Red Raven
Security

Charles Schwab Vulnerability Assessment

Comprehensive Report

By:

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

Table of Contents

Methodology

The Open-Source Intelligent (OSINT) framework methods of analysis were used on the Charles Schwab website, corporate email accounts, domains, subdomains, and IP addresses of Charles Schwab. We took a deeper look at Website security, Email security, Network security, and Malware/Phishing risks. We also reviewed Security group policies to help mitigate risk and improve security. Independent research was conducted to find 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.

Findings

During our OSINT research we have determined that Charles Schwab's website schwab.com has a high rating security protection against web vulnerabilities. Charles Schwab has a robust security posture and good attack surface management, especially compared to other companies in the same industry.

Risk Assessment – OSINT Analysis

Website Security

In this age of technology having a presence on the internet with a website is important for a business to build a brand, grow the business, interact with customers, and sell products. Web Trackers are third-party resources loaded onto a webpage. Trackable resources include social sharing widgets, JavaScript files, and images. These trackers can be used to monitor individual user behavior across the web. Data derived from these trackers are primarily used for advertising or analytics purposes. Schwab does not have any web trackers. That is important because it could potential be used as a back door vulnerability, if they had used them. However, with any website there are other security challenges in keeping private business and customer information from getting into the wrong hands. The following issues were found during our analysis for Website Security with risk level in parenthesis:

- **SSL** (critical) - We've detected websites that lack a valid SSL certificate. Without SSL, website visitors and customers are at higher risk of having their data stolen through man-in-the-middle and other cyber-attacks.
- **HTTP does not redirect to HTTPS** (high) - Websites are still accessible over HTTP. All HTTP requests should be redirected to HTTPS to ensure encrypted communications between the website and its visitors
- **X-Powered-By header exposed** (medium) - We've found websites that have their X-Powered-By header exposed. This header reveals information about the specific technology used to run the website which could be used to find known vulnerabilities that can be exploited
- **Apache Http Server 2.2.27** (low) - Apache Http Server 2.2.27 has known vulnerabilities published in the Common Vulnerabilities and Exposures (CVE) database. In some situations, these vulnerabilities can be exploited.

Email Security

Email is a critical part of communication in today's business world. Email provides a means for inter-office communication and communication with external customers and other organizations. Unfortunately email also provides a way for attackers to infiltrate a network and to cause problems that could result in loss of revenue and customer confidence. The following issues were found during our analysis for Email Security:

- **DMARC policy is p=none** (high) - We've detected domains that have their DMARC policy set to p=none. This provides no protection against fraudulent emails as it indicates that no specific action should be taken regarding the delivery of fraudulent messages.

Network Security

Network Security is imperative to secure the business' network infrastructure from unauthorized access, damage from malware, or theft of private and proprietary data. Network security implements multiple layers of hardware and software including anti-virus and anti-malware software, firewalls, network segmentation, access control, remote access VPN, and intrusion prevention systems. The following issues were found during our analysis for Network Security:

