Network Security Threats

[1]Divya,[2] Devika Krishna,[3] Sahridaya

1Assistant Professor, Department of CSE, BGSIT, BG Nagar

2 Dept. of CSE, BGS Institute of Technology, BG Nagar, Karnataka, India

3Dept. of CSE, BGS Institute of Technology, BG Nagar, Karnataka, India

ABSTRACT-As attacks have become more skeptical and continue to evolve, static technologies cannot sustain. Soloed solutions crumble your defences. Intelligence and meticulousness is required to stop cyber-attacks and unknown menace. The traditional approach to data and network security is hurriedly becoming accosted. Implementing security on individual applications, servers and networks to meet immediate security or compliance needs hinders companies in an economy where customers, suppliers or business partners may need secure access to the corporate network anywhere, any time and by using any type of device. Organisations can overcome this challenge and achieve their global business goals by incorporating a reliable approach to security and access control which is included by awareness of user identities and their roles.

There are two reasons for why organizations are rethinking about their security and compliance approaches.

First reason is the globalization and internationalization of everything a company does. Various geographies or jurisdictions have different regulations governing over the financial or customer data, for example, an organization's access-control policies must abide by those regulations.

Second reason is that real-time interaction is needed between the applications used by our employees and the supply chains we form with our partners. Lastly, the number of access devices exploding, the number of users exploding are the different methods they use to access network. A network administrator can't control, or may not even know, where his users are, what devices are used by them, or how they are accessing the network. But he or she has to assure them appropriate access to business information whenever and wherever they need it.

KEYWORDS: Denial of service attacks, phishing, malware, botnet, application of vulnerabilities, BYOD.

I. INTRODUCTION

Network security includes the policies and practices adopted in order to prevent and monitor unauthorized access, misuse, modification or denial of a computer network and network-accessible resources. A threat, in the framework of computer security, refers to anything that has the potential to cause serious damage to a computer system. And it is something that may or may not happen, but has the ability to cause serious harm. Attacks on computer systems, networks are led by these threats. Network administrator controls the network security which involves the authorization of access to data in a network. Users choose or are assigned with an ID and PASSWORD or other authenticating information that allows them to access information and programs within their authority. Network security incudes a variety of computer networks, both public and private that are used in everyday jobs, conducting transactions and communications among businesses, government agencies and individuals.

Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises and other type of institutions. It does as its title explains: securing the network, as well as protecting and overseeing operations being done.

The most common and simple way of protecting a network resource is by assigning it with a unique name and a corresponding password.

SECURITY MANAGEMNTS:

Security managements for networks is different for all kinds of situations. A home or a small office may only require basic security while large businesses may require high-maintenance and advance software and hardware to prevent beastly attacks from hacking and spamming.

Networks are subject to attacks from malicious sources. Attacks can be of two categories.

1.''Passive'', when a network intruder interrupts data travelling through the network.

2. "Active" in which an intruder initiates commands to disrupt the network's normal operation or scrutinize and lateral movement to find and gain access to assets available via network.

1. PASSIVE

Network

- Wiretapping

- Port scanner
- Idle scan
- Encryption
- Traffic analysis

2. ACTIVE
3. VIRUS
4. EAVESDROPPING
5. DATA MODIFICATION

- Denial-of-service attack
- DNS spoofing
- Man in the middle
- ARP poisoning
- VLAN hopping
- Smurf attack
- Buffer overflow
- Heap overflow
- Format string attack
- SQL injection
- Phishing
- Cross-site scripting
- CSRF
- Cyber

INTERNET SECURITY:

Internet security is a branch of computer security specifically related to the internet, often involves browser security but also network security on a more general level as it applies to other applications or operating systems on a whole. Its objective is to establish rules and measures to use against attacks over the internet. The internet represents an insecure channel for exchanging information leading to a high risk of intrusion or fraud, such as phishing. Different methods have been used to protect the transfer of data, including encryption and from the ground up engineering.

THREATS:

MALICIOUS SOFTWARE:

A computer user can be tricked or forced to download a software onto a computer that is of malicious intent. Such a software comes in many forms, such as viruses, Trojan horses, spyware, and worms.

