To: Professor Krasso

From: Rochelle Markham

Date: 26 August 2020

Subject: Secure Microservices

Microservice security can be more complex than security within monolithic applications. More working parts mean more vulnerabilities, but with careful planning and consideration it is possible to successfully implement security measures within a microservice architecture. Many different approaches to security have been developed and tested. Some of the best security measures include using OAuth for authentication, using API gateways and using third-party services to scan for potential risks.

OAuth is the industry standard for authentication and authorization; a fact that should not be ignored. Using OAuth has the added benefit of having been utilized and improved upon by some of the worlds’ greatest minds. There are platforms and libraries available that have been developed to enhance security and to fit many special cases.

The use of an API gateway is imperative to microservice security and also helps with speed and simplifying code within the microservice architecture. Utilizing an API with a firewall allows communication between users and the microservices but still secures services from attacks. By using a gateway, all requests go to the gateway, so all data flow is controlled and can be secured.

When implementing a microservice architecture, it is also important to remember that we are not alone in our goals of creating secure microservices. Many third-party services are available to scan microservices to locate security vulnerabilities within the infrastructure. Services also check for malware and other know malicious attack methods. They can also be used to help notify you in the case of unusual traffic flow, that may indicate an attack on your infrastructure.

Most importantly, maintaining secure microservices, means layering security measures. Utilizing multiple security methods is the best way to ensure minimal risk of security breaches. Using OAuth as the authentication method adds the experience and knowledge of the greatest minds in our field. Using an API gateway with an added firewall encapsulates the microservice and allows only one point of entry for user requests and potential attacks. Adding a security scanning service to these options helps us stay ahead of potential attackers and close up loopholes and vulnerabilities before they become security problems. By using multiple security methods, we can focus on microservice development and business uses, instead of dealing with security breakdowns.

Resources:

Bryk, A. (2018, August 23). *Microservice and Container Security: 10 Best Practices*. Retrieved from Apriorit: https://www.apriorit.com/dev-blog/558-microservice-container-security-best-practices

Troisi, M. (2015-2020). *8 best practices for microservices app sec*. Retrieved from Tech Beacon: https://techbeacon.com/app-dev-testing/8-best-practices-microservices-app-sec