Cybersecurity

Name

School or Institution Name (University at Place or Town, State)

**Suspicious Activity Report**

**Introduction:**

Cyber-criminals are always trying to develop new and sophisticated attacks to compromise as many information technology systems as possible. Despite the continuous improvements in cybersecurity technologies, the cyber-attacks are continually increasing not only in numbers but in the strength as well. None of the departments or institutions powered by the information technology systems are immune to cyber-attacks. Most of the time cyber-attacks are carried out on large-scale organizations for monetary benefit. The financial services sector is one of the major targets of cybercriminals. pFinancial institutions develop a suspicious activity report if they observe any unusual activity within the system (Fligstein & Roehrkasse, 2016). The report helps in the detection and prevention of highly sophisticated attacks. Suspicious activities observed in a financial institution are often related to asset misappropriation, cybercrime, accounting, money laundering, bribery and, corruption. Each main category may have many subcategories with the varying potential of causing financial loss. Suspicious activity has been observed by the financial services sector details of which are listed below;

**Threat:**

Cyber-criminals are always trying to target financial institutions using sophisticated attack vectors infiltrating existing protection capabilities of the system. One such activity includes phishing attacks. Phishing is a form of cyber-attacks in which hackers and cybercriminals use look-alike web links to trick users to provide confidential information. Most of the institutions providing financial services to end users rely on internet-based technologies. Such as online accounts providing all of the banking facilities over the internet. End users can access their accounts and perform banking related activities by providing credentials to authenticate their identity to a remote server. Phishing attacks use the web links of online banking services to trick users to provide their confidential information such as usernames and passwords.

**The motivation of Threat Actors:**

Attackers have the motivation of collecting as many credentials as possible through their phishing campaigns for monetary benefits. Once, an attacker has access to username and password; he can use the details to access the system as a legitimate user. To broaden the scope the malicious activity, the attackers not only forged look-alike links but also utilized spam emails. Emails that look like legitimate ones by the financial institutions but actually were from the attackers (Levi & Burrows, 2008). Emails contain the links to reset the password for online accounts and end users were fooled by the criminals. Once the user clicks and opens the fake link, he is asked to provide existing username and password which is then sent to the attacker command and control server and nothing happen at the user's screen.

 Incident was reported to customer services of different financial institutions by consumers that they are receiving many emails from their financial institution. After a large volume of complaints, the matter was investigated by the experts in the related sector, and they found that phishing attacks are targeting the financial services sector. Such campaign if successful can be used to fund terrorist organizations.

**Vulnerabilities in System:**

Most of the time cyber-attacks are successful due to inherent flaws of the software system. During early stage investigation, it was revealed that most of the critical machines in the sector were powered by outdated software abandoned by the vendor. Vendors were not releasing security patches for the software products as per the product support life cycle was ended for legacy systems. Targeted organizations failed to upgrade their system within the time frame of product life-cycle. Attackers exploited the security loopholes in the system to target innocent users. Financial institutions also noticed suspicious transactions using online systems that raised many concerns among information technology professionals working in the same sector.

 Many systems were not having access to online update servers leaving them vulnerable to potential attacks. During the last two years, ransomware attacks used the vulnerabilities in the system to target the financial services sector of the governments in the world. Following snapshot shows the percentage of reported frauds in the financial sector during 2009 and 2011 (Cummings, Lewellen, McIntire, Moore, & Trzeciak, 2012).

It is evident from the above graph that cybercrimes account for most of the financial frauds in the financial services sector. It can only be reduced by useful risk identification and mitigation plans to overcome vulnerabilities in the system.

**Impact on Critical Infrastructure:**

Financial services sector represents a vital component of the nation's critical infrastructure. Any potential attack on this sector will cause severe loss to the overall critical infrastructure of the country as well. The department of treasury works with all relevant agencies either state or local and private sector to improve the ability of the sector to prepare for and mitigate humanmade threats to the sector including cybercrime (Johansson & Carey, 2016). Financial institutions provide a broad array of services from the largest institutions to community-based banks. Allowing them to make deposits and transfer funds to other parties. Depending on the critical nature of the sector, any successful attack on the institutions such as observed in the phishing campaign will be able to shut down the whole financial system. Such a massive loss and risk is not affordable to any institution either public or in private sectors.

**Actions Taken to Prevent the Attacks:**

 It was identified that the attackers could exploit the vulnerabilities in software systems of the sector, it was decided to update all of the existing software to mitigate the potential risks of cyber-attacks. The updates to the existing system were planned in different phases because it is not possible for large-scale organizations to update existing systems quickly. Moreover, backward compatibility issues were also accounted for legacy systems. During the first phase of corrective actions of the mitigation plan, systems running obsolete UNIX based applications were updated to the modern operating system.

 Authentication mechanism for the internet-based services has been changed because traditional password-based authentication system can be infiltrated by the man in the middle attacks. In the identified activity criminals were able to collect credentials by fooling the end users. To overcome the problem, digital certificate-based authentication system and two-factor authentication have been made compulsory for all of the institutions in the financial services sector. Two-factor authentication has mitigated future attacks (Reurink, 2018). Whenever a user tries to access an online account, a notification will be sent to the mobile device of the user with a one-time password. The expiry time of the one-time password will be very short to prevent brute force attacks as well.

 Therefore, even if the credentials of a particular entity are compromised the attacker will not be able to authenticate on the server of financial institutions without the consent of the concerned party. The measure has eliminated the risk of all future attacks of this kind. User awareness campaigns will also help people to learn more about the tactics used by criminals to sabotage the system. Digital signature-based authentication at the application level will prevent online fraud activities by malicious and terrorist actors because the communication will be encrypted with advanced encryption standard using 256 bits length of the key. The attackers will not be able to compromise the system even if they exactly know the underlying algorithm used for encryption unless the encryption keys are kept secret. All of the preventive actions have mitigated the risks of suspicious activity observed for the future as well making the system more secure and robust in performance.

