International Journal of Management, IT & Engineering
Vol. 7 Issue 8, August 2017,
ISSN: 2249-0558
Impact Factor: 7.119Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Securing Walls from Fire

By
Dr.Rajnish Kumar, Research Fellow
Faculty of Social Science (Economics)
B.R.Ambedkar Bihar University, Muzaffarpur-Bihar

Abstract:

The world today stands a connected place today. Internet and the virtual world have created a pseudo existence where humans stand very close to each other. And as it has been the norm of ages, the need to secure the most important of resources call in as effort. Whether it is food, gold or the absolutely precious flow of data, there is a need to tie a lace around its edges.

Though often human effort to this regards keeps on failing on account of constant intrusion through security, it is in human nature to keep on trying and developing new standards of protection.

The importance and value that internet carries today makes it obvious to work in direction of laying down firewalls and securing websites to the best of our possibilities. Yes internet has made human world much vulnerable than it ever was, but the values it brings in heavily outmatches its banes. And as has been the norm of history, no such things ever could be restrained.

Internet is everywhere today and further expansion is the only possibility. And that makes the road ahead very clear. Strive to make the expanse of internet as secure as it could possibly be.

Robert Mueller, the Former Special Counsel for the United States Department of Justice once said, "There are only two types of companies: those that have been hacked and those that will be. Even that is merging into one category: those that have been hacked and will be again."

There is some deep hidden truth in this respective statement of his. A world wide survey over companies of all sorts might prove his second statement wrong. But the first one cannot be denied. And hence becomes of utmost importance the need to protect our systems. But not just protecting the nodes is required, but making the entire network free of breaching is of utter eminence.

Keywords: Internet, Software, Security.

International Journal of Management, IT & Engineering
Vol. 7 Issue 8, August 2017,
ISSN: 2249-0558
Impact Factor: 7.119Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

1. Securing Walls from Fire:

When the Houthi rebels attacked facility locations of Saudi Aramco, the Kingdom of Saudi Arabia's State owned Oil Production Company;it affected 50 percent of production of one of the biggest oil producing nation in the world. It not only increase fuel prices across the globe but also projected the vulnerability to technology that modern world can be open to. Explosives were dropped off using drones that had handlers sitting far away. All the work was carried out using modern concepts of Internet of Things, sensors, actuators and a whole lot of internet. And for all the threats that Saudi Aramco might be exposed to through such physical attacks, this isn't the first occasion when their security was breached on such an alarming scale.

Let's run our clocks back a little. In the holy month of Ramadan- year 2012, on the 15th day of August, over 30,000 computer systems running on Microsoft Windows started overwriting themselves. Numerous of these systems bore the American flag on their screens. All these systems were owned by Saudi Aramco and the cyber attack led the government into buying almost 50,000 new servers from eastern Asia to replace the existing futile ones. This not just pushed server prices up across the globe but also affected adversely the company's functionality. Delayed supplies and resorting to phone call based business transaction led to losses in billions to the company. '*Shamoon'* or *W32.DistTrack* was the modular computer virus that had brought down one of the biggest companies in the world.

The term ***cyber security***has grown insignificance over the past two decades and the increasing intrusion of computers into functionalities of widely dissimilar industries is slowly creating a unified system. Of verymuch importance here is the ease of work that comes along with software and how it has enabled trans-globe trade and connectivity. IT industry today prospers and employs millions. Not just industry and governments, the all so sceptical of all military has also completely integrated networking into its operations. But for all the great things that happen,

there are their darker sides as well. And although computers would always be unfortified from some front, there are those who stand guard to protect precious information.

1.1 Network Security:

What is network security exactly? It involves setting down standards and policies that decide how a network could be protected from the variables of semi-controllable or un-controllable premises, possible misuse, and attack, modification of text, unauthorised access and denial of a computer network. It provides safeguard to working and employs software as well as hardware components. A network could be privately held or may lie in public domain.

International Journal of Management, IT & Engineering
Vol. 7 Issue 8, August 2017,
ISSN: 2249-0558
Impact Factor: 7.119Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

1.2 The Basic Idea

Often the first step is a form of authentication of the user. Usernames and passwords are the most common forms. Fingerprint scanning, retinal scans and one time password verification are the new trends to it. Often a physical component like a digitised key, as in the form of an ATM card, could also be employed to verify user identity. This leads the user up to the firewall which then takes the decision as to what part of the entire system can the user be given access to. Here anti-virus software is employed to fight any malicious entity that the user or other source might have introduced. The foreign entity might be stopped or reported for remedial steps to be taken.

Data can be plaintext, that is transferred in its original form, or encrypted, that is transferred after altering its original form. While encrypted data does provide some resistance to mishandling and needs certain expertise if attacks are to be carried out, plaintext is absolutely volatile and can be easily affected by foreign sources.