- Malware, short for malicious, is any software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. Malware is defined by its malicious intent, acting against the requirements of the computer user, and does not include software that causes unintentional harm due to some deficiency. The term bad ware is sometimes used, and applies to both true malware and unintentionally harmful software.
- A botnet is a network of zombie computers that have been taken over by a robot or bot that performs large-scale malicious acts for the creator of the botnet.
- Computer viruses are programs that can replicate their structures or effects by infecting other files or structures in a computer. The common use of a virus is to take over a computer to steal data.
- Computer worms are programs that can replicate themselves throughout a computer network, performing malicious tasks.
- Ransom ware is a type of malware which restricts access to the computer system that it infects and demands a ransom paid to the creator of the malware in order to the restriction to be removed.
- Scare ware is a scam software with malicious payloads, usually limited or no benefit, which are sold to consumers via certain unethical marketing practices. The selling approach uses social engineering to cause shock anxiety, or the perception of a threat, generally directed at an unsuspecting user.
- Spyware refers to programs that confidentially monitor activity on a computer system and report that information to others without the user’s consent.
- Trojan horse, commonly known as a Trojan, is a general term for malicious software that pretends to be harmless, so that a user willingly allows it to be downloaded into the computer.

DENIAL-OF-SERVICE ATTACKS:

A denial-of-service attack (dos attack) or distributed denial-of-service attack is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out motivates and targets of Dos attack may vary, it generally consists of the concerted efforts to prevent an internet site or service from functioning efficiently, temporarily or indefinitely. According to businesses participated in an international business security survey, 25% of respondents experienced a Dos attack in 2007 and 16.8% experienced one in 2010

PHISHING

Phishing occurs when the attacker pretends to be a trustworthy entity, either via email or webpage. Victims are directed to fake web pages, which are dressed to look legitimate, via spoof emails, instant messenger/social media or other avenues. Often tactics such as email spoofing are

“NETWORK SECURITY” refers to any activity designed to protect the usability and integrity of your network and data. It includes both hardware and software technologies. Effective network security manages access to the network. It targets a variety of threats and stops them from entering or spreading onto your network.

HOW DOES NETWORK SECURITY WORK?

Network security combines multiple layers of defences at the edge and in the network. Each network security layer implements policies and controls. Authorized users gain access to network resources, but malicious actors are blocked from carrying out exploits and threats.

HOW DO WE BENEFIT FROM NETWORK SECURITY?

Digitization has transformed our world. How we live, work, play, and learn have all changed. Every organization that wants to deliver the services that customers and employees demand must protect its network. Network security also helps you protect proprietary information from attack. Ultimately it protects your reputation.

SECURITY POLICIES:

“A security policy is a formal statement of the rules by which people who are given access to an organization’s technology and information assets must abide.” The specifics of a security policy will naturally vary depending on the nature of the organization that is implementing it; however, any used to make emails appear to be form legitimate senders, or long complex subdomains hide the real website host.

Insurance group RSA said that phishing accounted for worldwide losses of $1.5 billion in 2012.

II. APPLICATION VULNERABILITIES

Applications used to access internet resources may contain security vulnerabilities such as memory safety bugs or flawed authentication checks. The most severe of these bugs can give network attackers a complete control over the computer. Most security applications and suits are incapable of adequate defence against these kind of attacks. Security policy should at least incorporate the following:

1 A policy should be in place that identifies the security-focused objectives and requirements of the network.

2 Access control rules should be in a place to determine whether a user is permitted to access certain objects.

3 All users should be briefed and trained on security principles on an on-going basis. A security policy should evolve over time to consider, for example, new developments in security threats to a network, and it is therefore important that users are familiar with any updates to the policy. Therefore, security training should happen regularly and not be one- time affair. It is thought, this point is the most critical, since a security policy is near useless if those it applies to do, but do not know how to follow it.Along with this a fresh perspective on internet security [1]:People don’t do enough task to protect

themselves on the internet. They don’t use good passwords. They are poor at recognising the URL of “Phishing” sites. They ignore certificate errors.It’s a rational behaviour, because people sense that all the headaches of keeping up to date on security probably aren’t worth the trouble. Time spent constantly changing passwords or taking other security steps is valuable time lost. By comparison, the reduction of risk of having an account hacked or another security problem is relatively minor.

