Security Metrics: Relevance in Securing Educational Institutions

Pooja Tripathi[1] and Saurabh Gupta[2]

[1] Scholar, Mewar University Rajasthan
[2] POS, Minister of Home Affairs,
Sr.Technical Director of NIC
{Tripathipoojamail,Nic.Saurabhgupta}@gmail.com

Abstract. Security is easy; simply stop all communication with the external world: be recluse or isolated and you are secured. Every enterprise whether it is in education or defense or IT sector, everyone wants to keep its data, information and knowledge secured from intruders and competitors and even wants to expose the right kind of data, information and knowledge to its enterprise partner, employees, customers, government and stakeholders. Educational Institutions tend to deal in abstract concepts and knowledge that may not deliver tangible outcomes for years, decades and even for centuries. Educational Institutions faces unique information security threats as well as increasingly frequent and severe incidents such as information theft, data tempering, viruses, worms, and terrorist activity constitute significant threats to security of various universities. In this paper we strive to present the problem which the educational institutions are facing and endeavor to find the solution for it through security metrics.

Keywords: Security metrics, Vulnerabilities, IDS, Vulnerabilities estimation, Security posture, Denial-of –Service.

1 Introduction

Security has always been prime concern for any institution, with increase in interaction and exposure with other world this has become contextually more important. In the current scenario various enterprise are investing significant amount of resources for developing the tangled solutions that are caviling to daily operations and long-drawn out success with recent economic downturn. With shrinking IT budgets in an enterprise, IT departments are seeking more efficient, effective and innovative ways to solve problems. Empowerment of users and experimentation in the learning process are one of them. However, it often causes enterprise to struggle with their security issues. It has been discovered that empowering non-technical users results in the security exposure of network, applications, workstation, or servers. All such exposures threaten the stability of the IT environment if not handled properly, hence can result in compromised servers and possibly lost data [2]. According to the Ward and Peppard [2002] "Most organizations in all sectors of industry, commerce, government and education are fundamentally dependent on their information system"[1].

V.V. Das and P.M. El-Kafrawy (Eds.): SPIT 2012, LNICST 117, pp. 215–221, 2014.

Certain obvious questions strike to our mind when we talk about the security from an enterprise perspective:

- ✓ What are the specific threats to an enterprise?
- ✓ What are the security controls are in place?
- ✓ How sensitively information are being disposed?
- ✓ What backup/recovery policy is in place?

Despite advancement in IT security many Educational Institutions remains vulnerable to exploitation especially the human attitude threats. Educational Institutions generally collect large amount of data is about their operations and because there are common elements to the data which is collected, these have often emerged as metrics by which educational institutions are assessed at both national and international level [3]. There exist a large number of suggestions for how to measure security, with different goals and objectives. In many cases the goal is to find a single overall metric of security. However, given that security is a complex and multi-faceted property, we believe that there are fundamental problems in finding such overall metrics. Thus, we are currently developing a framework for security metrics that is based on a number of system attributes taken from the security and the dependent ability disciplines [18]. Having metrics related to different types of attributes facilities making quantitative estimation of the concept of combined security and dependability and improves our understanding of the underlying system properties [19].The educational sector has been mark as being heterogeneous, comprise of insulated information system that keeps stakeholders information [4]. Any universities X is said to have certain security postures, and university Y is said to possess a certain security posture different from X, connecting X and Y will result into more vulnerable system than the individual system (Fig-1).

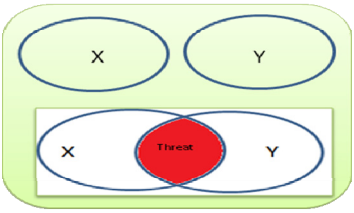

Fig. 1.

To ensure the interconnected system results into a moderate secure environment it is important to estimate the security of each enterprise systematically to reveal the overall security posture [5].

2 Study Design

We pursue the answers of the following questions in the study while when we are discussing about the Security metrics in context with the Universities:

- ➢ How information security can be improved at the educational institutions?
- ➢ What kind of security matrix to be determined to safeguard institution?

- What is the role of "User awareness" in security matrix?
- What kind of security matrix prevailing?
- How information security risks at the various educational institutional are determined?
- How various educational institutions are reducing information security risks?
- What is the impact of using security matrix in various universities?

3 Need and Benefits of Security Matrix

The metrics "gathering" process often leads to identification of security inconsistencies or holes. The motivation for seeking security metrics comes from different fact from an economic perspective , organization wants to know the return-on –investment(ROI), how much protection is gained per each additional investment[10][11]. Security metrics initiative can set the foundation for enabling organizations to identity risk levels, priorities corrective actions, raise awareness and helps to get answers for unclear questions such as: "Am I more secure today than before?", "How do I compare to others?" & "Are we secure enough?" This increases the confidence of the users towards institution. *Metrics is a quantities measures of degree to which a system, component, or process possess a given attribute, a calculated or composite quality based upon two or more years.* Measures or metrics in particular promote visibility, informed decision making, predictability, proactive planning and help avert surprises. [14]

