Jay Vimalbhai Trivedi

Student ID:218449725

Abstract

Analysis of the comodo security fraud attack and its various security issues imposed on a medium enterprise.

SIT735 Assignment 1

Analysis report

**Executive summary**

Internet has become one of the key ingredients to our day-to-day lives. The use of internet in our lives has reached beyond our imagination starting from browsing the net for extracting information, interacting e-mails, doing financial transactions, social media posts and many more. It is basically a global system that is interconnected through various computer networks with the help of various internet protocol suits (TCP/IP). Internet is also an insecure platform/channel to transfer a confidential information/transaction from one end to the other. With the increased usage of the internet there has been vast number of internet security attacks such as Man in the middle attack (MitM), malware attack, Denial-of-service (DoS) (Blog.netwrix.com 2019) attack and many more that has been occurring on a daily basis. Similarly, one of the attacks this report throws light upon is the Comodo security fraud attack occurred in the year 2011 (Raiu, 2012).

**Introduction**

Cyber security plays an essential role in the world where confidential information/transactions are occurred on a daily basis via the internet which also acts as a magnet for various malicious security attacks. Comodo security provides a platform to its customers where its system and data related threats are kept at bay. The company provides protection across LAN, web and cloud platforms (Comodo.com 2019). In 2011 the company underwent a cyber security attack which compromised its infrastructure and security. The aim of this investigation is to analyze various IT problems, risks that has been occurred during the attack and to provide a feasible, cost effective solution in-order counterpart these attacks in the future.

**Body**

Secure socket layer (SSL) is a medium through which the sensitive information is passed/transferred upon from one user to the another. Most of the processes such as electronic commerce, electronic business and electronic government is secured through SSL. It is also responsible for the lock icon at the corner of your web browser. Comodo SSL certificates provides their customers a secure transaction with the help of strong encryption. Although, in the year of 2011 an attacker attacked the comodo cyber security by compromising the registration authority (RA) leading to illegal distribution of various secure socket layers (SSL) certificates (The Inquirer 2019). The attacker generated nine SSL certificates of the well-known company websites such as mail.google.com, login.yahoo.com, addons.mozilla.com and login.skype.com (Raiu, 2012) (The Inquirer 2019). Deriving the fact that the SSL certificates doesn’t guarantee the security of communication on the internet. By taking certain steps the company revoked those certificates and traced back the origins of the attacker to be found in Iran (The Inquirer 2019).

One of the key issues faced by Comodo was the leakage of the username and password by one of their trusted partners in South Europe (The Inquirer 2019). Similarly, this issue would occur at a great extent in the medium enterprise (employing up to 100 employees). Because of the limited number of employees in the enterprise it would directly affect to the quality of technology it works up on. There might be cases where the employees would share their username, password within their work network or even outside through any online means such as social media, mail etc. This can easily be an attraction to the attackers/hackers to extract them by deploying various security attacks such as Man in the middle attack, Denial-of-service (DoS) and many more (Blog.netwrix.com 2019). This can also impose a great threat in the transfer of confidential transaction occurring within or out of their network. It would also lead to leakage of confidential data of a higher post personnel such as CEO, chairman that would result in downgrade of the enterprise.

After the attack the company traced back its origin with the help of the hacker’s IP address and was found that the attack was made from Iran (Raiu, 2012) (The Inquirer 2019). This clears the fact that the attack was made from a remote location in Iran. This draws attention with one of the issues known as Virtual Private Network (VPN) (How-To Geek 2019). VPN mostly provides a platform allowing to create a secure connection to another network across the internet. It is mostly used to access a region restricted website and even to protect your browsing activity from the public. Similarly, by not deploying any proper measures on the access/usage of the confidential data outside the enterprise publicly it would probably result in data loss and transaction fraud. Restrictions should be made for each employee that the access of the data should be done with the enterprise territory to prevent any future fraud.