MIS SECURITY INFOGRAPHIC:

As businesses large and small become more dependent on electronic data, a major focus has shifted towards information security. Businesses are investing more than ever to protect themselves from dozens of security threats, from malware infections to financial fraud.

In a survey of businesses worldwide, almost every industry surveyed has experienced an information security-based incident at some point in time.

As information security becomes more of a priority in the future, here are a few things organization can start doing now to protect itself:

- Implement a privacy and data security plan
- Conduct an inventory of potential data targets
- Develop a privacy policy
- Protect data collected online
- Create levels of security
- Plan ahead for data loss

A network security plan is also needed, and of course the ability to create strong passwords is a must to better handle security issues.

III. PREVIOUS WORK

Despite best efforts, attackers often know more about the networks they attack than the network owners and they are using that to their advantage. Modern networks are increasingly complex. Their components constantly evolve and spawn new attack vectors including mobile devices, wed-enables and mobile applications, hypervisors, social media, web browsers, home computers and even vehicles. To truly protect these extended networks, we have to accept the nature of modern networked environments and devices and start defending them by thinking like an attacker.

Few organizations think like this, and fewer still have shifted their security postures and approaches to reflect this reality. They secure extended networks that also include end points, mobile devices, virtual assets and data centres using desperate technologies that don’t – and can’t work together. Attackers fundamentally

understand the nature of the classic security technologies and their applications and exploit the gaps between them. They employ a methodical approach to remain undetected and accomplish their mission, using technologies and methods that result in nearly imperceptible indicators of compromise. A quick look at the “attack chain”- the chain of events that leads up to and through the phases of an attack-
Shows how:
Survey: Attackers start with surveillance malware to get a full picture of your environment including all elements across your extended network. To understand what attack vectors are available, the security technologies deployed and what accounts they can capture and use for elevated permissions. Continuation [2]

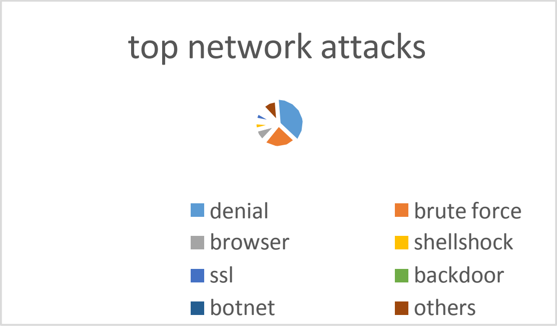
IV. PROPOSED METHODOLOGY

It is a well-established fact that 70%+ of threats to an organization’s network and network-based infrastructure originate from inside. US CERT in their recent study has predicted that malicious internal users deploy root kits, carry out identity thefts, use spyware and gain unauthorized access. Cyber-attacks with financial motives are based on a mix of strategies and mechanisms ranging from social engineering to viruses and the viruses have increased dramatically in the recent past. Till date, to a very large extent, the organizational security focus has generally been on protection of the perimeter and the end points. The LAN itself has lacked sufficient security provisions. With an increasing laptop population, organization-wide wireless connectivity and increasing number of remote sites to the organizational network, the traditional approach of fortifying the perimeter has diminished in providing adequate security. Now, there is a need to protect each and every network object rather than just perimeter or PCs. Newer technologies like Network Access Control (NAC), Data leakage prevention (DLP) and organization wide threat monitoring and alerting system along with policy enforcement are required to mitigate any threat or block any suspicious activity within the organization. The insider threat mitigation solutions are required for the following business challenges:
1. Preventing unauthorized system access to critical IT resources

2. Preventing data breaches
3. Preventing sabotage (internal)
4. Preventing theft of intellectual property
5. Reduction of administration cost related to security

6. Better audit ability to address compliance requirement.
Devices like iPads and Smart phones with 3G capabilities are becoming an accepted part of corporate IT infrastructure as converged IT devices for both voice and data traffic. These are likely to connect to corporate network and servers from public networks like Internet using VPN. The Corporate Information Security group will have the responsibility of protecting these mobile users as well as corresponding corporate information. Being on the public network, these users and devices will need protection from increasingly potent malware and hackers.
Higher speeds on wired or wireless network with higher speed processors will result in richer applications. These new applications will pose newer classes of security risks.
Running these rich applications on high speed network will require security devices that have higher performance along with deep packet inspection capabilities.

