OPTION #1: Retail Company

Liam Bergerson

CSU - Global

ITS441-1

J. Leaston

11/6/22

OPTION #1: Retail Company

ABC Company currently has five architects, ten programmers, three project managers, and two technicians along with five computers that are being used to house vendor and customer information. In addition to these assets, they have twenty-five store locations with each having a Local Area Network. They wish to move all of their data and applications over to the cloud using Amazon Web Services. They have asked me to evaluate the data security practices of Amazon Web Services to ensure that there is a safe and secure transition. There are multiple threats and vulnerabilities on the cloud that need to be considered throughout the assessment. Multiple methods and tools can be used to prevent exploitation of existing threats and vulnerabilities. There are multiple encryption techniques to choose from that will be used for ABC Company's wireless networks. Cyber attacks are very prominent right now and there are many methods of prevention towards these cyber attacks. Finally there are cloud-specific threats that need to be evaluated to ensure that they are not exploited.

Vulnerabilities on the Cloud

There are many vulnerabilities on the cloud that could result in stolen data from a breach by a threat actor. Misconfiguration of systems can open doors for unauthorized users and allow them to freely roam the network. Misconfigurations can be caused by a lack of knowledge of the cloud interface or a lack of peer review from the DevOps team (Alvarenga, 2022). A more specific cloud

misconfiguration that needs to be addressed is identity and access management. Identity and access management misconfigurations can result in users having access to resources or permissions that they are not allowed to have. This can substantially increase the chance of a breach because the user does not have the proper knowledge to use those resources or permissions securely. Another specific cloud misconfiguration threat has to do with the public data storage, for example, a SQL database on the web. If a SQL database that is tied to a website is not properly secured, it can pose a SQL injection vulnerability that threat actors will exploit. Other misconfigurations can include using Hypertext Transfer Protocol (HTTP) instead of Hypertext Transfer Protocol Secure (HTTPS) and not using the latest version of Secure Sockets Layer/Transport Layer Security (SSL/TLS) (Alvarenga, 2022).

Denial of Service/Distributed Denial of Service (DoS/DDoS) attacks are also two prominent threats on the cloud that need to be evaluated so they do not affect server uptime. DoS/DDoS attacks aim to render a system or a group of systems unavailable. This results in downtime of servers which will cost an organization large amounts of money depending on how long the servers are unavailable. Salam et al. (2015) states that ninety minutes of server downtime results in costs of around $505,500 for an organization. DoS/DDoS attacks flood the servers with an overwhelming amount of packets that will render the servers unavailable because they are trying to process the unnecessary packets and not the necessary packets (Cloudflare, 2022). The main difference between a DoS

attack and a DDoS attack is a DoS attack originates from a single computer whereas a DDoS attack originates from multiple computers. A DDoS attack utilizes a botnet or a group of compromised computers to flood servers with an overwhelming amount of packets. DoS attacks can be easily stopped by blocking packets from that one IP address on a firewall. DDoS attacks are incredibly difficult to stop because packets are coming from hundreds of computers. It's very difficult to block every IP address on that botnet with a firewall.