After the break of the comodo fraud hack, big brand companies that were being affected in the attack such as Google, Mozilla and Microsoft made changes in their browser so that it could recognize and eradicate any fraud certificate in-order to avoid any hack soon (Riva Richmond 2019). Small enterprise with a limited quality technology also possesses this threat of being attacked by the hacker if the browser they are working upon is of an older version. Sharing of any information on that browser may lead to confidential data loss or any kind of transaction fraud. This is also a gateway to vivid viruses, trojans and malware to enter into the existing system and make it more vulnerable to operate upon.

The enterprise with a limited employee flow seldom deploys a default allow security posture that allows the traffic that isn’t showing any bad behavior enter into the computer network. Most of threat that hasn’t shown any malicious effect enter the network not posing any effect in the beginning (Comodo News and Internet Security Information, 2019). But after a specific time interval, it starts showing its malicious effect and corrupts the network slowly. This leads to many network related issues including network breakdown.

The limited amount of employee in the enterprise has a direct relationship causing effect on its technological expenditure. In case of a virus or malware, more emphasis is laid on the detection of them rather than the prevention (Comodo News and Internet Security Information, 2019). Another reason for that is not using a well-equipped or up-to-date antivirus and even in the worst scenario not having one. This hinders various confidential transaction flow and even leakage/loss of data.

Lastly the employees are not very well equipped with various cyber security practices. That is responding to an unknown email from a user, opening an attachment that have unknown consequences. There are individuals that may seek harm to these enterprises and deploy various malicious content along with these attachments. Opening to these would cause a downgrade in the system network and various security attacks (Comodo News and Internet Security Information, 2019).

**Solution**

The systematic approach to tackle the various security and IT issues faced by the enterprise is listed below.

**A strong password protection policy**

Hacking the username and the password of a high post personnel has been a common thread for the attackers to enter into the system network. A mandatory code of conduct should be deployed in making a strong hack free password for each employee working in the enterprise. The password should have a minimum of 12 characters or more; includes numbers, symbols, capital letters and lower-case letter, it shouldn’t be dictionary obvious so that it could easily be found out and the last but not the least it should not have obvious substitutions (How-To Geek, 2019). Even emphasis should be laid on the use and regulations of the password where the personnel can’t share their password outside their work environment. And in the worst-case scenario if the personnel have to make a confidential online transaction which urges to use their password credentials then the security protocol should be double checked.

**Nonce (a number used only once)**

A secondary substitute for a strong password is Nonce. A nonce is a number used only once hence rather than using a strong password each employee should be well equipped with the use of it. In case of a confidential data transfer or transaction between two parties nonce should be used to minimize any cyber threat/attack keeping the process easy flowing (Nick Patterson, S779 Masters in IT Professional, PowerPoint Slides, 21 August 2019).

**Secure Socket Layer (SSL)**

The prime focus of an enterprise with a handful of employees providing electronic commercial transaction should be its communication security. Secure socket layer (SSL) is a cryptographic layer that provides communication security. SSL is also responsible for the little lock icon that is found at the corner of the website which is also known as HTTPS (Hyper Text Transfer Protocol Secure). Mainly used to secure electronic services, electronic commerce, electronic business etc. For any online transaction the first and foremost line of conduct is securing the communication protocol. With any minute breach in between could cause the enterprise a heavy loss. The stronger the SSL, more secure the transaction (Nick Patterson, S779 Masters in IT Professional, PowerPoint Slides, 21 August 2019).

**Virtual Protection Network (VPN)**

A strict rules and regulations should be deployed regarding the use of VPN outside the work environment. Otherwise the enterprise’s own employee can easily get into the network using a VPN outside the work environment as he/she also possess necessary credentials to extract confidential data from the network. This can also impose a threat in case of a huge online transaction occurring between two strong parties. Penalties should be applied to those who uses VPN outside the network with a negative or harmful intent (How-To Geek 2019).

**Default-deny security posture**

Allowing a heavy traffic of data to flow inside the enterprise that hasn’t shown any malicious effect in the beginning. But by passing of a certain amount of time interval that unwanted data causes various network breakdown and may impose a threat. Deploying a default deny security posture automatically blocks away any unwanted data that is not recognized as safe. This minimizes the risk of new entrances of any malware, trojan horse to enter into the system keep them at bay (Comodo News and Internet Security Information, 2019).