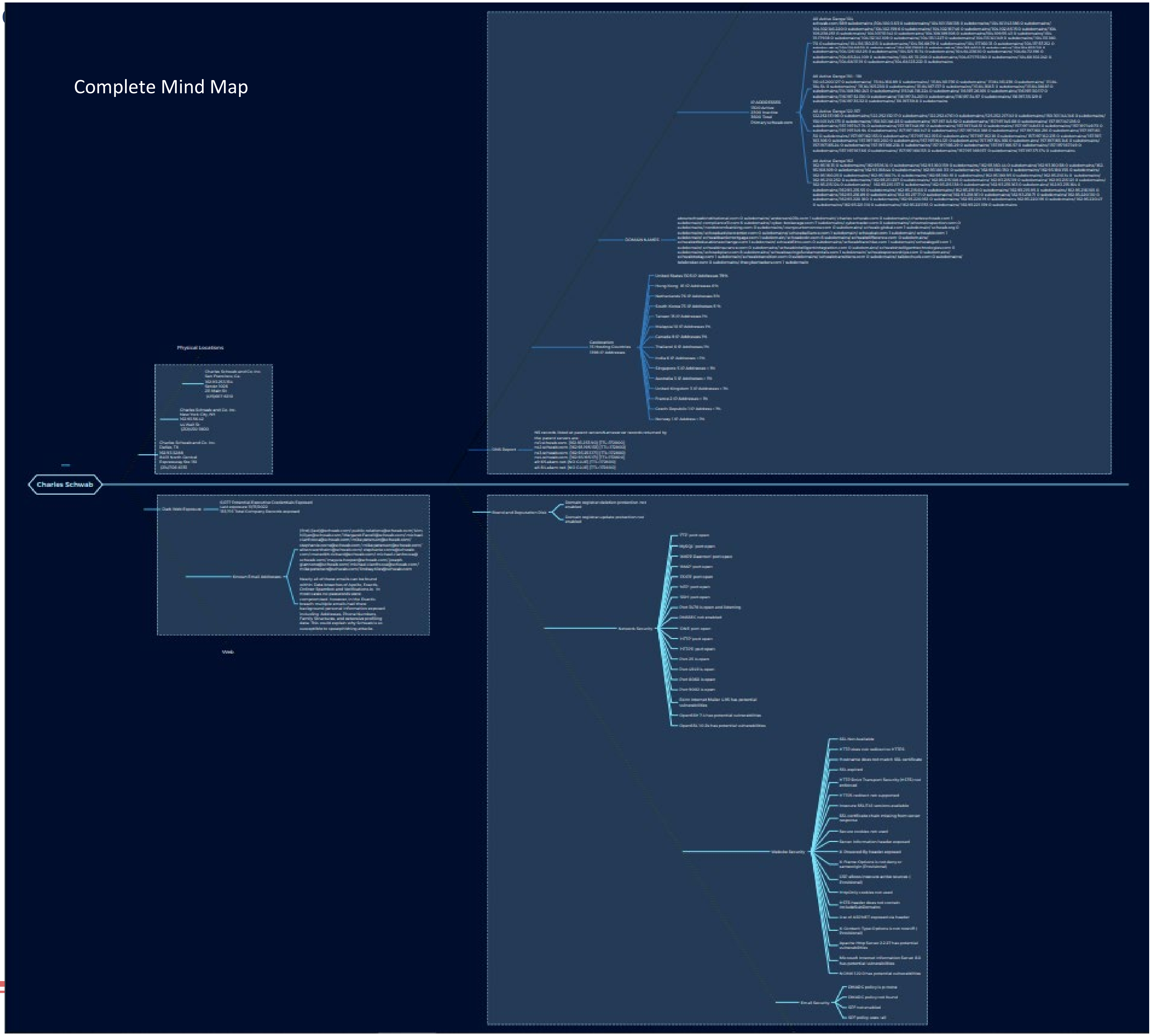
- **Open ports** – FTP port (critical), MySQL (critical), XMPP (high), IMAP (medium), NTP (medium), POP3 (medium), SMTP (medium), SSH (medium), Port 3478 (medium) ports are all open.

