Security incident report

Section 1: Identify the network protocol involved in the incident

The network protocol involved in the incident was http. The Http protocol is insecure.Hyper text transfer protocol is vulnerable and prone to attacks.

Section 2: Document the incident

Multiple customers contacted the help department through emails that the website was asking to download file in order to access free recipes. When they downloaded the file they were redirected to another domain with the name greatrecipiesforme.com. The cybersecurity department looked into the matter and found that the website was compromised as a java script was running on the server which was redirecting all the users to a different and malicious website. The login credentials of admin access to the control panel were found compromised and that might be the possible entrance of the malicious actor. The cybersecurity department tested and analyzed the website in an isolated and controlled sandbox environment, resulted in the above outcomes.

Section 3: Recommend one remediation for brute force attacks

The organization should use the complex password policies for all users, especially ones with the higher privileges. Also the website should be hosted on different protocols and moved to a different protocol HTTPs.