A study of cyber security practices with respect to use of firewall and IDPS in educational institutions in Pune area

Mr. Rajesh Mohan More

more.rajeshmore@gmail.com

Abstract:

Security measures are of prime *importance to ensure safety and reliability in fact it has become of paramount importance for existential support. Hacking of data and information has become almost a routine and regular aspect in case of IT/ITES industries as well as educational institutions. Before we think to combat such a situation; to avoid both predictable and unpredictable loss, danger and risk associated, tangible and intangible factors, we have to strategize in keeping cool in the heat of battle and find out the causes attributing to the same; so proactive action be taken to exterminate the same. The researchers feel to encircle parameter to have an in-depth insight such as – integrity of network connections and components, telecommunication issues, firewall, filtering, intrusion detection and prevention system, and network maintenance. These are in fact intra and interrelated.*

Keywords: Cyber security policy, cyber infrastructure, firewall, intrusion, attack, web filter

I] Introduction

Policy defines the meaning of security which talks about steps to achieve goals. Mechanisms provide tools and procedures to ensure that steps are followed [1]. Organizations implement several countermeasures designed to detect threats or minimize damage due to attacks. These countermeasures include antivirus software, firewalls, intrusion detection or prevention, and encryption.

The findings in a report released last year by the Center for Strategic and International Studies (CSIS), "In the Crossfire: Critical Infrastructure in the Age of Cyber war". Based on a survey of 600 IT security managers from critical infrastructure organizations, the report found that 37% believed the vulnerability of the sector they worked increased over the year prior, and two-fifths expect a significant security incident in their sector in the next year. Only one-fifth of respondents to the survey believe their sector to be safe from serious cyber attack in the next five years [2]. Around 10% to 20% of the 100+ incidents recorded in BCIT's Industrial Security Incident

Database (ISID) to date have been targeted attacks. The knowledgeable insider is the biggest threat and played a part in a high profile case in Queensland, Australia, in February 2000. A disgruntled employee of a water-utility contractor gained remote access to the utility's control system and managed to release over one million liters of sewage into local waterways [3].

To protect private or credential information or data from outside world is necessity of every organization. While using network, to work efficiently and exchange information within or outside world, it is necessary to follow certain parameter or instruction. It is obligatory to give proper permissions to each of the employees or users of the network. In this study we have considered different factors which affect network security. Organization has to focus on these attributes to work their cyber infrastructure effectively and securely.

To improve cyber security infrastructure integrity of network component like router, switch, server, work station etc we need to have security standards. Network connections need to prevent from unauthorized access. Periodic checks of its firewalls should be done to verify that the rule sets are up to the required security level. Security logs for intrusion detection systems and intrusion prevention systems can be consistently reviewed and regulated for abnormal patterns of activity. Web filter is used to protect the information being transferred from within or out of the organization. Policies of security requirements should be defined for wireless or dial-up network.

Security requirements for portable devices like USB drives, portable hard disk, IPods, mobiles, digital cameras etc that could be connected to the network. To maintain network efficiently; documentation of topology diagrams of the organization network along with geographical map showing exact location of network cables should be administered so that all the connection routes can be traced.

II] Security Strategies

To protect private or credential information or data from outside world is necessity of every organization. Security measures include password protection, software updates, firewall, malware protections as well as authentication, authorization, auditing, reviewing, vulnerability assessment and storage encryption.

Firewall is the crucial part in network security. To protect network; organizations have to prepare list of the traffic destinations as well as a list of kinds of traffic which include inbound and outbound traffic that have to allow through its firewalls. The organization need to configure its firewalls to allow only approved lists. There should be proper procedure for approval of any changes in the stated rules for firewall traffic. It needs prepare security logs for firewall and review it periodically also to verify that these rule sets have been implemented accurately. Security logs for intrusion detection and intrusion prevention systems should be maintained in a way which prevents them from being modified or deleted.

III] Data Analysis and Interpretation

- Below mentioned table illustrates that how many educational institutes follow security measures for Firewalls and IDPS –

IV] Hypothesis Testing

60% of the educational institutions are not following cyber security measures (Proper use of Firewall and IDPS).

H0: $\mu \neq 0.60$, Ha: $\mu = 0.60$

Z = (Pobserved – P) / sqrt [(P * Q) / N]

Pobserved = X / N

Pobserved = 20.9 / 40 = 0.52

P = 0.6, Q = 0.4, N = 40

Z = (0.52 – 0.60) / sqrt [(0.60 * 0.40) / 40]

Z = -1.0329

Since, $-1.96 < Z < 1.96$

that means our null hypothesis is accepted.