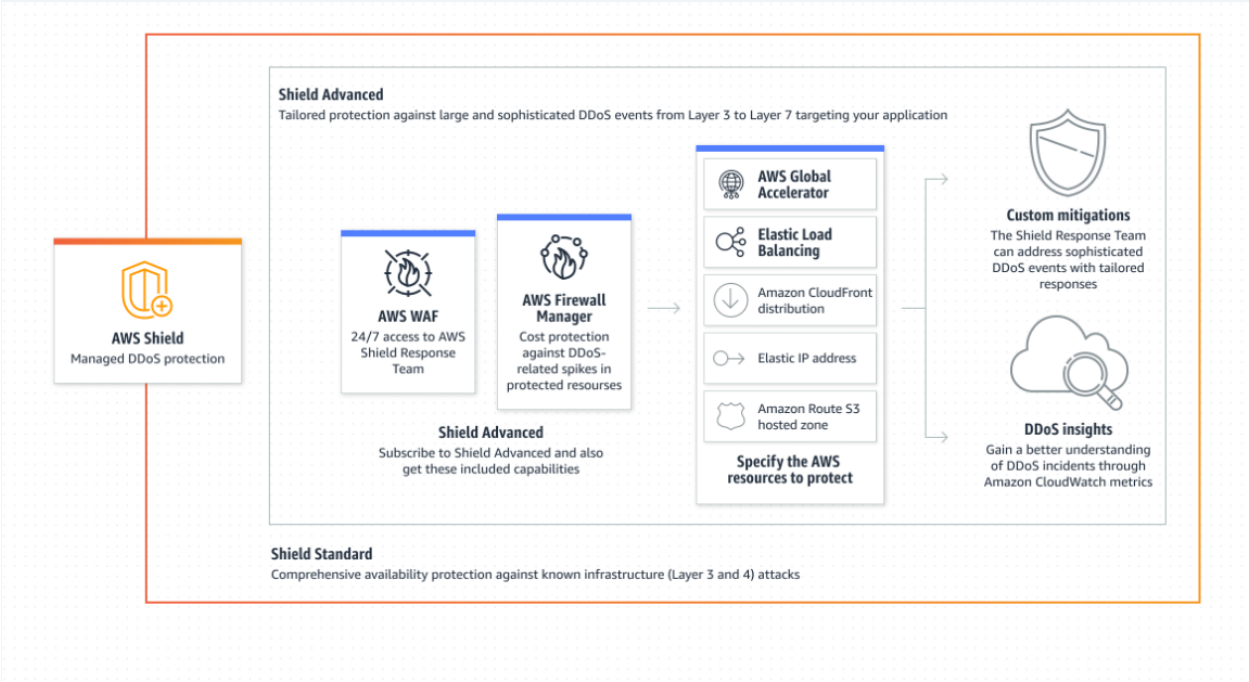
Methods Used to Overcome Security Threats

There are a couple of methods that can be used to prevent the threats discussed above from being exploited by threat actors. Logging practices and frequent auditing will ensure that systems are configured properly. Logging will allow privileged users to review logs and review any changes made (Knobel, 2021). Any misconfigurations that violate any policies or procedures will be spotted from the logs and fixed. Amazon Web Services provide their own logging practices that ABC Company can use to spot misconfiguration of systems so that misconfiguration threats are eradicated.

Frequent audits will expunge the threat of misconfiguration by specifically scanning each system and looking for any misconfigurations that may be exploited by threat actors. Third party tools and organizations can be used to achieve proper auditing and ensure that there is no misconfiguration of systems.

There are a couple of security measures that can be used to ensure that ABC Company does not fall prey to DoS and DDoS attacks. AWS has a built-in

measure against DDoS attacks. AWS Shield is a service that safeguards applications running on AWS against DDoS attacks. The figure below shows an accurate representation of AWS Shield's features.



Note. Adapted from AWS. (2022). *AWS Shield*. Amazon Web Services, Inc. https://aws.amazon.com/shield/

Other measures to prevent DoS/DDoS attacks involve network monitoring, configuring firewalls, and simulating a DoS attack. Monitoring network traffic will ensure that signs of a DoS/DDoS attack are spotted before the service goes down completely (Keary, 2022). By monitoring traffic, actions can be taken the moment unusual data traffic levels or unrecognized IP addresses are spotted. Attackers will usually test the network with a few packets before launching the full attack; that test period is the time that actions must be taken before the service is

taken out by the brunt of the attack. This can be achieved by configuring firewalls properly. In order to block the packets, firewalls must be configured to block repeated packets originating from IP addresses. Certain protocols can be blocked on a firewall that are used to carry out a DoS/DDoS attack such as a SYN flood using the TCP/IP protocol. Finally, simulating a DoS attack can allow ABC Company to create a procedure that can be used in a real scenario when they are being targeted by a DoS/DDoS attack.