**Updating the web browser version**

Using the older version of the web browser is an open entrance for various virus, malware into the computer network and can lead to corruption of various important data, files, transaction records and many more. By updating the web browser version minimizes the risk of entrance and reduces any cyber threat from entering the network. The employees should keep their web browser version up-to-date as it can also cause a threat for any on-going transactions (Comodo News and Internet Security Information, 2019).

**A strong antivirus which makes detection and prevention together**

In the era of cyber-attacks and various virus threats, a strong antivirus plays a role of a lifeline for any company, organization and even for a small enterprise. Any of them is incomplete without any antivirus installation. Not only the antivirus should be installed but it should also be of the latest version in-order to tackle any new viruses, malware deployed by the attackers. One of the main uses of it is that as soon as it detects any threat it automatically prevents it from entering the network. Hence prevention and detection both goes together (Comodo News and Internet Security Information, 2019).

**Conclusion**

The report mainly analyzes the comodo fraud security attack and imposes the various IT security threats and issues to a medium enterprise doing electronic commercial transactions. Keeping in mind various security risks and threats stated above there exists multiple cost-effective, feasible solutions that must be kept in mind for any further issues. By deploying these solutions would benefit each organization and even a small enterprise having a handful number of employee workforce.

**Recommendations**

By minutely analyzing the above scenario the organization/enterprise must undergo the following recommendations in-order to survive any cyber-attack or threat.

* The enterprise should be well-equipped with the existing new technology regardless of the employee workforce.
* Each employee should be aware of the prevailing threats in the market and should know how to skillfully deploy certain measures if any arose.
* Strict rules and regulations should be embedded within the enterprise network to keep the workflow easy going.
* As the enterprise is based on an electronic commercial transaction, the first and foremost line of conduct is the communication security.
* Secondly, the enterprise should be well protected internally with an up-to-date and powerful anti-virus that would act as a wall between the virus threats, hackers to infiltrate into the network.
* A strong password protection policy should be implemented along with a sharing criterion even in the outside of the network.
* A frequent update should be made to all the software and in the security communication protocols that would act as a strong layer against any upcoming threat in the future.
* Diagnosis should be made run on a regular basis that would keep track of the health of the network and its processes.

**References**

* Raiu, C. (2012). Cyber-threat evolution: the past year. *Computer Fraud & Security*, 2012(3), pp.5-8.
* The Inquirer 2019, Comodo admits hackers issued fraudulent SSL certificates, date retrieved 20 August 2019, <<https://www.theinquirer.net/inquirer/news/2037113/comodo-admits-hackers-issued-fraudulent-ssl-certificates>>
* How-To Geek 2019, What Is a VPN, and Why Would I Need One?, date retrieved 20 August 2019, <<https://www.howtogeek.com/133680/htg-explains-what-is-a-vpn/>>
* Blog.netwrix.com 2019, Top 10 Most Common Types Of Attacks, data retrieved 20 August 2019, <<https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/>>
* Comodo.com 2019, Comodo Cybersecurity | Innovative Cybersecurity Platform, date retrieved 20 August 2019, < <https://www.comodo.com/comodo-cybersecurity.php?track=14583&af=7639>>
* Riva Richmond 2019, Attack on Comodo Sheds Light on Internet Security Holes, date retrieved 20 August 2019, < <https://www.nytimes.com/2011/04/07/technology/07hack.html>>
* Comodo News and Internet Security Information 2019, Top 5 Common Pitfalls in your Security Stack, date retrieved 21 August 2019, < <https://blog.comodo.com/5-most-common-pitfalls-in-security-stack/?af=7639#_ga=2.127845133.106060672.1566192925-1920604278.1566192925>>
* How-To Geek 2019, How to Create a Strong Password (and remember it), date retrieved 21 August 2019, < <https://www.howtogeek.com/195430/how-to-create-a-strong-password-and-remember-it/>>