To: Professor Krasso

From: Sarah Kovar

Date: 21 June 2020

Subject: Securing Microservices

In an effort to stay current with industry best practices, the Solutions Architecture Department is recommending we follow the following best practices with regard to security microservices [1]:

1. Create secure microservices
2. Scan for dependencies
3. Use HTTPS
4. Access and identity tokens
5. Encrypt and protect
6. Slow down attackers
7. Cloud and cluster security – know it

Going forward, we will be more intentional when we build microservices. The first measure that will be implemented will be continuous stress testing across architecture. Security unit tests will allow us to detect vulnerabilities in the code in addition to dynamic analysis security testing to simulate attacks from the outside, in. Third party dependences can be a hole in security, as only 75% of majority of applications report security issues [1]. Scanning for dependencies can allow you to know what vulnerabilities might lie in our code. Next, we will begin using HTTPS everywhere, no exceptions. This insures privacy and data integrity [1].

Authentication can be tricky. OpenID Connect (OIDC) extended OAuth works across multiple identity providers. Going forward, we will be using OIDC and OAuth 2.0. There is no reason not to. You are able to look up identity via access tokens to a user end point. OAuth 2.0 allows us to use a consistent, repeatable means of authentication, creating a more secure environment and alleviating our developers from having to build authentication into every microservice.

The final three best practices will involve a few tactics in addition to required knowledge of your could and cluster security. Your microservices will likely contain API keys and other private data that should NOT be checked into source control. The proper way to secure, going forward will be to use Microsoft Azure Key Vault. This will allow us to generate master keys with encrypted messages. Next, we will be implementing rate limiting across the board in order to slow down would be attackers. Lastly, all team members must be aware of our cloud and cluster security. Code, Container, Cluster, and Cloud/Co-Lo/Corporate Datacenter [1].

Security is everyone’s business and microservice security is every application developer’s business going forward, no exceptions.

References

8 Ways to Secure Your Microservices Architecture. (2020, May 22). Retrieved from   
 [https://www.okta.com/resources/whitepaper/8-ways-to-secure-your-microservices-  
 architecture/](https://www.okta.com/resources/whitepaper/8-ways-to-secure-your-microservices-%20%20%20%20%20%20%20%20%20%20%20%20%20%20%20architecture/)