Network security in multiple threats: A critical study

Kapil Joshi[1], Rajesh Kumar[2], Harishchander Anandaram[3], Manoj Diwakar[4], Prabhishek Singh[5], Achyut Shankar[6], Sathishkumar V E[7,8]

[1]Department of CSE, Uttaranchal Institute of Technology, Uttaranchal University, Dehradun, India
[2]Department of CSE, Meerut Institute of Technology, Meerut, India
[3]Centre for Computational Engineering and Networking, Amrita School of Engineering, Coimbatore, India
[4]CSE Dept., Graphic Era Deemed to be University, Dehradun, India
[5]School of Computer Science Engineering and Technology, Bennett University, Greater Noida, India
[6]University of Warwick, UK
[7]Department of Software Engineering, Jeonbuk National University, Jeonju-si, Jeollabuk-do, Republic of Korea

[8]sathish@jbnu.ac.kr

Abstract. Any organization nowadays needs a secure network. High-speed wireless networks and internet services are becoming increasingly unsafe as a result of the daily rise in security threats. Threats to information security come from within the company, in close to 80% of cases. With the latest trend of mobility (portable devices such as laptops and smartphones etc.), ubiquitous 3G connectivity and this trend increases but as more web-based applications are manufactured and available over the Internet, the instances of insider threats have been rising at an alarming rate. Current or former workers, contractors, or business partners who have permission to access the organization's network and servers are typically the source of insider threats. Confidential information is frequently stolen for monetary gain or wellful harm. Access to hacking tools via the Internet, USB drives, and wireless connectivity make break-ins simple. Here, Millions of dollars in losses in the event of IP theft, and customer / individual information theft are yet too considered. This article provides insight into Insider dangers, attackers, and their rationales and recommendations for organizational-level mitigation methods.

Keywords: threats, network access control (NAC), network security, policy enforcement.

1. Introduction

Protection of networks and their services against unauthorized manipulation, destruction, or disclosure and assurance that the network [1] functions under urgent situations without harming either users or employees are some of the definitions of network security. It is a well-known statistic that at least 80% of internal threats to a company's network or network-based infrastructure come from within. In recent research, US-CERT anticipated that malevolent internal users will employ spyware, install rootkits and steal identities. Cyber-attacks for financial motivations involve a variety of mechanisms and strategies, from social engineering to various viruses. The LAN itself lacked adequate security measures. The conventional method of fortifying that perimeter has lost its effectiveness in providing adequate protection as a result of an increase in the number of laptop users, enterprise-wide wireless access, and an increased number of remote locations connected to the organizational network. Instead of only protecting the perimeter or PCs, it is now necessary to defend every single network object. To mitigate threats or stop suspicious activity within the business, newer technologies like Network Access Control (NAC) and Data Leakage Prevention (DLP) [2]. For the prevention of insider threats, it is necessary to implement the subsequent business challenges:

1. Prevent unwanted access to IT resources through systems.
2. Keeping data breaches sabotage and avoiding intellectual property theft.
3. Reduction of security-related administrative costs and increased audit ability to meet compliance obligations.

Security attacks can be classified under the following categories: Active attacks and passive attacks but the major classification of cyber security is illustrated below in Figure 1.

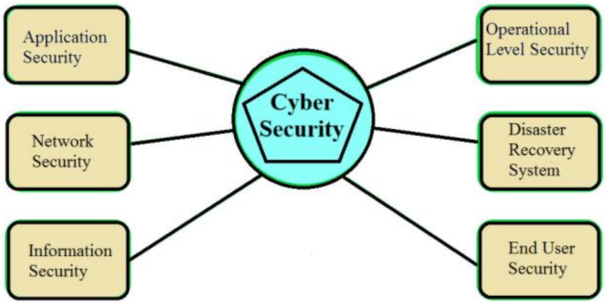

Figure 1. Classification of cyber security.

2. Evaluation of network security

There have been various patterns that are easily discernible in recent years. Due to their cheaper costs, superior form factors, and simplicity of use, among other factors, portable gadgets like laptops, notebooks, and smartphones have gained popularity. Additionally, they provide the benefit of mobility through "anytime, anyplace computing." These types of equipment are required for a specific class of employees to carry out efficiently and effectively carry out their work. By linking, sales or technical support staff can work remotely the connectivity to the Internet, generally utilizing VPNs business networks. The fact that these mobile devices may easily access corporate networks and retain sensitive organizational data makes them a potential [3] cause of data loss, whether done so on purpose or not.

Similarly, to this, employees who are inside a company and connect to the company's network can use the company's Internet facility to convey important and private information. Peer-to-peer apps of various kinds can be used for this. Due to their capacity to run within the network undetectably, a few of these applications may pose very significant security risks. Huge amounts of information (such as movies and music) are frequently downloaded using programs or services like BitTorrent. Such high data transfer rates over a LAN can strain its infrastructure. These apps employ a variety of tactics to avoid detection, including the use of dynamically provided ports and well-known/popular TCP ports (such as SMTP, FTP, etc.), which are typically not prohibited by an enterprise. Common firewalls and security tools are unable to recognize these applications. Applications of this kind will continue to increase. By 2014, Cisco has already forecasted that video would contribute to 91 percent of all Internet data volumes. Large storage capacity is currently offered by many USB-based removable storage devices kinds. The private information of the business can be discretely removed from a single disc due to its tiny size.