1.2 Forms of Attack:

The attacks that a network can be exposed to are broadly of two types- passive and active:-

1.3.1: Active Attack: When the intruder can modify the original message or create a false message. Active attacks are often difficult to get hold of, although they are detectable.

- **They are further classified as:-**

- Masquerade - When a foreign unauthorized entity pretends to be an authorized one.
- Modification –Alters the original message
- Denial of Service (DOS) - When a foreign unauthorized entity prevents an authorized entity formusing a service.

1.3.2: Passive Attack: When the attacker is more concerned with reading and monitoring of data.Passive attacks are harder to detectand hence should rather be prevented than detecting later.

- **They are further classified as:-**
  - Release of message content – When a foreign unauthorized entityreleases confidential data publically over anetwork.
  - Traffic Analysis – When a foreign unauthorized entitycompares between encrypted messages tofind the original message

1.4 Important Terms:

1.4.1: Cryptography:

Cryptography is a retaliatory form of protection against possible threats to data moving over a network. The plaintext here is converted into encrypted form by the cipher and the transported over the network. A special key is present with both, the source and the destination cipher which helps decrypt the plain text once it has reached its destination

1.4.2: Hashing:

Hashing has a different role in cryptography. Instead of being used as a way to encrypt and decrypt (two-way cryptography) it's used as a digital signature and uses one-way encryption, so in theory it's extremely difficult – if not impossible – to reverse the message.

1.4.3: Network Security Key:

The network security key, also known as the Wireless network password is that pass code which allows the user to gain access to the wireless network.
While for small scale applications as in the form of *Wi-Fi* set up in a house, the password is often mentioned on the router or is provided to the customer while installation. A connected device can also look up the password once he goes through the network settings.

1.4.4: Firewall:

Firewall is the line of control between the internet user and the internal network of a system. There are certain set of rules that are laid down by it that any incoming user has to follow if he wishes access to the internal network. There could a software firewall and/or a hardware firewall. Hardware firewalls are utilised for higher grade security in industrial and corporate sector.

1.4.5: Intrusion Detection System:

Intrusion detection systems alarm the user at the arrival of malicious software. They tend to reset the system in order to save the IP address from possible blockade and drop packets.

They carry out continuous scrutiny of the network and are the protective sheath of the node at use.

1.4.6: Content Filtering:

Private networks and often corporations have to deal with pornographic, violent or otherwise unwanted mails and web pages.

Often as a part of firewall itself, content filters keep such undesirable content away from the system and effectively keep the network or personal computer clear of them.

1.5 Forms of Security Required:

1.5.1: Denial of Service attack- This form of attack injects a huge mass of data on the serverand disrupts normal traffic. The best protection against such attack is early detection, providing a large bandwidth and asking ISP provider for help.

1.5.2: Client Security- Trojan attacks, entry of worms, viruses, unauthorized eavesdropping etc.Security through Obscurity(STO), or preventing third party from gaining knowledge of internal working of the system, installing password schemes and adopting newer methods of

biometric and retinal scans help protect clients. Often anti-virus could also be installed on the client node for protective measures.

1.5.3: IoT Security-Mechanical or Electronic devices working as a part of aweb based networks are prone to attacks. Using Virtual Private Network (VPN), using passwords, using internet security software, providing cryptographic keys and encrypting data at rest and in transit are some methods to mitigate the possible threats.

1.5.4: Network Access Control- It basically sets prescribed rules that a node would have to adhere to if it seeks to access the demanded data. This not only implements the security policies by force but also eradicates attacks like Non-zero-day attack.Impulse Safeconnect, Auconet BICS, ForeScout CounterAC and Pulse Policy secure are some of the many available NAC solutions.

1.5.5: IPv6 Security- Internet Protocol (IP) allows systems to connect online.It supports end to end encryption and at the same time makes port scanning harder.In IPv6, it is possible to bind a public signature key to an IPv6 address.

