Tanner Wale

CYB 250

22EW1

Professor Mark Edwin Carey

Final Project Cyber Defense and Emerging Trends Paper

October 10, 2022

One human factor for personnel is database administrator. A database administrator has a good understanding of an incident response. Also, a database administrator should have strong skills for configuring, maintaining, and troubleshooting the software being used for the database of the organization. They determine the interfaces needed to troubleshoot a ticket. The ticket system is used to track open incidents and provide interfaces for the storage of incident data in the main database of the organization (Lucas & Moeller, 2003). The database administrator has access to all the records and digital evidence that the team collects for the organization (Lucas & Moeller, 2003). Also, they train employees in the management and use of the organization's database systems.

Given the scenario for the headset being in constant communication with the server in the central office of the organization, database administrators would be crucial to control an incident when it occurs. The database administrator would oversee that the headset is in constant connection to the organizations database. They would make sure the headset is configured to send emails, text messages, invoices, and make sure the headset is configured to the server in the central office. Database administrators would also maintain this connection through constant monitoring and logs. Then when a problem occurs, they would have steps as to how to troubleshoot the headset and get it back up and running for the organization.

The human factor rewards of database admins are they install and configure database software for your organization. They also perform ongoing maintenance checks to make updates and patches so there are no vulnerabilities to the network. Database admins also protect organizations' data from unauthorized use.

The drawbacks or risks associated with database admins are they are the first target for hackers because database admins have high level privileges. If your database admin is not aware of the way a hacker can access their accounts through phishing attacks, brute force attacks, dictionary attacks, and social engineering than your organization is at risk by the employee in charge of the sensitive information. Another risk is an insider threat, this threat coming from the database administrator. If the database admin is doing malicious activity like deleting logs or looking at personal identifiable information, it would be hard to know because they could cover their tracks or explain it as an accident (Ekran, 2019).

The emerging trends in database admins cybersecurity landscape are with the online presence of every business as there are now millions of businesses online and growing database admins will have to produce a way to protect all this data on the web. To do this database admins have to get up-to-date patches to not be vulnerable to hackers. When data is taken from hackers there needs to be laws in place to protect database management. Customers of these businesses will want more information about protecting their data, with this information coming from someone in database security. Customers are expecting database admins to produce innovative ways of protecting their vital information and keeping them up to date with the latest to protect their data (iFour Team, 2022). Database admins are responsible for databases as the increase for better security is a need with all the news about hackers infiltrating sensitive customer data. The affect database admins have is on technology, as customers want a new way of protecting information on the web from hackers, that cannot be exploited. To help customers they should train them to gain experience of the vulnerabilities in their network, as someone who does not take precaution to phishing emails or knows they exist is an easier target and a bigger vulnerability them those that do.

One type of technology that protects an organization is encryption. A type of encryption an organization makes effective use of is symmetric encryption. Symmetric encryption is a way to secure data through ciphers. It takes plaintext and turns it into unrecognizable ciphertext. Organizations can use it for large amounts of data blocks as it is faster and more reliable with larger amounts of data. Another use of symmetric encryption is for transactions of payments because of the speed of symmetric encryption it makes it quick and efficient (What Is Symmetric Key Encryption? (Definition and Uses), 2021). Also, this can be used by organizations for making sure users are validated in the organizations for a secure network. Organizations tend to use Advanced Encryption Standard (AES) to keep data confidential. AES has an encryption key of different lengths, known as the secret symmetric key. According to (Crawford, 2019) it took the computational power of the Sunway TaihuLight in China around "885 quadrillion years to brute force a 128-bit AES key."

Given the scenario the data coming from the headset must use symmetric or asymmetric encryption to keep the data confidential to threat actors outside, just as well as inside, as insider threats to an organization have happened. If an organization fails to do this, they will face major consequences such as fines, breaking laws, and losing the reputation of their customers leading to a massive loss of profit. This symmetric encryption with AES could be the best scenario as all this data from technicians in the field is being sent back to the server located in the central office of the organization. The organization must take crucial steps to keep this data confidential as it has emails, text messages, invoices, schematics, and documents. This information is an asset to the company as threat actors will want to target it for financial gain. With symmetric encryption using a secret symmetric key with 128-bits it would be impossible to gain access to without the secret symmetric key. For security of the key, we use AES with RSA by implementing it with

OpenSSl. According to (Oliveira, 2020) first, we generate RSA key pairs, exchange public keys, generate AES key, encrypt the data in the server with AES key, and encrypt AES key with RSA.

