Acceptable Encryption Policy for [COMPANY NAME]

Josiah Baker

Liberty University

CSIS340: Studies in Information Security (D01)

May 8, 2023

DISCLAIMER

There may be references throughout this paper to other policies. These policies are fictional and are referenced solely because they would typically be found within an organization and would likely work well with this policy. Furthermore, this is assuming the company this policy is being designed for develops cloud technologies for smaller companies that cannot afford in-house servers.

Overview

At [COMPANY NAME], our main purpose is to provide the latest cloud technologies to companies that cannot afford powerful servers. By being a source for other companies for server housing, it takes the pressure off them to manage the system. Since it is up to [COMPANY NAME] to ensure the protection of the data stored within a server, it is important that the organization practices sound security principles. By Practicing the latest security principles, [COMPANY NAME] protects itself from having bad relations with customers, as well as protection against potential lawsuits due to not protecting private data effectively. One way security can be promoted as an organization is using effective encryption.

Purpose

The Purpose of this policy is to inform [COMPANY NAME] employees of the best practices when it comes to encryption. Since [COMPANY NAME]'s aim is to protect the database's it hosts, it is important to identify the main threat actors.

The first main threat actor is having an unauthorized individual gain access to one of the servers (Liu, 2022). This can result in a large amount of data being stolen and often goes unnoticed. It is important to catch an intrusion like this early or prevent it entirely. Employees msut keep their usernames and passwords private and secure. As encryption is a great practice, it will not cover an intrusion through an existing employee's account.

This ties into the next concern, which is the threat people within the organization pose (Wu, 2022). Although as a company the goal is to optimize computer systems to promote the highest level of security, people often get in the way. If the employees of the organization are

not practicing the security policies outlined in this document, this document is in vain. It is important that each employee applies the information here to ensure the security of the entire system.

Furthermore, this scope aims to educate employees on what encryption algorithms are substantial (SANS, 2014). Although there are a lot of encryption algorithms out there, they are not all effective, and some have been proven to be easily decrypted.

Finally, this document educates employees on the legal expectations legal authorities have on [COMPANY NAME] (SANS, 2014).

Scope

[COMPANY NAME] is a service to other companies, providing them with real time servers. Every employee is dealing with these servers to some level, so this policy applies to all employees.

Policy

First, each encryption method must meet certain standards. As discussed previously, there are a lot of different encryption algorithms, but they are not all sufficient. Encryption methods used at [COMPANY NAME] must meet the standards of "AES-compatible" (SANS, 2014). This standard is widely accepted by the public and does not seem to be cracked anytime soon. Since it is secure, it serves well as a standard to be implemented for [COMPANY NAME]. To view more information regarding this standard, go to https://datatracker.ietf.org/doc/html/draftirtf-cfrg-cipher-catalog-01#section-3.1.

Encryption is done using a key. The key is how data is encrypted. If the key is exposed, the encryption security breaks down and can be decrypted. Since the key is important to security, these also need to be properly secured. These keys must be secured using a cryptography protocol, such as Diffie-Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH) (SANS, 2014). These different protocols help protect keys from being readable.

Furthermore, both sides of a transaction must be authenticated (SANS, 2014). What this means is that before a key is sent, both sides, the side sending the key and the side requesting the key, must reach sufficient levels of authentication to even receive the encryption key.

Finally, these encryption keys must be stored in a secure location (SANS, 2014). Although they should be accessible, they should only be accessible to authenticated people, and should be protected by sufficient layers of security.

Policy Compliance

Not adhering to the above-listed policies can and will have consequences. The only time it is permissible to go against this standard is if an exception has been granted by a supervisor. Each non-compliance case will be assessed individually, with the consequences resulting in employee termination at [COMPANY NAME] (SANS, 2014). Other consequences could be reduced pay and/or reduced privileges.

It is important for individuals in a leadership role to follow these rules and promote them to other employees. According to the article “Establishing information security policy compliance culture in organizations”, it is important for leaders to support these rules, as it impacts how those that are under these individuals’ leadership perceive the importance of the

policies. (Amankwa, 2018). When leadership supports the policies, other employees are more likely to follow suit.

Related Standards

A related standard to encryption is digital signature schemes (DSS). A digital signature is a way of ensuring that an individual is who they claim they are (Chia, 2021). By doing this, a system can be sure that the individual trying to access the system is who they claim they are, and then see if they have the proper authentication to access the system.

Definitions

Encryption is a way of ensuring that information is properly protected. The article "The importance of Encryption" defines encryption as "the process of rendering data as only accessible to authorized individuals who have the encryption key to decrypt the information." (Ang, 2020)

Cryptography is the process of using mathematical techniques to alter data so that it cannot be read or understood (nist.gov). It is very comparable to encryption.

Terms

[COMPANY NAME] created this document to promote the use of encryption. As discussed, encryption can serve to create security for the data that is stored within the organization, which is critically important to [COMPANY NAME] Encryption, when done right, has proven to be so powerful, that even governments are beginning to consider actions against the use of encryption (Thresher, 2023). This is because not all people that use encryption have

good intentions. Terrorist groups also use encryption, since they can then communicate without anyone understanding what they are talking about. However, since governments recognize the security gained by encryption, so does [COMPANY NAME]. It is [COMPANY NAME]'s hopes that each employee will apply this policy and help promote data security going forward.

References

Acceptable Encryption Policy. SANS. (2014, June). https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt0759f19972ec623e/5e9dd1fa33f6b8718946a2b9/acceptable_encryption_policy.pdf

Amankwa, E., Loock, M., & Kritzinger, E. (2018, October 8). *Establishing Information Security Policy Compliance Culture in organizations*. Information & Computer Security. https://doi.org/10.1108/ICS-09-2017-0063

Ang, R. J. (2020). *The Importance of Encryption*. ProQuest. https://www.proquest.com/docview/2561883359/fulltext/8E343F52D0DF482DPQ/1?accountid=12085

Chia, J., Chin, J.-J., & Yip, S.-C. (2021, September 16). *Digital signature schemes with strong existential unforgeability*. NIH. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC9925878/

Cryptography. NIST. (n.d.). https://www.nist.gov/cryptography

Liu, G. (2022, August 29). *The application of Data Encryption Technology in Computer Network Communication Security*. Mobile Information Systems. https://doi.org/10.1155/2022/3632298

Thresher, K. (2023, January 18). *Deciphering Australia's encryption laws: a human rights approach*. Taylor & Francis Online. https://doi.org/10.1080/1323238X.2022.2157674