Malware & Phishing

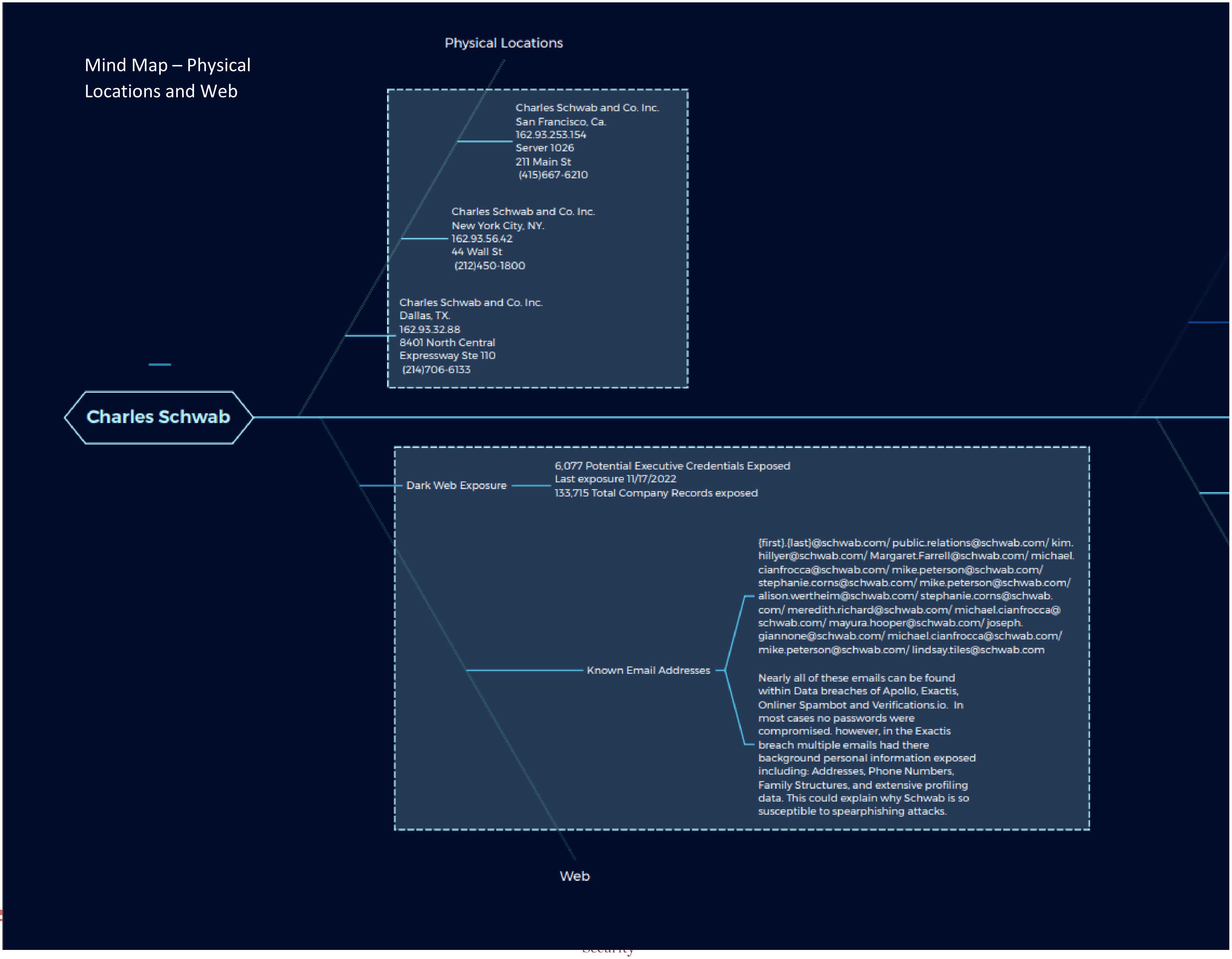
A phishing attack is a type of social engineering that targets company employees or contractors to collect information such as login credentials, personal information, and client data. Phishing can also be used as a means to introduce malware into a company's network or an endpoint. Malware can result in activity that is anywhere from mildly annoying to greatly destructive. Any company with Internet and email and human users has security vulnerabilities due to human nature and security policies must be implemented to prevent a breach. Risks for malware and phishing could not immediately be determined.

Mind Map

The following mind map was developed as a result of our OSINT reconnaissance.



Complete Mind Map



Mind Map – Physical Locations and Web

Physical Locations

Charles Schwab and Co. Inc.
San Francisco, Ca.
162.93.253.154
Server 1026
211 Main St
(415)667-6210

Charles Schwab and Co. Inc.
New York City, NY.
162.93.56.42
44 Wall St
(212)450-1800

Charles Schwab and Co. Inc.
Dallas, TX.
162.93.32.88
8401 North Central
Expressway Ste 110
(214)706-6133