The risk of using symmetric encryption is that every time you share the key with someone else the risk of sharing the key that decrypts the message goes up because of the chance of interception of a third party (AppViewX, 2022). If this happens, they can decrypt all the data sets with the shared key (AppViewX, 2022). To avoid this, you should share the key in person with the trusted user.

The reward of using symmetric encryption is how fast it is compared to asymmetric encryption. Also, the fact of using one key to ensure protection and confidentiality helps make the process faster and protect the one key, instead of protecting multiple keys. Symmetric encryption helps take blocks of data sizes 64-bit and above. To do this you can use AES or Advances Encryption Standard as it is better than Data Encryption Standard (DES) because of the short length of 56-bit keys and the encrypted block sizes of 64-bits it caused this block cipher to not be very secure. AES was later developed and can handle sizes of 128, 160, 192, 224, and 256 bits (Contributor, 2021). This is better secured than DES as this block cipher is used by the US government, Google, and Microsoft (Contributor, 2021).

The cryptographic techniques used in symmetric encryption are encrypting the message that will be sent to the receiver who is the only person with the same key that can decrypt the message from the sender. If the message is “Hi” it will be encrypted into ciphertext before being sent over the network to the receiver. The sender and receiver must agree on a common secret key first. The sender would meet in person for security purposes and give the recipient the common secret encryption key. The sender will encrypt the message with the private key and then send the message to the recipient. Once the receiver has the message, they use the common secret key to decrypt the message that was sent to her from the sender. Having shared the key in person with the recipient you are less vulnerable to man-in-the-middle attacks. Now no third-party can read their messages on the network without knowing what that shared secret key is. This is the process of how symmetric encryption achieves security protection of data. Using block ciphers is a way to take chunks of raw data and convert it into a certain size used by the symmetric-key algorithms. If we use AES for the block cipher, we can use 128-bits which will take 128-bits of plaintext and convert it into 128-bits of ciphertext after it takes all the data and puts in into 128-bit blocks (Simplilearn, 2022).

The advantages of symmetric encryption are the speed as it is faster than asymmetric encryption and better optimization as large amounts of data is being encrypted it makes it easier to use for servers. Also, symmetric encryption has been found to have a higher level of performance when compared to asymmetric encryption because of the fewer calculations needed it helps give better memory to the host (Simplilearn, 2022).

The disadvantage of symmetric encryption is sharing the single secret key over the internet as you are vulnerable to man-in-the-middle-attacks (Contributor, 2021). Also, if the key is compromised everything used with that key can be decrypted from the threat actor. If your security is vulnerable and keys are not in a secure place, it can only take one attack like a software-gain attack to gain access to insecure location of the stored keys making data inaccessible and lead to decryption of messages (Contributor, 2021).

The security concerns of AES so far are only if you implement it wrong it could be used as a gateway for hackers. Other than that, there are no known issues with AES in the real world yet. There are theories of how someone could infiltrate the AES encryption though. One is using related-key attacks, this is targeting of the encryption key itself. This attack would only work if the hacker suspected a relationship between the two different keys (Rimkiene, 2020). AES was attacked like this in 2009 but later adjusted by making the AES key schedule more complex (Rimkiene, 2020).

One type of network protection technology is a firewall. A firewall can help the organization block bot attacks, malware attacks, and vulnerability exploits (Cloudflare, 2022).

In the scenario the headset sends information to the server which could be protected by a firewall to prevent the organization from certain attacks, like a malware attack. Depending on the headset technology firewalls could be software installed in the headset to block the data that is already on the headset. This would help provide protection for potential vulnerabilities within the organization and not just the server.

The risks of using a firewall are having unnecessary services available on the firewall that could lead to more vulnerabilities of the network (Sunny Valley, 2022). This can lead to a greater chance of a hacker stealing or deleting information. If the firewall implemented returns deny response instead of drop response for the ports that are not needed it is a security risk. This is because the hacker gains additional information and can use a port scan faster to discover open doors and weak points on your network (Sunny Valley, 2022).

The benefit of a firewall is it can monitor network traffic and can have filters to get rid of potential vulnerabilities that could impact your network. Another benefit of a firewall is it can stop hackers in their tracks as it prevents unauthorized access to emails, data, systems, and more (Fortinet, 2022). Also, firewalls can use a whitelist to stop not only certain threats but threats that they are not aware of in their network. Whitelisting can stop malicious software, keyloggers, and ransomware (Yasar, 2021).