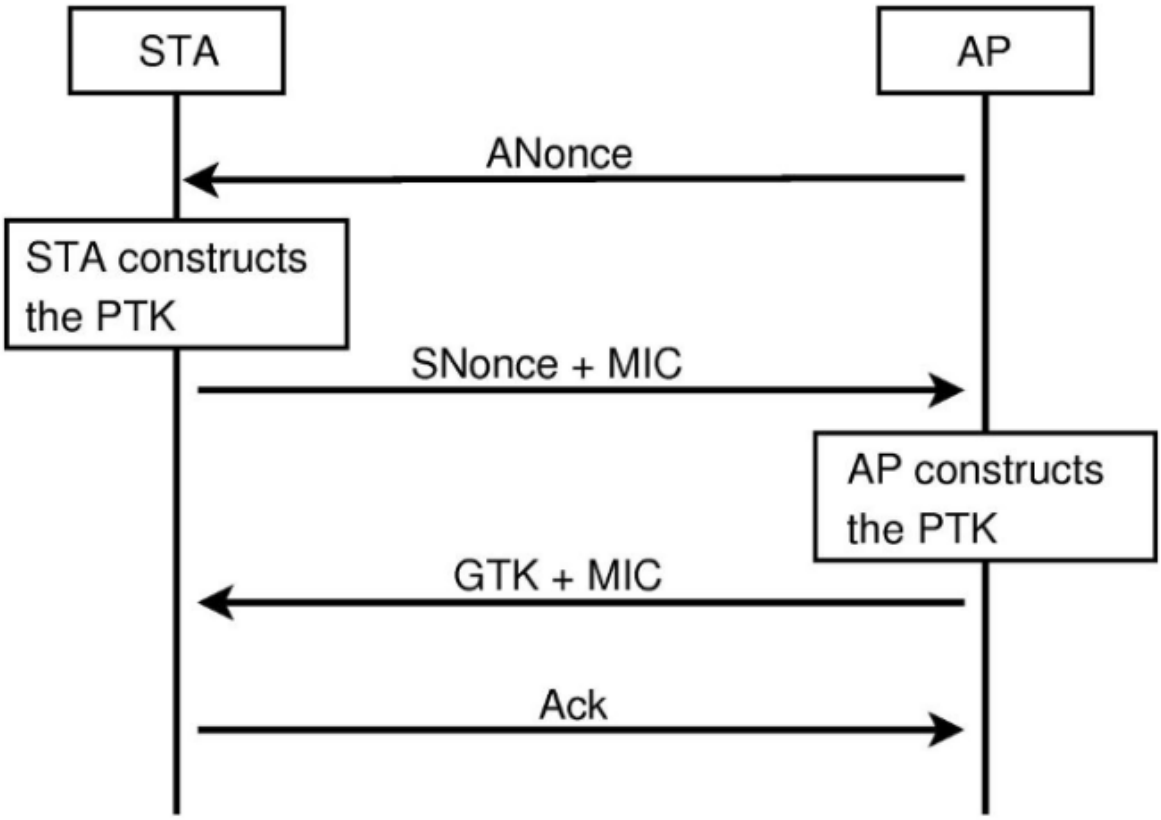
Wireless Encryption Techniques

There are multiple methods of encrypting wireless networks that can be used to protect data being transferred between networks and devices. Currently, there are four methods to choose from, Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 2 (WPA2), and Wi-Fi Protected Access 3 (WPA3) (CISA, 2020).

WEP is the oldest and least secure standard of the four. It uses either a 64-bit or a 128-bit key. What makes this standard weak in regards to security is that this encryption method is not very complex and it's been around for many years. Due to the age of WEP, there are already methods of cracking in place to crack these weak keys.

The second encryption method, WPA, is a slightly better standard in terms of security compared to WEP. It uses a Temporal Key Integrity Protocol as the encryption key. WPA, however, is still relatively easy to crack. Therefore, it is not a secure wireless encryption standard.

WPA2 is more secure than the previous two because it involves a four-way handshake to authenticate into a network protected by WPA2. WEP or WPA did not have this feature which made them both insecure. WPA2 is also secured with the Advanced Encryption Standard (AES). AES can generate key sizes up to 256 bits which will take the attacker a lot longer to manually decipher. The figure below shows the four-way handshake process that WPA2-protected networks use to authenticate a user into the network.



