William Simpson

Professor Krasso

WEB420

23JUNE2018

1. Security is extremely important within microservices. Everyday millions of websites and databases are attacked and it is our job to protect them in the best and most efficient ways possible. This memo is going to explain what is expected of the company in terms of best practices, ways to improve, and looking to the future.
2. Currently there are many practices that we could integrate and follow within our own microservice security climate. The first step is access control, the industry standard is Oauth, which is a common token-based authentication library that will enable us to store sensitive data without it being exposed during transactions. Our second strategy will be to utilize multiple defensive layers after a user has gained access to our systems. This mentality will ensure defense against both malicious and accidental system exposure. Next, one of the most common ways that someone can gain access to a system is through old software that has not received the most up to date security patches and fixes, so from now on we will always have security updates be delivered throughout the system automatically to make sure that we avoid legacy exploits.
3. It is also necessary to visit some ways to improve our current security. Currently we have some in-house built encryption code, from now on we will be using trusted and verified open source libraries to handle most security protocols. Open source options have a large development base, are more thoroughly tested and don’t cause as much of a drain on company resources to keep unique source code up to date. We will conduct security reviews for each microservice to certify that the current security protocols are the most current and best for that specific service, this way even when one service is compromised there is a good chance that other services will still be protected. We will also make sure that our API gateway is correctly keeping access to our microservices away from the outside network and that it can’t be coerced into routing malicious traffic throughout our application.
4. Thirdly, it is important to always keep the idea of security at the forefront of our practices and to make it a priority when developing new microservices for our application. Staying abreast of the newest security practices, tools and expertise in the industry will allow us to maintain our integrity and our clients.
5. It is with this mentality that you should go about your coding, make sure that current services are well protected and we maintain a high standard of security mindedness, that we continue to improve our practices and always be ready to adapt to new threats and an everchanging technological landscape.