**After Action Report**

 Financial services sector always remain a top target for criminals trying to use hacking tools for monetary benefits. Cybercriminals always try to invent sophisticated attack techniques to compromise a large number of computers and related information technology infrastructure. Phishing attacks are an important technique used by criminals to trick users of online services. Attackers made people click on forged links to obtain their login credentials. Stolen credentials were then sold on the black market and used by criminals to authenticate on servers of financial services. There were no restrictions on authentications of users by the servers. Reports by the users were investigated, and financial institutions found suspicious transaction happening in the network.

 Attack campaigns were successful due to the vulnerabilities in the system. It was investigated that most of the information technology infrastructure in the sector was powered by obsolete software leaving them a potential target for cyber-attacks. Targeted attacks can break the whole financial system. Therefore, mitigation steps were taken to reduce the threat surface. During the first phase of the corrective actions, all of the outdated systems were updated to the latest available software programs available with the vendors of legacy systems. The move was helpful in patching the exploitable loopholes in the information technology infrastructure of the sector.

 To specifically overcome the issue of phishing attacks, two significant changes were introduced in the system. The first change was the implementation of two-factor authentication for online financial services. In this way, whenever the user will try to access the online financial system, a one-time password will be generated and communicated to the owner of the service via a different channel, e.g. phone or email. The approach will render phishing campaigns useless. Even if the attacker has access to the login credentials of the user, he will not be able to authenticate his identity without having access to the one-time password. There can be a problem in the one-time password generation mechanism because the attackers can brute force the service to bypass the two-factor authentication. The risk of brute force attack was mitigated by the implementation of the synchronous clock at the server end to generate short lived passwords. Each password generated by the authentication server will be valid for a very short time only.

 The second thing was the implementation of a digital signature based authentication system to prove the identity of the client to the server. The implementation of the measure mitigated the risk of man in the middle attacks to steal the login credentials of the users. With the implementation of the system, the password and other credentials of the end user are not transmitted over an insecure channel (Moore, Dynes, & Chang, 2016). All the details are first encrypted using a digital certificate using the private key of the sender. Digital certificates are issued by a trusted third party playing the role of authenticator. The sender encrypts the contents of the message with a private key corresponding to the digital signature. On the server side, the message is decrypted using the server private key along with the public key of the certificate. The public key is known to the overall system while the private keys are only known to individual machines.

 The public key cryptographic mechanism has mitigated the risk of theft for the credentials of the user. The attackers will never be able to collect the original message even if they are aware of the underlying encryption algorithm as well. It is true as long as the private keys are kept secret. If this line of defense against cyber-attacks is somehow compromised then combined with the two-factor authentication system, the mitigation techniques will render most of the attacks useless (Etzioni, 2011). The financial service sector is an essential component of the nation's critical infrastructure. Ensuring the confidentiality, integrity, and availability of the data in the financial services sector is inevitable. Without appropriate risk reduction and mitigation plans, these objectives are impossible to achieve.

 With the improvement in protective and risk mitigation techniques, cyber threats are also increasing not only in their number but in complexity as well. During the last two years, ransomware campaigns caused billions of dollars in loss due to the encryption of critical data by the criminals. Criminals locked the institutions out of their systems and demanded ransom money to restore access (Martin, Ghafur, Kinross, Hankin, & Darzi, 2018). The exponential increase in cyber threat landscape has made it inevitable for the financial services sector to implement rigorous mitigation techniques to protect critical infrastructure. User awareness campaigns must also be initiated to educate general users of the system that how to differentiate legitimate web links from fraudulent websites.

 There will always be tradeoffs between the security and efficiency of the system. Too much security will also impact the system negatively. Appropriate measures must be devised to make the sector more beneficial to end users and governments as well. Latest innovations in cybersecurity such as artificial intelligence and machine learning algorithms will help in overcoming these potential issues. Careful risk identification and appropriate risk mitigation plans must be part of the strategic planning of institutions operating in the financial sector. Otherwise, any potential breach of financial information can cause severe damage to the nation’s critical infrastructure.

References

Cummings, A., Lewellen, T., McIntire, D., Moore, A. P., & Trzeciak, R. (2012). *Insider threat study: Illicit cyber activity involving fraud in the US financial services sector*. CARNEGIE-MELLON UNIV PITTSBURGH PA SOFTWARE ENGINEERING INST.

Etzioni, A. (2011). Cybersecurity in the private sector. *Issues in Science and Technology*, *28*(1), 58–62.

Fligstein, N., & Roehrkasse, A. F. (2016). The Causes of Fraud in the Financial Crisis of 2007 to 2009: Evidence from the Mortgage-Backed Securities Industry. *American Sociological Review*, *81*(4), 617–643.

Johansson, E., & Carey, P. (2016). Detecting fraud: The role of the anonymous reporting channel. *Journal of Business Ethics*, *139*(2), 391–409.

Levi, M., & Burrows, J. (2008). Measuring the impact of fraud in the UK: A conceptual and empirical journey. *The British Journal of Criminology*, *48*(3), 293–318.

Martin, G., Ghafur, S., Kinross, J., Hankin, C., & Darzi, A. (2018). WannaCry-a year on. *BMJ: British Medical Journal (Online)*, *361*.

Moore, T., Dynes, S., & Chang, F. R. (2016). Identifying how firms manage cybersecurity investment. *University of California, Berkeley*.

Reurink, A. (2018). Financial fraud: a literature review. *Journal of Economic Surveys*, *32*(5), 1292–1325.