Charles Schwab

Dark Web Exposure

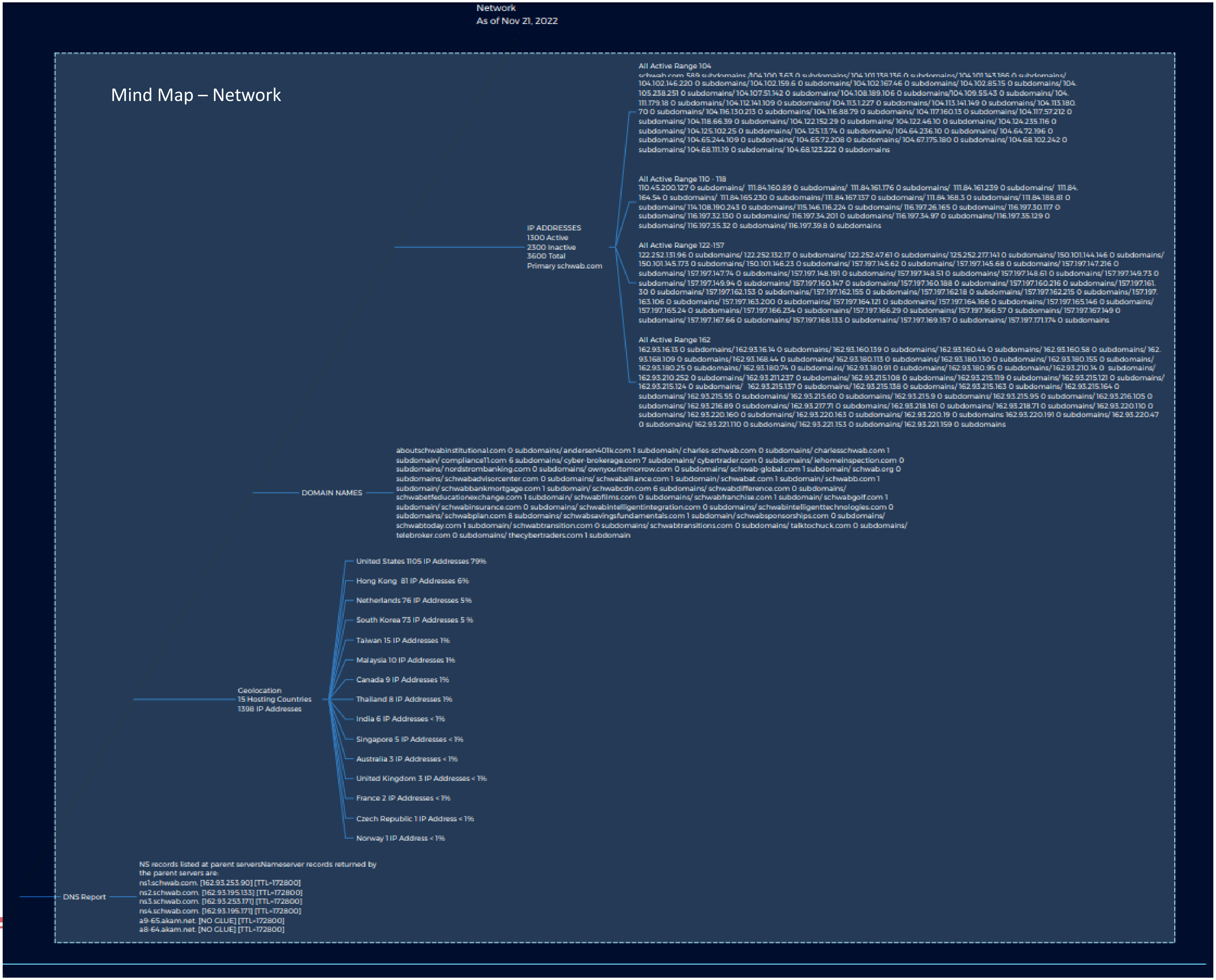
6,077 Potential Executive Credentials Exposed
Last exposure 11/17/2022
133,715 Total Company Records exposed

Known Email Addresses

{first}.{last}@schwab.com/ public.relations@schwab.com/ kim.hillyer@schwab.com/ Margaret.Farrell@schwab.com/ michael.cianfrocca@schwab.com/ mike.peterson@schwab.com/ stephanie.corns@schwab.com/ mike.peterson@schwab.com/ alison.wertheim@schwab.com/ stephanie.corns@schwab.com/ meredith.richard@schwab.com/ michael.cianfrocca@schwab.com/ mayura.hooper@schwab.com/ joseph.giannone@schwab.com/ michael.cianfrocca@schwab.com/ mike.peterson@schwab.com/ lindsay.tiles@schwab.com

Nearly all of these emails can be found within Data breaches of Apollo, Exactis, Onliner Spambot and Verifications.io. In most cases no passwords were compromised. however, in the Exactis breach multiple emails had there background personal information exposed including: Addresses, Phone Numbers, Family Structures, and extensive profiling data. This could explain why Schwab is so susceptible to spearphishing attacks.