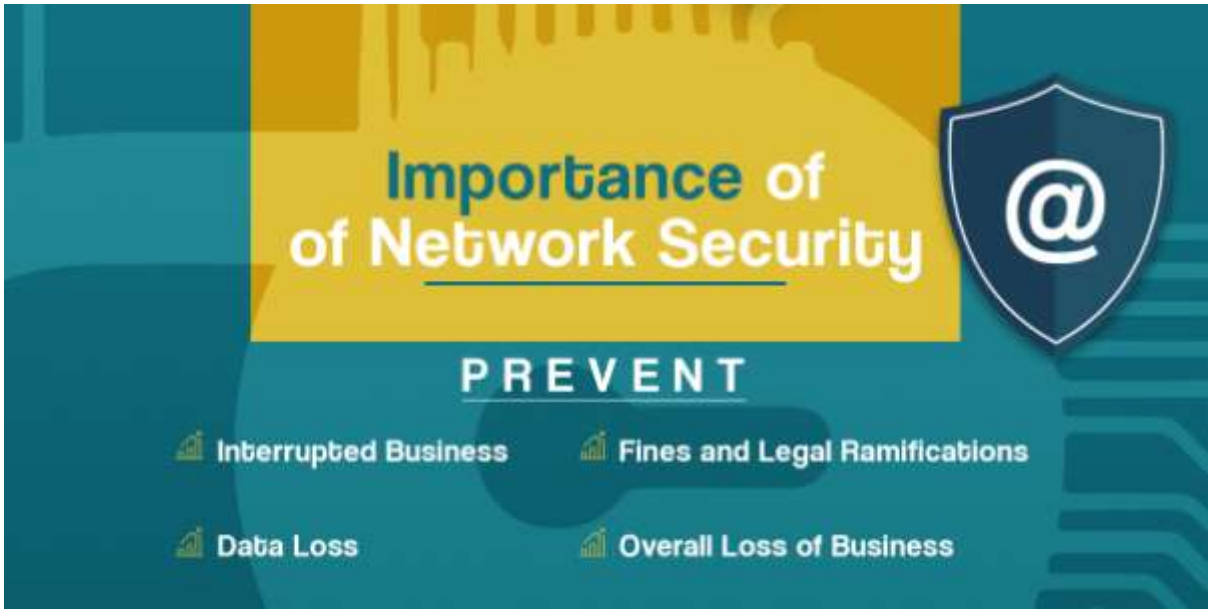
1.5.6: Software defined security-It is a type of security model where the information security that exists in a computing environment is implemented, controlled and regulated by pre installed security software.

1.5.7: VPN Security- Encrypted data is transmitted through VPN tunnel and on reaching the destination node, decrypted data is presented to the end user.A remote access server on the provider's side connects to VPN and the client software connects on the client side. This maintains a secured pathway for data motion.

1.5.8: Secure Remote Access- Mostly pertaining to the corporate sector, secure remote access refers to safeguarding harm prone data when an alien operator to the network tries gaining access to it. It normally utilises SSL VPN to authenticate users and encrypt data, though end point security might still be a requirement.

International Journal of Management, IT & Engineering
Vol. 7 Issue 8, August 2017,
ISSN: 2249-0558
Impact Factor: 7.119Journal Homepage: http://www.ijmra.us, Email: editorijmie@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gate as well as in Cabell's Directories of Publishing Opportunities, U.S.A

1.6Why the need for Network Security???



The definite need for network security cannot be denied. Considering the amount of data flowing through banking systems, there is a potential threat to billions and trillions of dollars. Considering the advent of cyber warfare, militarists have outlined the need for secure connectivity to state owned systems and also the need to prevent them from falling into militant hands. Large scale organizations and even Universities often have found it necessary to secure details that could be misused if they fall into wrongs hands.

- It minimizes the risk that is often related to transfer of information over networks across the globe.
- Recovery from a disaster can be possible through its implementation.
- It works continuously and is not prone to human like need of resting to regain energy.
- It demarcates the line beyond which the system does not remain vulnerable to other entities.
- Private networks can be provided protection from external attacks by closing them off from the internet.

- Reduced stress on the part of humans considering there are active organs on the network always standing up against intrusion.

1.6.1: Is it enough??

For all the protection that the regularly evolving forms of security tend to offer. They are never complete in the true sense. And the rate at which protective measures are evolving is the very rate at which trespassers are bulking up their abilities. It may not be wrong to mention that security measures are often steps aimed at countering the existing form of threats. And to this effect, they would always lag a step behind the rapidly changing forms of attacks.

Crime, terrorism, leakage of personal information, bank heists and malware attacks are even to this day commonly carried out through internet services. The existence of dark web and its potential threat to the well being of society and to the security of numerous fields spread across internet have found no permanent solution.

The involvement of Cambridge Analytica in US Presidential election and the possible leaking of data on the part of Facebook to that organization raise the question that how much of our data available on the internet can be protected and how much prevention is within our reach.

Use of high end security can often pose problems to non-technical users who are not exposed to accessing methods. While definitely maintaining security standards is a necessity, it starts biting back when the used procedures pose hindrance to utilization. And considering that invent of technology is often for ease of work, the usefulness of protective measures stand tested when seen through layman's eyes. And there stands the very important question.

Is network security a boon or a necessary evil?

References:

1) Forms of Security Required-
https://searchsecurity.techtarget.com/resources

2) Denial of Service Attack-
https://www.esecurityplanet.com/network-security/5-tips-for-fighting-ddos-attacks.html

3) Software Defined Security-
https://www.techopedia.com/definition/29942/software-defined-security-sds

4) Is it enough-
Possible disadvantages of network security
https://turbofuture.com/misc/Disadvantages-of-Digital-Technology

5) Network of Security Key-
https://lazyadmin.nl/home-network/network-security-key/

6) VPN Security-
https://www.expressvpn.com/internet-privacy/guides/vpn-security-work/