V. SIMULATION



Denial-of-service	37%
brute force	25%
browser	9%
shellshock	7%
SSL	6%
Backdoor	2%
botnet	2%
Others	12%

Criminals can pick from a long list of various network attack methods to employ against a small business. Some types are more common, and knowing them can make it easier to prioritize network attacks.
The list above is based on a chart from 2016 McAfree Labs Threat Report. It highlights the network attack types in Q4 2015, based on data from millions of sensors across file, web, message and network vectors.
The following flow chart is about

BYOD SECURITY RECOMMENDATION [3] fig.1

BYOD- BRING YOUR OWN DEVICE.
Based on the security issues identified in the previous

two chapters, the following recommendations are put forward to develop an effective BYOD security policy. Whilst the focus is on BYOD, certain points are also relevant to the development of security policies in general.

Regardless of who owns the device being used to access corporate data, the data is owned by the organization they therefore need to have the right to access it. It is essential that these points are made clear to employees, since if corporate data is being stored locally, this will mean that the organization will require a certain level of access to the employee's

personally owned device. Depending on the tasks the device is being used for, the organization may require the ability to
remote-wipe the device. In many cases this could cause concerns of a privacy related nature to arise for employees, hence the next point made that BYOD should not be compulsory.

Also of concern is data protection. With reference to the previous point made about lost/stolen devices, if an employee-owned device is lost or stolen, and the device contains customer data which is subsequently compromised, this could result in legal implications for the organization in relation to the Data Protection Act.

BYOD Security Recommendations

Based on the security issues identified in the previous two chapters, the following recommendations are put forward to develop an effective BYOD security policy. Whilst the focus is on BYOD, certain points are also relevant to the development of security policies in general.

Regardless of who owns the device being used to access corporate data, the data is owned by the organization they therefore need to have the right to access it. It is essential that these points are made clear to employees, since if corporate data is being stored locally, this will mean that the organization will require a certain level of access to the employee's personally owned device. Depending on the tasks the device is being used for, the organization may require the ability to remote-wipe the device. In many cases this could cause concerns of a privacy related nature to arise for employees, hence the next point made that BYOD should not be compulsory.

As mentioned, Gartner has predicted that many employers will make BYOD compulsory by 2017.

Despite the benefits BYOD can bring, it is thought that

an 'all or nothing' approach is the wrong one, since it would have unfair impact on employees unwilling to share their devices with their employer. In addition, since the employer would require a certain level of access to the device (see previous point), there could also be legal implications from a privacy perspective. It is therefore suggested that employees are given the option to opt-out of a BYOD programme and use company owned equipment should they wish to.

Mobile Device Management (MDM) enables personal employee devices to be identifiable to the organization's network administrators. An MDM client should always be used by staff to access the corporate infrastructure using their personal devices. The device should be registered with the MDM, which would involve authentication, ensuring that the device meets the security requirements of the organization before network access is granted.

The process of registration with the MDM should at minimum involve the following:

- User authentication.
- Agreement to comply with BYOD policy and any other applicable policies.
- Ensure that the device is running up to date antivirus software approved by the organization.
- Run a security scan to ensure that the device is free of malicious software.
- The device should be scanned on a regular basis, at minimum once a week. Ideally, the antivirus software should work in collaboration with the MDM, thus if malicious software was detected by the antivirus software, the MDM could immediately disconnect the device from the network, reducing or even eliminating the risk of damage to other devices on the network.

- Security training for staff is the most important aspect of ensuring the success of a network security policy;
- There is an apparent general lack of security training given to employees by their employer;
- Security policies are generally poorly enforced, evidenced by the high percentage of employees who had knowingly violated them. This indicates that better enforcement and disciplinary procedures are required;
- Many employees violate security policies because they need to do so in order to complete tasks. This indicates the need for security policies to be developed in collaboration with staff, in order to take into account the type of work the employees will be doing when developing the policy;

A systematic research of internet security: security policies and BYOD.