Web



Network
As of Nov 21, 2022

Mind Map – Network

IP ADDRESSES
1300 Active
2300 Inactive
3600 Total
Primary schwab.com

All Active Range 104

schwab.com 589 subdomains /104.100.3.63 0 subdomains/ 104.101.138.136 0 subdomains/ 104.101.143.186 0 subdomains/ 104.102.146.220 0 subdomains/ 104.102.159.6 0 subdomains/ 104.102.167.46 0 subdomains/ 104.102.85.15 0 subdomains/ 104.105.238.251 0 subdomains/ 104.107.51.142 0 subdomains/ 104.108.189.106 0 subdomains/104.109.55.43 0 subdomains/ 104.111.179.18 0 subdomains/ 104.112.141.109 0 subdomains/ 104.113.1.227 0 subdomains/ 104.113.141.149 0 subdomains/ 104.113.180.70 0 subdomains/ 104.116.130.213 0 subdomains/ 104.116.88.79 0 subdomains/ 104.117.160.13 0 subdomains/ 104.117.57.212 0 subdomains/ 104.118.66.39 0 subdomains/ 104.122.152.29 0 subdomains/ 104.122.46.10 0 subdomains/ 104.124.235.116 0 subdomains/ 104.125.102.25 0 subdomains/ 104.125.13.74 0 subdomains/ 104.64.236.10 0 subdomains/ 104.64.72.196 0 subdomains/ 104.65.244.109 0 subdomains/ 104.65.72.208 0 subdomains/ 104.67.175.180 0 subdomains/ 104.68.102.242 0 subdomains/ 104.68.111.19 0 subdomains/ 104.68.123.222 0 subdomains

All Active Range 110 - 118

110.45.200.127 0 subdomains/ 111.84.160.89 0 subdomains/ 111.84.161.176 0 subdomains/ 111.84.161.239 0 subdomains/ 111.84.164.54 0 subdomains/ 111.84.165.230 0 subdomains/ 111.84.167.137 0 subdomains/ 111.84.168.3 0 subdomains/ 111.84.188.81 0 subdomains/ 114.108.190.243 0 subdomains/ 115.146.116.224 0 subdomains/ 116.197.26.165 0 subdomains/ 116.197.30.117 0 subdomains/ 116.197.32.130 0 subdomains/ 116.197.34.201 0 subdomains/ 116.197.34.97 0 subdomains/ 116.197.35.129 0 subdomains/ 116.197.35.32 0 subdomains/ 116.197.39.8 0 subdomains

All Active Range 122-157

122.252.131.96 0 subdomains/ 122.252.132.17 0 subdomains/ 122.252.47.61 0 subdomains/ 125.252.217.141 0 subdomains/ 150.101.144.146 0 subdomains/ 150.101.145.173 0 subdomains/ 150.101.146.23 0 subdomains/ 157.197.145.62 0 subdomains/ 157.197.145.68 0 subdomains/ 157.197.147.216 0 subdomains/ 157.197.147.74 0 subdomains/ 157.197.148.191 0 subdomains/ 157.197.148.51 0 subdomains/ 157.197.148.61 0 subdomains/ 157.197.149.73 0 subdomains/ 157.197.149.94 0 subdomains/ 157.197.160.147 0 subdomains/ 157.197.160.188 0 subdomains/ 157.197.160.216 0 subdomains/ 157.197.161.30 0 subdomains/ 157.197.162.153 0 subdomains/ 157.197.162.155 0 subdomains/ 157.197.162.18 0 subdomains/ 157.197.162.215 0 subdomains/ 157.197.163.106 0 subdomains/ 157.197.163.200 0 subdomains/ 157.197.164.121 0 subdomains/ 157.197.164.166 0 subdomains/ 157.197.165.146 0 subdomains/ 157.197.165.24 0 subdomains/ 157.197.166.234 0 subdomains/ 157.197.166.29 0 subdomains/ 157.197.166.57 0 subdomains/ 157.197.167.149 0 subdomains/ 157.197.167.66 0 subdomains/ 157.197.168.133 0 subdomains/ 157.197.169.157 0 subdomains/ 157.197.171.174 0 subdomains

All Active Range 162

162.93.16.13 0 subdomains/ 162.93.16.14 0 subdomains/ 162.93.160.139 0 subdomains/ 162.93.160.44 0 subdomains/ 162.93.160.58 0 subdomains/ 162.93.168.109 0 subdomains/ 162.93.168.44 0 subdomains/ 162.93.180.113 0 subdomains/ 162.93.180.130 0 subdomains/ 162.93.180.155 0 subdomains/ 162.93.180.25 0 subdomains/ 162.93.180.74 0 subdomains/ 162.93.180.91 0 subdomains/ 162.93.180.95 0 subdomains/ 162.93.210.14 0 subdomains/ 162.93.210.252 0 subdomains/ 162.93.211.237 0 subdomains/ 162.93.215.108 0 subdomains/ 162.93.215.119 0 subdomains/ 162.93.215.121 0 subdomains/ 162.93.215.124 0 subdomains/ 162.93.215.137 0 subdomains/ 162.93.215.138 0 subdomains/ 162.93.215.163 0 subdomains/ 162.93.215.164 0 subdomains/ 162.93.215.55 0 subdomains/ 162.93.215.60 0 subdomains/ 162.93.215.9 0 subdomains/ 162.93.215.95 0 subdomains/ 162.93.216.105 0 subdomains/ 162.93.216.89 0 subdomains/ 162.93.217.71 0 subdomains/ 162.93.218.161 0 subdomains/ 162.93.218.71 0 subdomains/ 162.93.220.110 0 subdomains/ 162.93.220.160 0 subdomains/ 162.93.220.163 0 subdomains/ 162.93.220.19 0 subdomains 162.93.220.191 0 subdomains/ 162.93.220.47 0 subdomains/ 162.93.221.110 0 subdomains/ 162.93.221.153 0 subdomains/ 162.93.221.159 0 subdomains

