To: All Employee’s

From: William Thomason

Date: 11 February 2018

Subject: Security in Microservices

Authentication is one of the biggest ways to manage security. Authentication can be passed to the API in the HTTP header allowing access to the API. There are a number of ways that you can authenticate a user with various login systems, where the user registers and then logs into the system. After doing this the system gives them a key that is stored and passed with the request to the API. OAuth is another option. This authentication system is an open standard for token-based authentication and authorization and allows the users account information to be used by third-party services without exposing the user’s password.

Validation is crucial to any web application. Validating any data being stored to be used in the API will keep your data clean and valid for the desired output. This begins by knowing what type of data to you expect to receive and then structuring your API to filter out bad data and return an error to the user. Encoding data going into and out of the database the API is using will help protect the data your API is using. All private information should be encrypted to ensure the safety of the user in case your database in compromised. This brings me to my last security tip. HTTP status code - Properly handling status codes and redirecting the user to appropriate pages will help keep users out of where they don't belong.

References

Levin, G. (2018, October 04). Top 5 REST API Security Guidelines - DZone Security. Retrieved June 18, 2019, from https://dzone.com/articles/top-5-rest-api-security-guidelines