International Journal of Advance Research in Science and Engineering
Volume No.06, Issue No. 12, December 2017
www.ijarse.com
IJARSE
ISSN: 2319-8354

NETWORK SECURITY

C.Sunitha[1], Lavanya.S[2], Subasri.K[3]

[1] HEAD OF THE DEPARTMENT

[2, 3] MSC SOFTWARE SYSTEM

DEPARTMENT OF BCA & MSC SS

SRI KRISHNA ARTS & SCIENCE COLLEGE

ABSTRACT

Endpoint security alludes to a strategy of ensuring the corporate system when gotten to by means of remote gadgets, for example, portable workstations or different remote and cell phones. Every gadget with a remote associating with the system makes a potential section point for security dangers. Endpoint security is intended to secure every endpoint on the system made by these gadgets.

Keywords: endpoint security,gadgets,security dangers.

I.INTRODUCTION

In the recent days we have been facing much more advanced security threat everywhere around the world. There have been many strategies that the companies follow for not being a victim of the security breach but still there has not been a complete success. Recent research states that 43% of the companies had a data breach last year, 2015.Even the top companiessuch as Apple,Walmart and shockingly JPMorgan Chase faced a security threat recently. To overcome all these kinds of security breach and threats there have been several models being developed to secure the data.

II.ENDPOINT SECURITY

Some of the popular endpoint security software productsare from Symantec and Sophos. Symantec Endpoint Protection uses Symantec's Insight platform to collect and collate data from over 200 million systems in 200-plus countries. It uses this data to identify and create a security rating for every file accessed through the Internet. As a result, it stops targeted attacks and advanced persistent threats with a degree of protection that far exceeds the capacities of traditional anti-virus. Sophos functions in a similar way such that it spots the malfunctioning connection and tries to overcome it.

As a whole the endpoint security software works in such a way that it checks each and every connection which tries to communicate with the server, detectsthe misbehaving connection by using its information senses preloaded and kills it such that it does not proceed further to attack the components of the server and function as a malware so that the data is protected completely.

III.PERIMETER SECURITY

There is a similar security model to the endpoint security which functions for the same purpose in a different way called **Perimeter Security**.In simple, perimeter security states that all the mission-critical and Tier-1 applications are maintained inside the secure network and the bad guys are outside the firewall.
Perimeter security consists of prevention control devices which perform the most essential functions like deter, detect, delay and deny. These starts from the basic password to complex firewall pattern analysis that are designed to sort the "good guys" from the "bad guys" in today's highly techno-savvy society and grant access to only those who are authorized to have it.

Initially, based on the risk assessment, system boundary is determined which explains what should be inside it, what should be outside it, to what degree the system must be protected from theft, confidentiality breach and corruption arising from unauthorized external access. One way of implementing the perimeter security is that strong passwords are set and firewalls are deployed between the PC/network and an unsafe network. Firewall rules range from very simple to extremely complex which should be carefully devised, formally approved and implemented under strong surveillance. This mechanism prevents any malicious data packets crossing the firewall. Once the prevention control mechanisms are implemented the network is subjected to penetration test (ethical hacking) by a trusted third-party in a view to prove whether the secured information in the organization's network can be view, stolen, deleted or corrupted.

Other way of implementing perimeter security is to deploy a proxy server between internal and external network resources. The external requestor connects to the proxy server requesting a service that is provided by the organization's network. Based on the predefined set of criteria, the proxy analyses the request and retrieves the necessary service from the organization's network only when the request is validated. In this case, at no point the external IP address that raised the request will be connected directly to the internal IP address of the resource server preserving the internal anonymity. Similar to firewall, Intrusion Detection System (IDS) and maintaining the log of perimeter activity works as a detection control mechanism in perimeter security.

The network which has perimeter security is still under threats. This is because the organization no longer has a clearly defined perimeter. Organizations are running applications in cloud taking the data outside the scope of security methods. Many breaches go undetected for months which extend the severity of damage. Also the bad guys are already inside because simple mistakes even create more security breaches than malicious attacks. The perimeter security does not give a clear structured representation to find a threat and does not give a successful result in securing the data completely. Recently this perimeter security has become fuzzy. There are chances that the perimeter network might get eroded. In such cases the issue becomes critical and definitely needs to be redefined since the protection is not guaranteed. Another issue is that applications presented by a Web program and keep running on nearby machines are hard to control with conventional system edge instruments. The frameworks don't need to move to present undesirable access on the framework itself.

IV.NETWORK VISIBILITY

The **Network visibility**is quite different from the other security models and functions in a different way. Network visibility is to have a consciousness of different applications and discussion navigating the system, be it LAN or WAN. To know is to have the capacity to control the system exercises. Network visibility helps in allocating ideal data transfer capacity to the business basic applications. In the late years the work of the system manager has gotten to be harder with the entire world going to the web. The video/sound spilling, internet shopping, and programming like Skype has made the observing of big business organizes hard.

This makes the process a bit simpler so that it allows faster troubleshooting and network monitoring, detection of unauthorized WAN traffic, capacity planning and network trends, application monitoring and profiling. This method is called as a security delivery platform which was introduced to address the problem which couldn't be solved by the perimeter security. Network visibility gives a broad visibility of the infrastructure and a way to control and command activity. This method is seen as highly developing structure since it gives us a visibility into theencrypted and plain text traffic data. To summarize the network visibility gives a clear view of what is just present as a structure for the data security.

V.CONCLUSION

When the network visibility is compared with the perimeter security I think the **Network visibility overcomes the limitations of the perimeter security.**The perimeter security states that the bad guys are outside the firewall which doesn't seem to be true as the existence of bad guys have still been observed. The network visibility, as the name suggests gives a clear visibility of the infrastructure and functions in such a way that the threat is cleared in a very efficient way.Unlike the perimeter security the network visibility has a well-defined structure. The perimeter security burdens the networking staff since the firewall setting and updating it frequently and stuff needs to be a repeated process and needs checking every time the setup runs which is overcome in the network visibility since the work load is very less. The network visibility allows virtualization and real time data sharing at a faster way. This is seen to be a highly developing method as it is gives a proactive monitoring process for ensuring high speed performance with reliability. In short, the network visibility says if a threat is seen it is seen just by the way it comes in, detected and removed at the start without affecting the data any further.

REFERENCES

[1.] http://www.webopedia.com/TERM/E/endpoint_security.html retrieved on 03/01/2016

[2.] http://fortune.com/2014/10/03/5-huge-cybersecurity-breaches-at-big-companies/ retrieved on 03/01/2016

[3.] http://www.redbooks.ibm.com/redpapers/pdfs/redp4397.pdf

[4.] http://policy.bcs.org/content/1-perimeter-security

[5.] https://www.gigamon.com/sites/default/files/resources/analyst-industry-resports/ar-network-visibility-monitoring-1015.pdf