DOMAIN NAMES

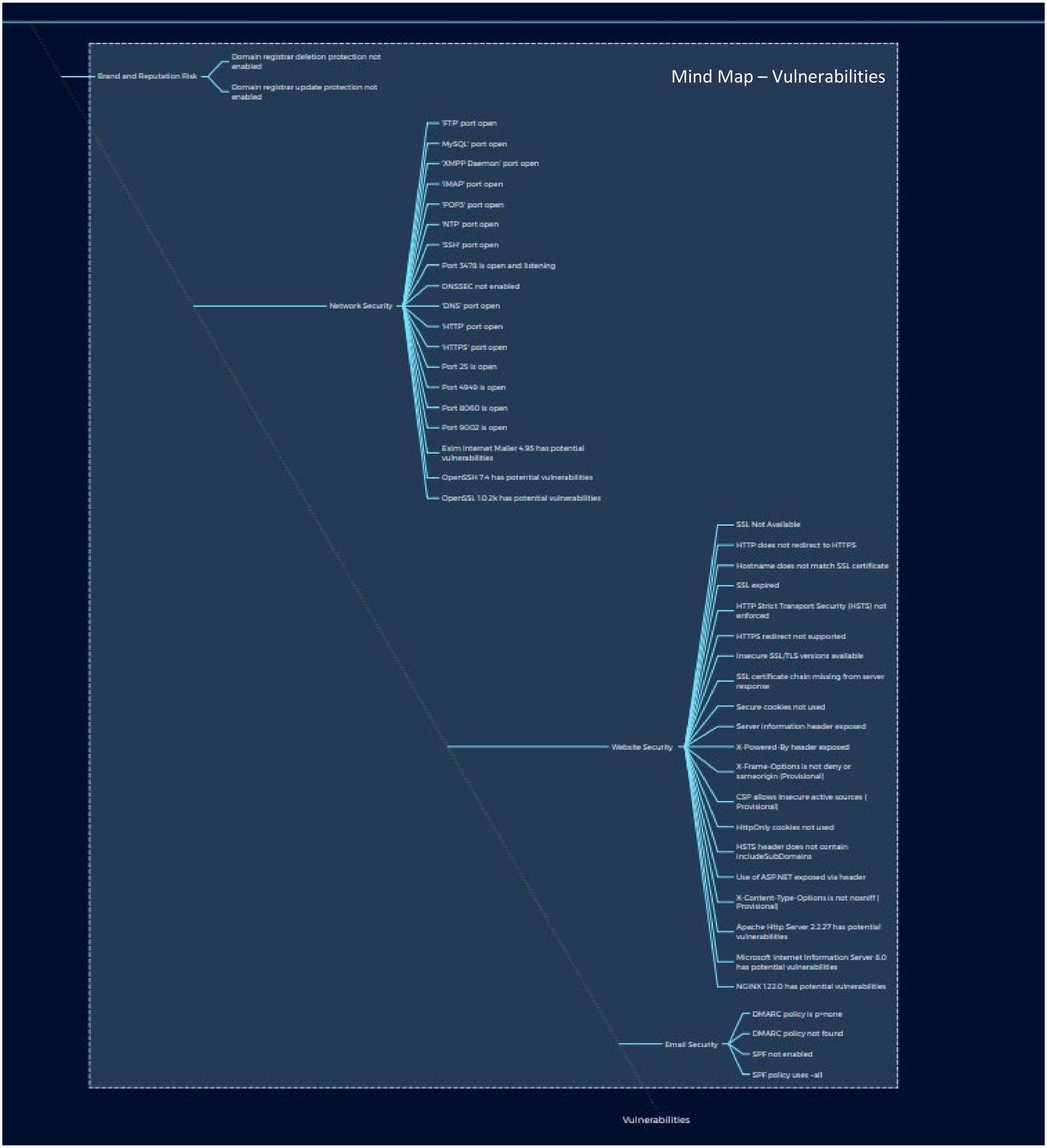
aboutschwabinstitutional.com 0 subdomains/ andersen401k.com 1 subdomain/ charles-schwab.com 0 subdomains/ charlesschwab.com 1 subdomain/ compliance11.com 6 subdomains/ cyber-brokerage.com 7 subdomains/ cybertrader.com 0 subdomains/ iehomeinspection.com 0 subdomains/ nordstrombanking.com 0 subdomains/ ownyourtomorrow.com 0 subdomains/ schwab-global.com 1 subdomain/ schwab.org 0 subdomains/ schwabadvisorcenter.com 0 subdomains/ schwaballi ance.com 1 subdomain/ schwabat.com 1 subdomain/ schwabb.com 1 subdomain/ schwabbankmortgage.com 1 subdomain/ schwabcdn.com 6 subdomains/ schwabdifference.com 0 subdomains/ schwabetfeducationexchange.com 1 subdomain/ schwabfilms.com 0 subdomains/ schwabfranchise.com 1 subdomain/ schwabgolf.com 1 subdomain/ schwabinsurance.com 0 subdomains/ schwabintelligentintegration.com 0 subdomains/ schwabintelligenttechnologies.com 0 subdomains/ schwabplan.com 8 subdomains/ schwabsavingsfundamentals.com 1 subdomain/ schwabsponsorships.com 0 subdomains/ schwabtoday.com 1 subdomain/ schwabtransition.com 0 subdomains/ schwabtransitions.com 0 subdomains/ talktochuck.com 0 subdomains/ telebroker.com 0 subdomains/ thecybertraders.com 1 subdomain