The way in which firewalls have impacted the cybersecurity landscape is by the emerging trends of VPNs, enhances virus protection, and wireless communication (Team, 2021). These call for a greater demand for better firewalls like third generation and fourth generation firewalls. The third-generation firewall helps by giving specifications to security with little impact to network performance (Team, 2021). The fourth-generation firewall helps by filtering and being strict of what is allowed pass the firewall. The firewall does this by recording IP packets and port numbers (Team, 2021). This helps with whitelisting and protecting against emerging threats like malicious software and ransomware.

References

Crawford, D. (2019, February 4). A Complete Guide to AES Encryption (128-bit & 256-bit) - ProPrivacy.com. ProPrivacy.com. https://proprivacy.com/guides/aes-encryption

Oliveira, G. (2020, October 23). Sharing AES Key using RSA with OpenSSL. B2w Engineering -En. https://medium.com/b2w-engineering-en/sharing-aes-key-using-rsa-with-openssl-bc470afd2fb7#:~:text=Sharing%20AES%20Key%20using%20RSA%20with%20OpenSSL%201

Lucas, J., & Moeller, B. (2003, September). Effective Incident Response Team, The [Book]. Www.oreilly.com; Addison-Wesley Professional. https://learning.oreilly.com/library/view/effective-incident-response/0201761750/?sso_link=yes&sso_link_from=SNHU

Cloudflare. (2022). What is network security? Cloudflare. https://www.cloudflare.com/learning/network-layer/network-security/#:~:text=Network%20security%20is%20a%20category%20of%20practices%20and,refers%20to%20the%20protection%20of%20large%20enterprise%20networks.

What Is Symmetric Key Encryption? (Definition and Uses). (2021, August 11). Indeed Career Guide. https://www.indeed.com/career-advice/career-development/what-is-symmetric-key-encryption#:~:text=Here%20are%20several%20common%20uses%20for%20symmetric%20key

Ekran. (2019, November 8). How to Protect an Enterprise Database from Privilege Abuse. Www.ekransystem.com. https://www.ekransystem.com/en/blog/database-admin-protection#:~:text=Potential%20dangers%20of%20database%20administrators%3A%20Insiders%20can%20harm

iFour Team. (2022, April 22). Top 8 emerging database management trends. Www.ifourtechnolab.com. https://www.ifourtechnolab.com/blog/top-8-emerging-database-management-trends

Contributor. (2021, July 19). What Is Symmetric Key Encryption: Advantages and Vulnerabilities - Phemex Academy. Phemex. https://phemex.com/academy/what-is-symmetric-key-encryption#:~:text=Symmetric%20key%20encryption%20has%20two%20main%20advantages%3A%201

Simplilearn. (2022, February 15). The Ultimate Guide to Symmetric Encryption. Simplilearn.com. https://www.simplilearn.com/tutorials/cryptography-tutorial/symmetric-encryption#:~:text=Two%20types%20of%20ciphers%20can%20be%20used%20in

Rimkiene, R. (2020, December 11). What is AES Encryption and How Does It Work? CyberNews. https://cybernews.com/resources/what-is-aes-encryption/

Sunny Valley. (2022). What are the Top Firewall Vulnerabilities and Threats? - sunnyvalley.io. Www.sunnyvalley.io. https://www.sunnyvalley.io/docs/network-security-tutorials/what-are-the-top-firewall-vulnerabilities-and-threats#:~:text=Drawbacks%20of%20a%20firewall%20system%20are%20as%20follows%3A

Fortinet. (2022). Firewall Benefits: The Importance of Firewall Security. Fortinet. https://www.fortinet.com/resources/cyberglossary/benefits-of-firewall#:~:text=Top%205%20Firewall%20Benefits%201%201.%20Monitors%20Network

Yasar, K. (2021, May 27). What Is Whitelisting and How Do You Use It? MUO. https://www.makeuseof.com/what-is-whitelisting/#:~:text=Benefits%20of%20a%20Whitelist%201%201.%20Improved%20Cybersecurity

Team, D. (2021, April 8). Emerging Cybersecurity Technologies you should know for Business. DataFlair. https://data-flair.training/blogs/emerging-cybersecurity-technologies/#:~:text=The%20arrival%20of%20stateful%20inspection%20firewalls%20was%20to,helps%20in%20monitoring%20the%20state%20of%20active%20connections