Red Raven
Security

Charles Schwab Vulnerability Assessment

Executive Summary

By:

Kalyn Cowdin
Anthony Fusco
Richard Langdon
Jeff Lange
Lisa Prince
Garrett Wiese

Background

Charles Schwab recently went through a security incident when an employee was tricked into giving a username and password in a phishing scam. It is believed the scam came from a well-known advanced threat group called FIN7 that had targeted Charles Schwab. FIN7 is a financially motivated hacking group primarily out of Russia and consisting of multiple international hackers and servers located all over the world. FIN7 relies on phishing and social engineering techniques to gain access to a company's network. In 2020 FIN7 moved to the use of ransomware. By October 2021 they had their own fake network intrusion operation set up to recruit IT specialists and conduct attacks under the guise of pen testing. They also work with various ransomware gangs.

Purpose Statement

It has been over three years since Charles Schwab had an assessment of their network security. The concern is that their equipment, software, and policies may be outdated in this rapidly evolving world of network technology and cyber threats. The purpose of this assessment is to determine if the company is vulnerable to further malicious attempts by hackers like FIN7.

Scope

The scope of this assessment determines if there are any vulnerabilities in the company's network security equipment configurations, applications, and security policies. An external vulnerability assessment will be performed to identify any weaknesses of the internet-facing applications, web servers, email servers, network endpoints, firewall configurations, and VPN. An internal vulnerability assessment will focus on policies, standards, and procedures to determine if it follows industry standards for data security, data protection, and least privilege access for subnetworks, work groups, and administrators. The preventative and recovery procedures and policies were also evaluated to ensure up to date and sound practices are implemented in the case that there is ever a breach from being targeted by such malicious actors as FIN7 and others.

Methodology

The aim of our research was to complete a risk and vulnerability assessment for our client, Charles Schwab. We used Open-Source Intelligent Gathering (OSINT) and took a deeper look at Website security, Email security, Network security, Malware/Phishing, and the Reputation risks associated.

Then we had a look at the Security group policies to help mitigate risk and improve security.

Independent research was conducted to find the estimated cost to implement fixes for the issues found from reputable vendors as well as deeper insight into the threat group FIN7 that has been a threat actor towards Charles Schwab and has almost compromised security through phishing attacks.

Limitations

We were limited in the amount of information that was provided regarding the computing environment. Charles Schwab requested that we approach it in the same manner as a malicious attacker with no prior knowledge. We were also limited in the assessment methods we could use. Charles Schwab provides 24x7 accessibility to its customers and no downtime could be granted for performing a scan of their network.

Summary of Findings

Through the use of OSINT, we have found multiple inconsistencies related to the Website that cause the website to be insecure to both employees and customers. Due to the lack of Secure Sockets Layer (SSL) Certificates, and how the HTTP protocol does not redirect to HTTPS causes there to be no guarantee that the web traffic is encrypted between the client and server. We have also found that websites have the X-Powered header exposed causing the release of information about versions, and other technology that can be used to find vulnerabilities and exploit on the websites in a malicious manor. There are known vulnerabilities in Apache HTTP Server Version 2.2.27 and these are cause for concern as they can be exploited. For the mail servers some domains have been detected to having their DMARC policy set to none this causes there to be no protection against emails and they fly under the radar whether legitimate or malicious. The final issue found using OSINT was the open ports. Currently the open ports are FPT, MySQL, XMPP, IMAP, NTP, POP3, SMTP, SSH, 3478. Ports that are left open cause security risk.

Recommendations

Firstly, we are recommending the implementation of semi-annual mandatory training of KnowBe4 Diamond Level for all employees to help address phishing and increase awareness across the company.

For all employees that possess an organizational account to complete Duo Beyond training.

Installation of valid SSL Certificates, HTTP to immediately redirect to HTTPS for a more secure connection for customers and prevent data loss. Websites need to stop exposing the X-Powered By header this will mitigate the risk of an attacker finding an attack vector by using the information obtained from the header. Apache 2.2.27 vulnerabilities can be fixed by updating latest patch or applying work-arounds to fix security issues. DMARC policy can be amended by setting the policy to p=quarantine and having the email traffic monitored so legitimate emails are not misplaced and once they have been cleared change the policy back to p=reject.

Close all open ports: FTP, MySQL, XMPP, IMAP, NTP, POP3, SMTP, SSH, VoIP STUN.

Closing Thoughts

The vulnerability assessment performed outlined some issues found within Charles Schwab from the websites and overall awareness of the risks associated with emails that leads to high probability for cyber-attacks from threat actors and could diminish customer trust and increase loss of profits for Charles Schwab. While Charles Schwab ranked higher than the standard of the industry there can be improvements made. From implementing our recommendations, the security can be greatly improved and help limit the avenues of attacks.