Geolocation
15 Hosting Countries
1398 IP Addresses

- United States 1105 IP Addresses 79%
- Hong Kong 81 IP Addresses 6%
- Netherlands 76 IP Addresses 5%
- South Korea 73 IP Addresses 5 %
- Taiwan 15 IP Addresses 1%
- Malaysia 10 IP Addresses 1%
- Canada 9 IP Addresses 1%
- Thailand 8 IP Addresses 1%
- India 6 IP Addresses < 1%
- Singapore 5 IP Addresses < 1%
- Australia 3 IP Addresses < 1%
- United Kingdom 3 IP Addresses < 1%
- France 2 IP Addresses < 1%
- Czech Republic 1 IP Address < 1%
- Norway 1 IP Address < 1%

DNS Report

NS records listed at parent serversNameserver records returned by the parent servers are:
ns1.schwab.com. [162.93.253.90] [TTL=172800]
ns2.schwab.com. [162.93.195.133] [TTL=172800]
ns3.schwab.com. [162.93.253.171] [TTL=172800]
ns4.schwab.com. [162.93.195.171] [TTL=172800]
a9-65.akam.net. [NO GLUE] [TTL=172800]
a8-64.akam.net. [NO GLUE] [TTL=172800]



Mind Map – Vulnerabilities

Brand and Reputation Risk
Domain registrar deletion protection not enabled
Domain registrar update protection not enabled
Network Security
'FTP' port open
MySQL' port open
'XMPP Daemon' port open
'IMAP' port open
'POP3' port open
'NTP' port open
'SSH' port open
Port 3478 is open and listening
DNSSEC not enabled
'DNS' port open
'HTTP' port open
'HTTPS' port open
Port 25 is open
Port 4949 is open
Port 8060 is open
Port 9002 is open
Exim Internet Mailer 4.95 has potential vulnerabilities
OpenSSH 7.4 has potential vulnerabilities
OpenSSL 1.0.2k has potential vulnerabilities
Website Security
SSL Not Available
HTTP does not redirect to HTTPS
Hostname does not match SSL certificate
SSL expired
HTTP Strict Transport Security (HSTS) not enforced
HTTPS redirect not supported
Insecure SSL/TLS versions available
SSL certificate chain missing from server response
Secure cookies not used
Server information header exposed
X-Powered-By header exposed
X-Frame-Options is not deny or sameorigin (Provisional)
CSP allows insecure active sources (Provisional)
HttpOnly cookies not used
HSTS header does not contain includeSubDomains
Use of ASP.NET exposed via header
X-Content-Type-Options is not nosniff (Provisional)
Apache Http Server 2.2.27 has potential vulnerabilities
Microsoft Internet Information Server 8.0 has potential vulnerabilities
NGINX 1.22.0 has potential vulnerabilities
Email Security
DMARC policy is p=none
DMARC policy not found
SPF not enabled
SPF policy uses ~all
Vulnerabilities

Risk Analysis

Overall, Charles Schwab has good security protection compared to companies in the same industry. We gave Charles Schwab a rating of 'A'. However, there are areas that need immediate attention. Three critical risks were identified that put Charles Schwab in immediate danger of a data breach. These are the lack of SSL certificate and the open FTP and MySQL ports. There were high risks identified that need to be remediated immediately. These are the lack of HTTPS redirect, the DMARC policy, and the open XMPP port. Several medium risks were identified that could lead to more vulnerabilities, and several low risk areas were identified that could use improvements.