Note. Adapted from Ronder, A. (2021, December 13). The 4-way handshake WPA/WPA2 encryption protocol - Alon Ronder. Medium.

https://medium.com/@alonr110/the-4-way-handshake-wpa-wpa2-encryption-protocol-65779a315a64

The STA is the client and the AP is the access point. The AP first sends a randomly generated number called the ANONCE to the client. The client then generates a Pairwise Transit Key (PTK) which is the encryption for the traffic. The client then sends a randomly generated number to the AP called the SNONCE along with the Message Integrity Code (MIC). The MIC is a way to verify the identity of the client to the AP and vice versa. The AP then generates its own PTK. Then the AP sends the Group Temporal Key (GTK) along with an MIC. The client then sends an acknowledge message to the AP. If the keys match, then the user is authenticated into the network.

The last wireless encryption standard, WPA3, is a new standard. It is more secure than WPA2 because with WPA2, packets can be intercepted when someone authenticates into a network. This will allow the attacker to decipher the packets and easily crack the password. WPA3 has fixed that vulnerability by requiring the user to interact with the wireless access point every time they wish to authenticate into the network. This makes cracking into the network much more difficult and time consuming.

The wireless encryption standard that will be used for the ABC Company's networks will be WPA2. Even though WPA3 is more secure than WPA2, WPA3 is a new standard. For that reason, there aren't many devices that are compatible

with WPA3 as of now (CISA, 2020). Since WPA2 has been out for a lot longer than WPA3, therefore, it is more universal.

Prevention of Cyber Attacks

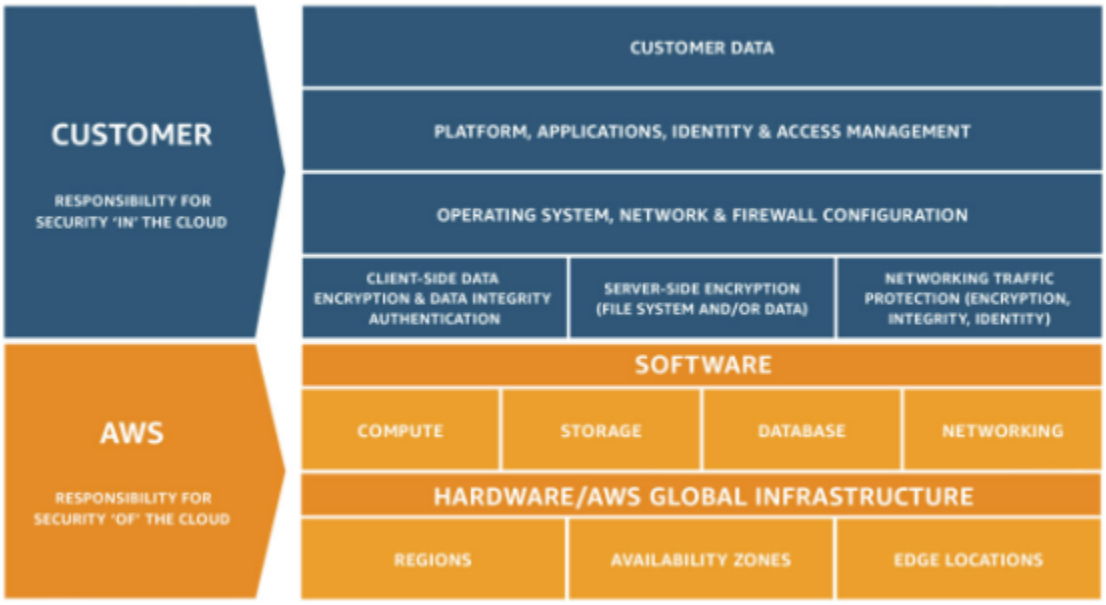
The common denominator that allows most cyber attacks to exploit organizational systems and networks is weak credentials or passwords. If the authentication process can be secured, systems and networks would be better protected against most cyber attacks. The first step is to create strong passwords and change them regularly. WCM (2020) states that passwords must be around sixteen characters long with the inclusion of numbers, upper and lowercase letters, and special characters. For example, a weak password would be “allcowseatgrass”. In order to fortify that password, numbers, upper and lowercase letters, and special characters must be added. For example, the same password but fortified would be “AllC0w$EatGra$$35%”. Passwords must also be changed every ninety days so attackers do not have an indefinite amount of time to crack a password (WCM, 2020).

