Jackson Warren

Jeremy Bergen

CSCI 370

10/25/21

Week 7 Assignment

For this assignment, I’ll be creating an encryption policy for Fictional Company Inc. For this company, we are going to assume that they have a company laptop and phone provided, as well as the company size being somewhat large. We’re also going to assume that the main purpose of these devices is to communicate within the company, and not necessarily outside of the company. For this policy, every employee’s laptop and phone would both fall under the encryption scope. For implementation, both devices would have to have software uploaded before being given to the employee. This software would serve as a built in encryptor that will automatically encrypt all sensitive data that is being sent over the network. This data would include emails, images, progress reports, names of employees, sales, passwords, etc.

Things such as employee passwords and usernames would automatically be hashed using something like RSA. Then, the storage of these items will be more secure and less likely to be grabbed and put into the wrong hands. Any sensitive data (such as progress reports, specific numbers, emails with personal information, and many other data elements) shared across the network would be encrypted using something along the line of gpg so they cannot be intercepted halfway through. The system, once received and verified by the company computer/phone, can decrypt these files and gain their information.

Things like zoom sessions or teams sessions are a bit more out of my understanding, but the company would obviously want to use a software that guarantees privacy in this area as well.

When it comes to encryption level, obviously the more we can do here the better to better secure data. So, staying at the RSA level would be best. Perhaps for things such as emails without important personal info or sensitive files it could be flagged to have lower protections or somethings along those lines. It could also be an option where each employee has a key to “unlock” files of their granted level, so then only employees with the correct keys can view items.

In general, it looks like encryption of data is most commonly provided through a cloud provider or something of the such. This could encrypt data for your company would simply need to be hired and maintained. Then, for things such as keys, this service provider could also handle or another source would have to be hired to manage how this is implemented and upkept.