Richard Schall
CS-405-H4327: Secure Coding 21EW4
Southern New Hampshire University
April 15, 2021

7-1 Journal: Consider the Motive for the Attack

How will you apply this concept to your own practice?

Security attacks are getting more frequent. The motives are wide ranging. There are those that are motivated by recognition and are not doing it for monetary gains. There are nation states that conduct attacks to develop defenses. (OfficialIBCshow & Loginov, 2018) There are also nation states that conduct attacks to manipulate other countries and to gain sensitive information. There are also those that are criminals that conduct attacks for monetary gain. The company I work for last year experienced a ransomware attack. This has changed the way we go about our daily work and how we communicate and exchange information as a global company with teams across the globe.

The ways that I will and have already applied this concept is using some of the tools in this course to change the way I develop applications and how I go about my job. I have been forced to consider security and make it a part of every piece of code I write where before it was not the priority it should have been.

How would you explain this to a new developer on your team?

The way I would explain this to a new developer is to drill the idea that we are all responsible for the code we write, and we must be professional and consider the risks associated after a piece of software is deployed in the field. I would mention that security needs to be incorporated throughout the software development life cycle. This means making security checks a part of the unit testing program. These unit tests will look for things like buffer overflow situations and unhandled exceptions.

What is one example of this concept you can use in your final reflection in Module Eight?

One example of this is to be careful when writing code that updates a SQL server with data. This is something I must do often. The two methods I deploy are using stored procedures that are safe because the data sent to the stored procedure is parameterized, SQL injection is ineffective on stored procedures. The stored procedure will spit back an error if the parameter data is ill-formed or if used to query table data, there will not be any results or there will be an error returned.

If using LINQ messages in C# or VB.NET it is important to parameterize data that is input by a user or data file and not make it a part of the SQL query directly. This is where injection can occur. This is a very valuable lesson I have learned in this course.

References

OfficialIBCshow, & Loginov, M. (Directors). (2018, June 21). What motivates hackers? [Video file]. Retrieved April 15, 2021, from https://www.youtube.com/watch?v=BoWouwPGtVY