Multi-factor authentication will be used on ABC Company systems and websites. The goal of multi-factor authentication is to provide an extra layer of authentication security by requiring users to input a randomly generated code before fully authenticating into a system or website. A third party application can be used to generate a random code that can be inputted into a field on the system or website. This will drastically increase the difficulty for threat actors to breach a system. Since the system is secured with a strong password, it will

already take the attacker a long time to crack the password. Now that a code is also required to authenticate into a system, threat actors will be strongly discouraged to breach a system.

Cloud-specific Mitigation Strategies

In order to mitigate cloud-specific risks, the cloud Application Programming Interface (API) must be secured. The cloud API is what facilitates the cloud services. It essentially provides access to the cloud infrastructure and software as a service (Thor, 2019). In order to mitigate any risks that could compromise the cloud API, a strong security model must be implemented, strong authentication must be used, and access control mechanisms must be implemented along with encrypted transmissions. The figure below shows how Amazon Web Services provide a security model that educates the user how proper security is implemented in the cloud.



Note. Adapted from AWS. (2022). *Shared Responsibility Model - Amazon Web Services (AWS)*. Amazon Web Services, Inc. https://aws.amazon.com/compliance/shared-responsibility-model/

In order for strong authentication to be implemented, strong passwords must be used. Similar to what was discussed above, passwords must be around sixteen characters long with the inclusion of numbers, upper and lowercase characters and special characters.

The access control mechanism that will be implemented will be role-based access. Role-based access allows administrators to create roles that have a defined set of permissions and users will be added to those roles according to what job they do. In order for transmissions to be encrypted, Virtual Private Networks will be used with all systems.

Conclusion

In order for the ABC Company to migrate their data and applications to the cloud, a variety of security practices have been evaluated. Practices such as misconfiguration prevention, DoS/DDoS prevention, strong password practices, wireless encryption standards, etc. It's crucial that these security practices be implemented so that ABC Company can have a safe and secure transition of applications and data over to the Amazon Cloud.

References

Alvarenga, G. (2022, August 30). *Top 6 Cloud Vulnerabilities | CrowdStrike*. crowdstrike.com. Retrieved October 2, 2022, from https://www.crowdstrike.com/cybersecurity-101/cloud-security/cloud-vulnerabilities/

CISA. (2020). *Securing Wireless Networks | CISA*. Cisa.gov. Retrieved October 2, 2022, from https://www.cisa.gov/uscert/ncas/tips/ST05-003

Cloudflare. (2022). *What is a denial-of-service (DoS) attack?* https://www.cloudflare.com/learning/ddos/glossary/denial-of-service/

Keary, T. (2022, June 6). *Dos vs DDoS Attacks: The Differences and How To Prevent Them*. Comparitech. https://www.comparitech.com/net-admin/dos-vs-ddos-attacks-differences-prevention/

Knobel, J. (2021, April 1). *Cloud Misconfiguration: What It Is and How to Prevent It*. BARR Advisory. Retrieved October 2, 2022, from https://www.barradvisory.com/blog/cloud-misconfiguration/

Salam, A., Gilani, Z., & Haq, U. S. (2015, January 27). Deploying and Managing a Cloud Infrastructure: Real-World Skills for the CompTIA Cloud+ Certification and Beyond: Exam CV0-001 (1st ed.). Sybex.

Thor, D. (2019, April 30). *Cloud APIs and How to Mitigate the Security Risks*. dzone.com. Retrieved October 2, 2022, from https://dzone.com/articles/cloud-apis-and-how-to-mitigate-the-security-risks

WCM. (2020). *11.15 - Password Policy and Guidelines | Information Technologies & Services*. Weill Cornell Medicine. Retrieved October 2, 2022, from https://its.weill.cornell.edu/policies/1115-password-policy-and-guidelines