Access to loads of free or inexpensive hacking tools is available online. Anyone without much programming experience or computer understanding can readily download and try these tools. These instruments can assist with the remote deployment [4] of key loggers or the frequent collection of screenshots from the desktop. Due to the prevalence of social media sites, employees are spending countless hours on websites like Facebook and utilizing their Internet connections for activities other than what is necessary for their jobs, such as playing games, trading stocks, and downloading content. Due to the resources and lost revenue, these costs businesses millions of dollars. Although wireless access is more convenient and less expensive, it is less secure than wired networks. Wireless communication is booming because of its benefits. Corporate wireless networks are also exposed as a result. For instance, the Black Hat conference recently showed methods for compromising wireless WPA-II security.

3. Motivation and background for internal threats

Insider Threat is the use of permitted or illegal access to compromise the confidentiality of organizational information systems. Attackers may be current or former employees, partners in business, or independent contractors. Insider attacks ultimately cause losses for the organization. Insiders have access to and knowledge of internal data. The majority of organizational intellectual property (IP) is now held across multiple servers in digital form, making it simple for employees [5] to access and potentially leak to rival businesses, among other things. As an illustration, Gary Min was jailed in 2007 after stealing from his company, DuPont, about 16,000 papers and 22,000 scientific abstracts. Using both his permitted access and methods to acquire unauthorized access, Gary had gathered these documents from multiple servers. Financial gain continues to become one of the very prevalent reasons for insider attacks. Disgruntled workers inflicting harm or damage are occasionally cited as a factor. Terry Childs was given a 4-year prison term on August 9, 2010. Childs, gave himself and have to the administrator passwords, when asked by his supervisor to turn over the passwords, he refused, resulting in a 12-day standoff that cost the city 900,000 US dollars in losses. Nations are using a lot of resources to enter enemy networks and infrastructure also with the sole purpose of either stealing important information or taking the enemy's infrastructure hostage as cyber warfare becomes an essential component of military strategy around the globe. Custom spyware (sometimes known as bots) is frequently used to infect a machine, which then spreads to the whole network. Additionally, these bots can continue communicating vital internal data [6] to an external command centre, impair or block the functioning of the infiltrated network, or all three.

4. Various methods used for internal attackers

A variety of the following methods can be employed by an insider with harmful intentions.

- Social engineering when a coworker leaves their computer unattended, it is possible to discover their password by peering over their shoulders or by allowing remote management to access the system. Malicious software can also be inserted by the attacker to retrieve passwords, etc. Later.
- Use of Tools: A wide range of hacking tools, including rootkits, password crackers, sniffers, and installers for remote key loggers, are available.
- Misuse of Privilege: An administrator may purposefully provide privileged access on a newly installed machine so that he or she can utilize it later. Backdoor accounts could also be made as an alternative.
- Installing a modem enables Internet connectivity, which enables transferring information outside the company. Data cards may be installed into a system to offer this access. Other commonly used methods are sending confidential correspondence or communicating with the outside world using encryption.
- Authorized users who delete or modify databases with the intent to later conduct fraud are known as "willful data deletion."
- Installing rouge; devices such as placing a malicious wireless access point on the network to allow unauthorized connections or putting a malicious laptop on the network to monitor network activities in preparation for future intrusions.
- Internal resources might be overloaded with unwanted traffic using Denial - Of - service to shut down the services. Most worms and viruses can generate a lot of network traffic.
- Gaining permitted access by breaking into wireless networks, using man-in-the-middle attacks, or using complex assaults that use impersonation, such as User/System/Switch/VLAN.

Internal web servers frequently host vital information, and all these servers are breached by several internal attacks. The aforementioned attacks can be easily executed with readily [7] available tools and only require a rudimentary computer and network understanding.

5. Better solution for mitigation of attacks

The majority of attack tools and malware take advantage of flaws in operating systems, software, and network infrastructure. Other assaults take advantage of lax security procedures within an organization. Insider attacks can also result from having solid security policies but bad implementation. Due to the lack of proper security evaluations, monitoring, and the lack of an internal alerting mechanism, organizations are exposed to these vulnerabilities. Various compliance requirements include the following: Business compliance regulations such as Surbanes-Oxley (SOX), HIPAA for medical records and data, PCI for credit cards, and ISO27000 for corporate security requirements are all covered by these regulations. The majority of governments are taking action to make sure all information security requirements are upheld and are binding on enterprises. Additionally, growing in popularity is information security system certification, whereby companies can vouch for the effectiveness of their information security measures to their business partners [8]. The first step toward security is having an information security policy that is widely recognized throughout the whole organization. The next crucial step is to effectively implement this strategy, together with routine monitoring and alerting systems. Since there is no magic bullet with information security, businesses must rely on multi-layered security solutions from a variety of providers without overcomplicating the solution. These solutions should properly fulfil the security requirements of the enterprise while addressing security throughout. Planning for security is frequently neglected since it is thought that security does not provide a good return on investment. But that opinion is quickly shifting. With increased organizational security, businesses have witnessed improvements in their procurement costs and greater sales results. In addition to penalties, a security problem can harm a company's reputation in the marketplace. Both preventive and reactive security procedures are needed to protect corporate information assets from insider threats. Before allowing an endpoint or user to access the network, proactive measures are implemented once the endpoint or user has undergone the necessary authentication and had its security posture evaluated. Through these checks, it is made damn sure also that the user system is just a corporate resource and is not attempting to join the corporate network on its own. Dual-factor authentication is one method used to solve the password issue. Dynamic passwords are used for two-factor authentication, and they change over time. A lot of places utilize biometric authentication to prevent password misuse and to make sure that someone can be held accountable. Single sign-on solutions make the user receives access under the policy and by his or her position [9] while the password policy is in place. Usage records and notifications for any unusual behaviour are provided by the log management.

