Samuel Powers

04-20-2022

CS-405

Hodde, Trevor

Reflection

Secure coding in a digital world is not only something that we should all consider, but also something that we should all start implementing today. With virtually unlimited access to anything that you can imagine right from your fingertips, it just makes it easier for those that wish to perform malicious activity on our lives and within our jobs to take what they want and use it for their own bad intentions. Secure coding does not only need to be something that is done at work; by simply setting up 2 factor authentication for our own personal things like bank accounts, social media logins and emails, we are already taking the first steps to securing our data and personal information. This is also known as zero trust. Your phone implements zero trust by making you put in your fingerprint or face ID every time you unlock your phone. 2 factor authentication is zero trust because in order to log in to Facebook from an unknown computer, you need to have a link or password sent to your phone or email that grants permission to log in. We experience zero trust in our lives every day and it should be something that businesses implement into its daily routine as well. Every time you log in to the database, you should also be submitting some form of secondary authentication and not something that can just be saved in found inside a file on the database, an *approve* or *disapprove* of a login or change is important, and also verifies who might have made a mistake of allowing a leak of data to happen.

In business, secure coding should be a top priority. Within any business, data is the number one tool that is used to continue marketing and keeping the business at boy. Everywhere you go today there is a “membership” that one can sign up for any kind of purpose, whether it be for discounts, free birthday lunches at your favorite restaurant, or even just to track your purchases, your data and your information is now in the hands of that business. Especially if you decide to make online transactions, these businesses now have your bank and credit card information. Performing online applications for loans and other reasons to enter in your social security card is now putting *you* at risk of having your identity stolen which can lead to many headaches and endless issues. Again, as a business, it should be top priority to protect the very reason that you remain in business, your paying customers. By implementing multiple layers of protection for the data and information that you hold, you are securing the future of your company and the safety of everyone around. By not leaving that level of security for the end, you take the risk level down to a minimum. This doesn’t mean that it won’t be impossible for some hacker to steal information, but it does mean that it can make it very hard for them to do so and can make it easier to spot a data breach before it is too late, and the information stolen.