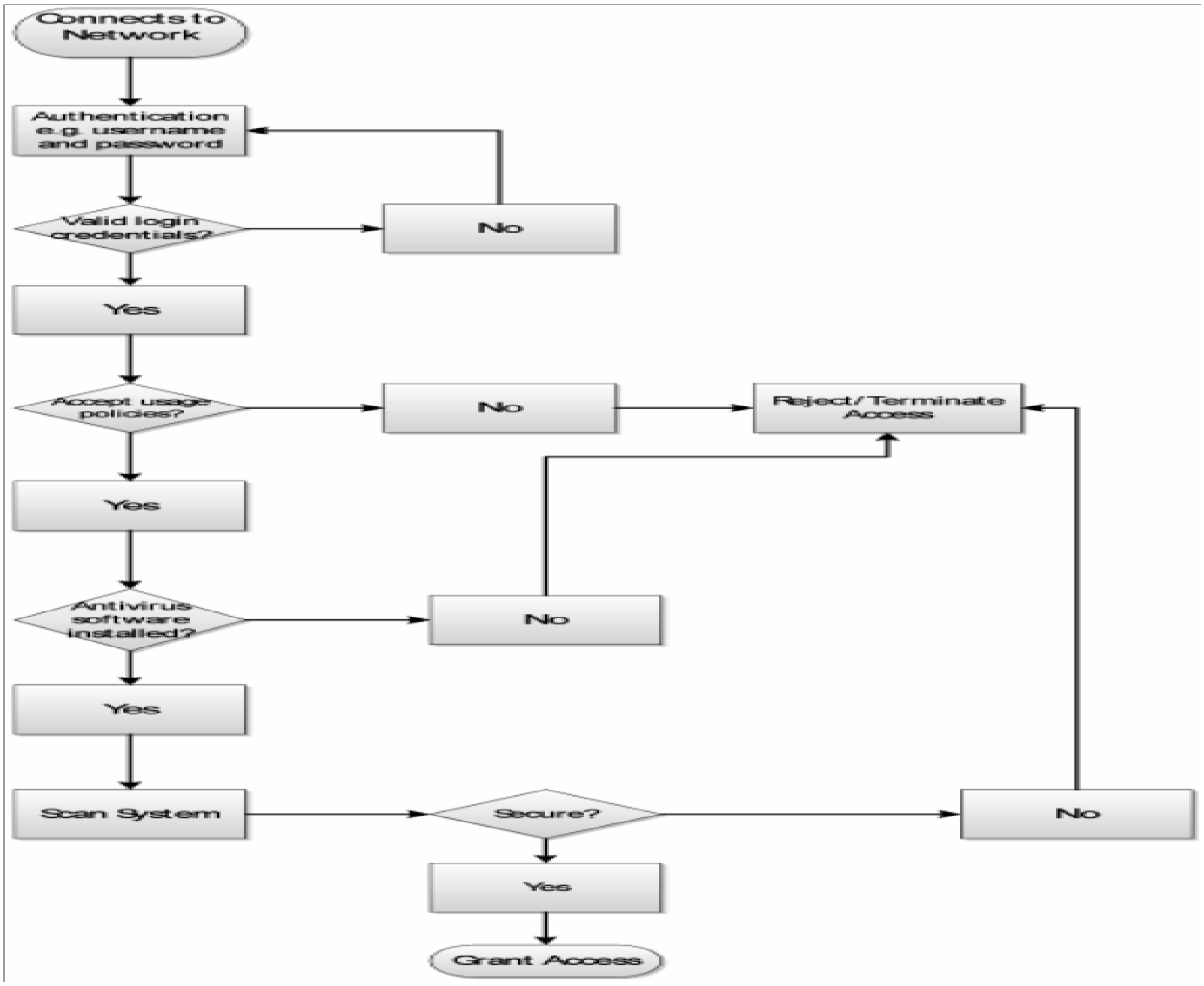


Figure 1: DEVICE REGISTRATION PROCESS

VI. CONCLUSIONS

The research work has examined about the network security, network threats, different types of attacks and causes for that. And research work also evaluated about security policies with an emphasis on BYOD. Based on the research carried out, the following conclusions have been drawn:

ACKNOWLEDGEMENT:
I would like to thank Professor Divya mam, for her encouragement and support, and for nominating my work to be published. I would also like to thank my co-author for co-ordinating with me.