Security Presentation about Breaches!

By Steven Yeung

Ticketmaster Breach Where? When? What was it?

- This breach occurred between February 2018 through June 23, 2018
- This breach occurred on a Ticketmaster UK website.
- The breach's topic was that Ticketmaster UK's website had suffered a data breach that was scamming people for their money
- Not only was their money scammed, but personal information was collected as well.

What happened?

- The issue with how this breach happened was mainly all software.
- The issue started with Inbenta Technologies, which is a third-party vendor for Ticketmaster.
- Inbenta had altered Javascript code to make it easier on the customers who were using Ticketmaster.
- Ticketmaster used this script code without informing Ibenta.
- Hackers found the script code and modified it so that it will extract user information

Damage Report

- Approximately 40000 UK customers who used Ticketmaster during this period had their credit card number stolen as well as their personal information.
- After the breach already occurring, Monzo, a UK mobile only bank, discovered that there were an unusual amount of transactions on Ticketmaster.
- Monzo replaced the affected cards and notifies other banks and US secret service.
- Inbenta released a statement to Ticketmaster users after the breach incident was resolved an apology for violating users’ privacy.

How to prevent something like this from happening

- A way to prevent this type of breach from happening is to always communicate.
- Since Ticketmaster just used code, they found from their third-party contributors, it was probable that were going to be at risk.
- Had Ticketmaster informed Inbenta they were planning to use the JavaScript code, Inbenta could have gone back and fixed any loopholes that may have been there.
- As a programmer, use variables not public. Make them private or make the protected. By taking this step, people who want to rewrite code must receive permission to do so.
- So, the moral is double check, double check, and double check.