AAA%20stands%20for%20authentication%2C%20authorization,necessary%20to%20bill%20for%20services> [Accessed 17 September 2021].

Etutorials.org. 2021. AAA System Components :: Chapter 3: Cisco AAA Security Technology :: Part II: Securing the Network Perimeter :: CCSP Cisco Certified Security Professional Certification :: Networking :: eTutorials.org. [online] Available at: <http://etutorials.org/Networking/Cisco+Certified+Security+Professional+Certification/Part+II+Securing+the+Network+Perimeter/Chapter+3+Cisco+AAA+Security+Technology/AAA+System+Components/> [Accessed 17 September 2021].

SearchSecurity. 2021. What is AAA server (authentication, authorization, and accounting)? - Definition from WhatIs.com. [online] Available at: <https://searchsecurity.techtarget.com/definition/AAA-server> [Accessed 17 September 2021].

En.wikipedia.org. 2021. Defence in depth - Wikipedia. [online] Available at: <https://en.wikipedia.org/wiki/Defence_in_depth> [Accessed 17 September 2021].

Exabeam. 2021. Defense In Depth: Stopping Advanced Attacks in their Tracks. [online] Available at: <https://www.exabeam.com/security-operations-center/defense-in-depth/> [Accessed 17 September 2021].

Youtube.com. 2021. [online] Available at: <https://www.youtube.com/watch?v=jOYvI6aBVE8&ab_channel=SaurabhITCorporateTrainer> [Accessed 17 September 2021].

En.wikipedia.org. 2021. Virtual private network - Wikipedia. [online] Available at: <https://en.wikipedia.org/wiki/Virtual_private_network> [Accessed 17 September 2021].

Services, P., 2021. What Is a VPN? - Virtual Private Network. [online] Cisco. Available at: <https://www.cisco.com/c/en_in/products/security/vpn-endpoint-security-clients/what-is-vpn.html> [Accessed 17 September 2021].