Recommendations

Website Security

Websites are hacked multiple times every day. According to the 2022 annual report of SiteLock a website is attacked on average 172 times a day. SiteLock analyzed about 14 million websites and found that the number of attacks has doubled over the past year and over 60% of the sites analyzed were vulnerable at some point during the year.

Our analysis discovered 1 critical and 1 high risk vulnerability that puts Charles Schwab at immediate risk of a breach and should be corrected immediately. Based on our findings we are making the following recommendations for Website Security:

- Install valid SSL certificates on affected domains. Websites without valid SSL certificates are shown as 'non-secure' in modern browsers and will rank worse in Google and other search engines.

- Redirect users and search engines to the HTTPS page or resource with server-side 301 HTTP redirects. This ensures all communications are encrypted, preventing certain man-in-the-middle attacks.
- The website needs to stop exposing the X-Powered By header. This reduces the risk that an attacker will be able to find an exploitable vulnerability in the software running the website.
- Check affected domains to determine whether the Apache Http Server 2.2.27 vulnerabilities are present and if so, apply the required patch or work around to fix security issues.

Email Security

The number of attacks by email is increasing. According to statistics, email is responsible for 91% of all cyber-attacks and 94% of all malware (Source: Deloitte). The Register reports that phishing attempts went up 100% in one month in the Middle East leading up to the Word Cup. We are recommending the following to help mitigate the number of email attacks from reaching the users at Charles Schwab.

- The DMARC policy should be set to p=quarantine and email deliverability should be monitored for unintended consequences, such as legitimate email being sent to spam. Once the domain owner is sure nothing is wrong, they should change to p=reject.

Network Security

More and more of the world is getting connected to the Internet and cybercrime is on the rise. Parachute IT company reported that the cost of cybercrime averages $1 trillion a year and amounts to 1% of the global GDP with $18.3 million in the financial sector alone. Our analysis found 2 critical and 1 high security risks with open ports. Open ports leave a door open for a skilled attacker to infiltrate a network. To reduce the attack surface of the network we recommend the following:

- Closing the open ports will reduce the risk of an attack

Malware & Phishing

As reported by the FBI's Internet Crime Complaint Center in their 2020 Internet Crime Report, the number of phishing attacks doubled from 2019 to 2020 resulting in over $54 million in losses. These attackers are social engineers using tactics that rely on human ignorance, emotions, or trusting nature to successfully trick employees to gain information and data and to introduce malware. To help increase employee awareness of such tactics and thus reducing the number of successful phishing and malware attacks we recommend the following:

- Providing more regular training to promote awareness in employees and contractors will strengthen security at the first point of contact with phishing emails and social engineering tactics.
- Perform your due diligence of any 3rd party contractors before entering into an agreement with them by requesting annual vulnerability assessments of their systems and documentation of their response and remediation plans in the case of a breach.

Costs

Duo Beyond Training

Duo Beyond allows you to identify corporate vs. personal devices with easy certificate deployment, block untrusted endpoints, and give your users secure access to internal applications without using VPNs.

Cost per user per month	$ 9
Estimated number of users	$ 32,000
Total monthly cost	$ 288,000
Total quarterly cost	$ 1,152,000
Total yearly cost	$ 3,456,000

KnowBe4 Training

KnowBe4 is the world's largest integrated platform for security awareness training combined with simulated phishing attacks.

**Note: The pricing estimate may vary as for any more than 3000-5001 seats you must request a quote from KnowBe4

Cost per seat (price varies by number of seats)	$ 10
Estimated number of users	$ 32,000
Total monthly cost	$ 26,667
Total quarterly cost	$ 106,668
Total yearly cost	$ 320,000

Legal/Compliance Issues

The findings of our vulnerability assessment resulted in minimal critical and high-level security risks and the recommendations we are making to address these have no legal or compliance implications.