6. Futuristic approach to security

Coverage of gadgets like iPads, as well as Smartphones having 3G capabilities, are increasingly being regarded as a standard component of corporate IT infrastructure applications [10]. These are probably going to link to the servers and corporate network by Using a VPN, or public networks like the Internet. The task of safeguarding these mobile users and associated company data would fall under the purview of the Corporate Information Security group. These people and gadgets must be protected from hackers and more powerful viruses because they are using a public network. Richer apps will be produced as a result of faster CPUs and wired or wireless networks. Additional classes of security vulnerabilities will be posed by these emerging applications. These sophisticated apps need high-performance security devices featuring deep packet inspection capability to run on high-speed networks. Between maximum information with vulnerabilities for ordinary networks is described in Table 1.

Table 1. Vulnerabilities data for sample network.

Host	Vulnerabilities	CVE#	Probability	Cost	Profit	Damage Impact
Gateway Server	Improper cookie handler in open-SSH	CVE2007-4752	0.51	0.162	0.35	0.50
Web Server	IIS Vulnerabilities in web-Dev sciences	CVE2009-1536	0.62	2.70	-1.89	1
SQL Server	SQL Injection	CVE2008-5416	0.78	1.70	0.75	1
Local Server	Buffer Overflow in Video	CVE2008-0015	0.59	0.38	0.90	0.47

7. Conclusion

Insider dangers are growing alarmingly as the technological landscape changes. The majority of security breaches are much more advanced and challenging to stop. Through this study, we also consider the maximum parameters of network security which is better for any IT organization. Since these attacks are carried out using inside information, it is typically exceedingly expensive for the business to prevent them. Insider attacks frequently go undetected because the perpetrator leaves no evidence. Both a proactive and a reactive approach are needed to stop these attacks. The proactive strategy implies that security policies will be automatically enforced throughout the firm, along with a strong monitoring, forensic, and logging framework. Instead of the conventional strategy of focusing on perimeter security, each component of the network must be safeguarded. To prevent any assault on the resources, it is advised to use event correlation and multi-layered security. A reactive strategy includes real-time monitoring & alerting in the event of any dangerous action. The overall study is useful for better establishment of network security against unauthorized access in the future term.

References

[1] Cai, T., Wu, Y., Lin, H., & Cai, Y. (2023). Blockchain-empowered big data sharing for internet of things. In Research Anthology on Convergence of Blockchain, Internet of Things, and Security (pp. 278-290). IGI Global.

[2] Yazdinejad, A., Dehghantanha, A., Parizi, R. M., Srivastava, G., &Karimipour, H. (2023). Secure intelligent fuzzy blockchain framework: Effective threat detection in IoT networks. Computers in Industry, 144, 103801.

[3] Peltier, T. R. (2005). Information security risk analysis. CRC press.

[4] Li, Y., & Liu, Q. (2021). A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, 7, 8176-8186.

[5] Liu, Z., & Wang, C. (2019). Design of traffic emergency response system based on internet of things and data mining in emergencies. IEEE Access, 7, 113950-113962.

[6] Cui, J., Liew, L. S., Sabaliauskaite, G., & Zhou, F. (2019). A review on safety failures, security attacks, and available countermeasures for autonomous vehicles. Ad Hoc Networks, 90, 101823.

[7] Pięta, P., & Szmuc, T. (2021). Applications of rough sets in big data analysis: an overview. International Journal of Applied Mathematics and Computer Science, 31(4), 659-683.

[8] Easwaramoorthy, S., Thamburasa, S., Samy, G., Bhushan, S. B., & Aravind, K. (2016, April). Digital forensic evidence collection of cloud storage data for investigation. In 2016 International Conference on Recent Trends in Information Technology (ICRTIT) (pp. 1-6). IEEE.

[9] Easwarmoorthy, S., Sophia, F., & Karrothu, A. (2016, March). An efficient key management infrastructure for personal health records in cloud. In 2016 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET) (pp. 1651-1657). IEEE.

[10] Harris, J., Ives, B., & Junglas, I. (2012). IT consumerization: When gadgets turn into enterprise IT tools. MIS quarterly executive, 11(3).