Security Journal

Leaving security to an end can lead to hackers taking advantage of the situation and unprotected data. Security should be the base of any application and it must be the standard. Security must be present on every layer. For example if there is security only for the network, it doesn’t guarantee the security for company from phishing emails and app security. There always must be other security layers covered.

One of the most important steps is to train and educate people. The most common security breaches are happening from giving away valuable information to hackers. Valuable information is passwords, answers to the security questions and log in information. Having those hackers can easily access and steal the data. Another way to protect employees from this is to provide training with phishing campaigns and to educate people how dangerous it can be for the company. To protect companies even more if the passwords were leaked is to provide multi factor authentication. Another way is pushing patches to the computer and updating the software. There are companies that use free versions of Adobe reader, and they never upgrade the old version they have. Old versions of software can be a great opportunity for hackers to attack the company. Windows server 20121 is going off the market and will stop providing support for it. Companies that didn’t move from servers 2012 will be at risk.

After working as IT admin for 1 year I can say that zero trust should become a number one rule in IT industry. Device trust is very important for us because we need to know the processes the device goes through, the OS it is running, what processes/services are normal and which ones are not. User trust from my experience "Never trust your user" I had users saying they did not click on the links, but I know that they did and received the alert for it. every organization should have double layer authentication because users like to reuse their passwords and to simplify them to be password = password what can give allow hackers an easy access. As a user I can say that I use secure application to store my passwords. I try not to use public internet. I prefer to follow and only open secure links, I do not trust any emails I was not expecting to receive and will call to verify for an email. As a user I am using multifactor authentication. I am trying to follow the five pillars form the threat post article device trust, user trust, transport trust, application trust and data trust. I will persuade it in a positive direction and will absolutely support it. As a future cybersecurity engineer, I can say that cybersecurity is always growing into more and more education and alerts, I am sure that this looks new now, but it will be old for us very soon. Cybersecurity field is growing fast, and

Having a data back up every other week should provide more security for occurring data loss. If something will happen to a physical device with all of the information and it won’t be accessible anymore we should be able to access the backups. There must be access management for every company. The reasons for that is giving admin permissions only for the installation of necessary for work applications or none at all. Some companies d not allow admin permissions for the employees and they require permission from management or IT department to install software.

Junit testing for Java programming. Testing is important in cybersecurity and Junit provides one of the best test frameworks for testers. Junit testing is comfortable to use for small sections of the code. As Nikhil Bansal mentioned in his article “JUnit testing is used to test the behavior of methods inside classes we have written. We test a method for the expected results and sometimes exception-throwing cases—whether the method is able to handle the exceptions in the way we want.” Also, cppcheck that was done for some assignments in this class is useful for checking for some vulnerabilities and can be mentioned in the Project 2. Cppcheck is an analysis tool for C++ and C. Cppcheck can detect bugs and analyze the. There is a lot of tools for code analysis and testing.

References

*10 ways to prevent cyber attacks*. Leaf. (2022, July 15). Retrieved January 28, 2023, from <https://leaf-it.com/10-ways-prevent-cyber-attacks/>

Bansal, N. (2019, August 27). *Build with confidence: A guide to junit tests: Toptal®*. Toptal Engineering Blog. Retrieved January 28, 2023, from https://www.toptal.com/java/unit-integration-junit-tests#:~:text=JUnit%20testing%20is%20used%20to,in%20the%20way%20we%20want.

Kueh, I. S. I. T., & Kueh, T. (n.d.). A practical guide to zero-trust security. Threatpost English Global threatpostcom. Retrieved February 23, 2023, from https://threatpost.com/practical-guide-zero-trust-security/151912/