EasyJet hack

About EasyJet:

-**EasyJet plc**, styled as easyJet, is a British multinational low-cost airline group headquartered at London Luton Airport. It operates domestic and international scheduled services on over 1,000 routes in more than 30 countries via its affiliate airlines EasyJet UK, EasyJet Switzerland, and EasyJet Europe.

About cyberattack:

-The EasyJet hack was a cyberattack on the computer systems of EasyJet. EasyJet first learned of the cyberattack at the **end of January 2020**.

-They publicly announced the attack in **May 2020**. They told the BBC that they were only able to notify customers whose details were stolen **in April 2020.**

-EasyJet said "This was a highly sophisticated attacker. It took time to understand the scope of the attack and to identify who had been impacted" to the BBC. They also said "We could only inform people once the investigation had progressed enough that we were able to identify whether any individuals have been affected, then who had been impacted and what information had been accessed".

-EasyJet said they had gone public to notify the nine million customers whose email addresses had been accessed to beware of **phishing** attacks and that it would notify everybody by 26 May. Passengers whose credit card details were accessed were notified in April. They did not reveal details of the attack but said it seemed to be aimed at "company intellectual property" rather than information that could be used in identity theft.

Exposure:

-Approximately **nine million people** were affected with the credit card details of **2,208** also accessed. They notified the Information Commissioner's Office while they were investigating the crime.

-The affected data covers bookings made from **17 October 2019 to 4 March 2020**. The stolen credit card details include the **Card security code**.

What should have been done to prevent the breach?

-It is still not specified what how exactly EasyJet breach occurred, but it was probably something similar like in Brittish airways breach.

-The way the hackers accessed the information of affected people, was probably through a vulnerability in third-party Javascript used on the website. Hackers have probably secreted some lines of code that diverted crucial details around payments to a separate website controlled by the criminals. The third-party piece of Javascript, could probably send users to a separate page not controlled by company on which sensitive information could then be accessed.

-One thing that would prevent this breach or at least minimize it is having the right security management infrastructure – knowing at all times what the risks are, being able to find the solutions. Having dedicated security department that would do effective monitoring so they could find exposure and act quickly.

-Definitely not using third party JS plugins.

What are the consequences?

-**9 000 000** people affected

-**2 208** credit card details accessed

-Stolen credit card details includes **Card security code**

-Because of accessed emails from people that were affected there was increase in **phishing** attacks that could further make more damage

-The real consequences are **yet to be seen**. They are surely lot worse than EasyJet is claiming.