Option #1: Security and Encryption Policies

Liam Bergerson

CSU - Global

ITS415-1

K. Brogi

2/20/22

Option #1: Security and Encryption Policies

Encryption is crucial in keeping important data and files confidential. Intruders can easily intercept important data traveling across the network if it is not encrypted. The same can also be said about data stored on an unencrypted hard drive. An intruder could walk in and steal the hard drive and extract the unencrypted information on it. There are many methods to encrypt data that is at rest and in transit on a network. However, depending on how complicated the encryption is, it can be difficult for businesses to properly implement and maintain encryption. A case will be discussed where a business did not implement proper encryption which resulted in compromised data.

Encryption At Rest and In Transit

Data at rest is defined as data that isn't being used or transmitted on a network (Ryan, 2019). Symmetric or asymmetric encryption can be used to encrypt hard drives at rest. In symmetric encryption one key is used to encrypt and decrypt the hard drive when it comes time for that data to be used. In asymmetric encryption, a public and private key are used. The public key is used to encrypt the data and the private key is used to decrypt the data. For data in transit, either SSL or TLS can be utilized. These protocols use symmetric and asymmetric encryption to encrypt data in transit. A Virtual Private Network (VPN) can also be used to encrypt data in transit since a VPN creates an encrypted tunnel used to send data back and forth.

Challenges of Encryption

Key management is the most challenging aspect of proper encryption deployment (Fornetix, 2019). In an organizational setting, there are many files and data

that need to be encrypted and the decryption keys keep adding up to. In a small business, an employee could be in charge of solely managing the decryption keys. Eventually the keys will accumulate so much that the chance of losing keys due to human error will be inevitable. An automated solution for key management will rid the chance of keys being lost due to human error.

Ineffective Encryption

Ineffective encryption methods can result in a data breach. In Equifax's case, they suffered a data breach due to an expired digital certificate (Nohe, 2020). A digital certificate authenticates the user and ensures that only trusted users and devices connect to the network (Easttom, 2019). As was the case with Equifax, intruders infiltrated the network and spied for valuable data and stole it. The situation could have easily been prevented by keeping documentation of all of the digital certificates used and dates on when they were last updated and when to update them.

Conclusion

There are many encryption methods to choose from that will encrypt data at rest and in transit. Symmetric or asymmetric encryption can encrypt hard drives that are not used or in transit on the network. SSL or TLS protocols and VPNs can be used to encrypt data in transit on a network. Encryption can be challenging for an organization because managing the many keys used to decrypt hard drives can be too much for a human which could result in lost keys. Documentation for digital certificates needs to be kept to see when certificates were last updated and when they need to be updated next. This could have prevented the breach of Equifax data.

References

Easttom, C. (2019). *Computer Security Fundamentals (Pearson IT Cybersecurity Curriculum (ITCC))* (4th ed.). Pearson IT Certification. https://platform.virdocs.com/r/s/0/doc/1278606/sp/133556880/mi/409911631/?cfi=%2F4%2F2%2F18%2F24%2F10%2F6%2F4%2F2

Fornetix. (2019, April 5). *Top 4 Encryption Problems - Data Encryption Management Fornetix*. Retrieved February 17, 2022, from https://blog.fornetix.com/top-4-challenges-when-managing-encryption

Nohe, P. (2020, August 26). *The Equifax Data Breach went undetected for 76 days because of an expired certificate*. Hashed Out by The SSL Store™. Retrieved February 17, 2022, from https://www.thesslstore.com/blog/the-equifax-data-breach-went-undetected-for-76-days-because-of-an-expired-certificate/

Ryan, R. (2021, June 9). *Encryption in-transit and Encryption at-rest – Definitions and Best Practices*. Ryadel. Retrieved February 17, 2022, from https://www.ryadel.com/en/data-encryption-in-transit-at-rest-definitions-best-practices-tutorial-guide/