Hence it is concluded 60% of the institutions are not following cyber security practices (Proper use of Firewall and IDPS).

V] Finding and Suggestions

To study existing cyber security infrastructure of educational institutions, a survey has been conducted on random sampling basis. However coverage of heterogeneous yet essential attributes is ensured to have right mix of all related parameters. An attempt is made to collect sufficient data and analyze.

From the response received from the respondents;

1.It is concluded; by and large a significant number of respondents feel that even though system is installed. Periodic checking regarding its authenticate working, use of standardized and reliable components ensuring functional applicability is not only necessary but indispensable as well.

2.Further the periodicity enforced is differing from organization to organization. This is to be harrowed from viewpoint of ensuring objective/aim compliance.

3.Majority of the respondents (80%) have answered affirmatively for-

i.Organization periodically reviewed the list of the traffic allowed through its firewall.

ii.Security logs for firewalls are regularly reviewed.

iii.Firewall and router rules prevent authorized outbound connections like web server.

4.There was a fencing sitting approach by the respondents in respect of-

i.Automatic checking of changes made in software components.

ii.Automatic start up of critical components when other application tries to connect repeatedly.

iii.Allowing only the lists of approved traffic through its firewall.

iv.Approval process for any changes in rule sets defining the traffic.

v.Maintaining of security log in such a way that prevent modification and deletion.

vi.Deployment of firewall to protect critical systems from unauthorized access.

vii.Maintaining of comprehensive lists for its router including internet protocol addresses and port numbers being utilized.

viii.Review of security logs of IDPS regularly for abnormal patterns of activity.

ix.Prevention of IDPS security log from being modified and deleted.

x.Use of web filters to restrict uploading of sensitive information to outside network.

xi.Filtering on unfriendly java scripts and applets.

xii.Content filtering on file attachment transmitted outside network via email or ftp.

xiii.Filtering of executable email attachments.

5.In a nutshell more concentrative and focused efforts are required for-

i.Regular monitoring of security alerts from IDPS.

ii.Regular updating of signature on IDPS.

iii.Periodic checking of firewall to verify the rule sets have been accurately implemented.

VI] Conclusion

Having followed the parameters indicated in the preceding paragraphs we will be in a position to streamline a safe, secure, healthy and all proof system. It is necessary to use security technologies such as firewall and IDPS properly so that organization can protect their cyber infrastructure.

VII] References

1. Matt Bishop, “What Is Computer Security?” IEEE Security & Privacy, January/February 2003.
2. George V. Hulme, “SCADA Insecurity-Stuxnet put the Spotlight on critical infrastructure protection but will efforts to improve it come too late?”, Information Security Magazine, Volume 13-No.1, 2-2011, 38-44.
3. Paul Marsh, “Controlling Threats”, IET Computing & Control Engineering, April/May 2006, 12-17.
4. Singh, Akhand Pratap. "Fortified Multimedia Application." *International Journal of Research* 1.5 (2014): 283-291.
5. http://www.cyberlawsindia.net
6. http://www.indiancyberlaw.com
7. http://www.mit.gov.in/content/role-government

8. http://www.cert-in.org.in
9. http://www.indiadefenceonline.com

VII] Appendix

Security Measures	**Y**	**N**
Lists of the traffic destinations and kinds of traffic	24	16
Allows only the traffic on its approved lists	24	16
Approval process for any changes in the rule sets defining the traffic to allow through its firewalls	24	16
Periodic review of lists of the traffic it allows through its firewalls	32	8
Periodic checks of its firewalls to verify that the rule sets have been accurately implemented with no ad hoc changes	8	32
Prevention of security logs of firewalls from being modified or deleted	24	16
Regular review of security logs of firewalls for unauthorized traffic	32	16
Deployment of firewalls to protect critical systems from unauthorized access	24	16
Use of intrusion detection and/or intrusion prevention systems used on the network	16	24
Continuous monitoring of security alerts from intrusion detection systems	8	32
Regular updating of signatures on intrusion detection and prevention systems	8	32
Regular review of security logs for intrusion detection systems and intrusion prevention systems for abnormal patterns of activity	24	16
Prevention of security logs for intrusion detection and intrusion which prevents them from being modified or deleted	24	16