It is impossible to get accurate figures for the number & cost of security breaches mainly because organizations are either not aware that the breeches has occurred, or reluctant to publicize it, for fear of ruining their reputations or destroying the trust of their stakeholders. However, in one instance the impact of malicious software in the form of worm/viruses attacks on the Internet was estimated to have caused $32.8 billion in economic damage for august 2003(Berghal 2003). In the recent years it has become widely acknowledge that human factors play a part in many security failures (Werich and Sasse 2002, Whiteman 2004). Technical threats are usually more high profile and grab much media and financial attention; however non-technical human and physical threats are sometimes more effective and damaging to information security. Non technical threats include Act of God (i.e. Fire, Flood, and Explosion). Threat analysis is necessary for specifying a concrete and comprehensive set of requirements so as to build all needs of security mechanisms for efficiently protecting the system. Moreover when conducted on an existing system, a correct evaluation and assessment of the threats and vulnerabilities allows us to priorities them. This analysis of prevailing security of the system would facilitate to propose an optimal enhancement plan. [17].

4 Plan for Building the Security Metrics in an Enterprise

Effective planning for security metrics implementation will serve as strong foundation for secured institution; below mentioned figure will enable us to plan for secured future institution (Fig-2).

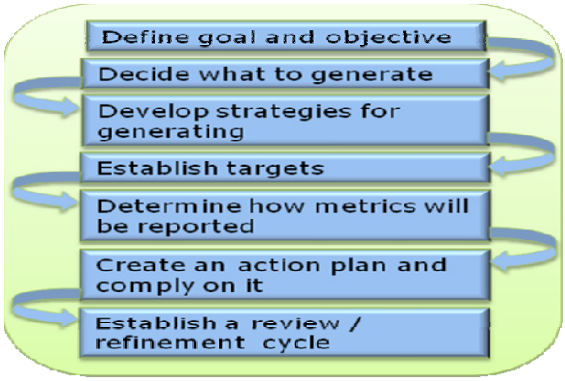

Fig. 2.

- ✓ Starts with statement of objective that must be collectively executed to accomplish the goal.
- ✓ Step 2 would focus on identifying the Security posture for which defects could be detected and managed. It would identify those standards for which compliance should be tracked.
- ✓ Step 3 defines strategies for collecting needed data and deriving the metrics those must be developed.
- ✓ In step 4 appropriate benchmarks would be identified and improvements target sets. This process provides fresh ideas for managing an activity, but also can provide comparative data needed to make metrics more meaningful.
- ✓ Step 5 emphasizes on Graphic representations (Dashboards), as they are particularly effective so that the end product can be visualized early on by those who will be involved in producing the metrics.
- ✓ Time to get the real work done. Step 6 defines action plan, the action plan should contain all tasks that need to be accomplished to launch the security metrics program, with expected completion dates.
- ✓ Final step emphasizes on formal, regular re-examination of the entire security metrics program which should be built into overall process. Certain Queries Should answered on priority during the review process.
- How much effort is it taking to generate the metrics?
- Are the metrics useful in determining new courses of action for the overall security programs?
- Is there reason to doubt the accuracy of any of the metrics?

5 How Security Metrics Works

The above figure (Fig-3) is just an approach to explain how security metrics works. Firewall is the primary component and provides protection at the perimeter level to ensure access policy control and it does not provide extensive threat detection capabilities due to the large amount of traffic handled. Security Metrics integrates vulnerability estimation with its IDS (Intrusion Detection System) which monitors all

network traffic and analyze the traffic in real-time. On the basis of IDS an IT administrator is notified in real time when an attack occurs. When an attack is launched, the system automatically looks at the last vulnerability estimation database for the attack target. An analysis is initiated to discover if the target is vulnerable to attack. If the target is not vulnerable then no alert is sent to the administrator. Attack Prevention require insertion into flow of traffic(two network interface connections) where an IDS simply sniffs exiting traffic and does not need to block the dataflow (one network interface connection).If the alert is real then an alert is sent to the administrator.

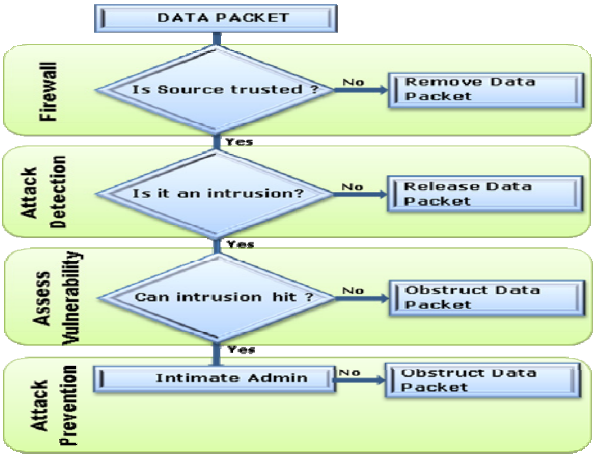

Fig. 3.

6 Vulnerability Estimation by Security Metrics

Vulnerability is defined as "a flaw or weakness in the security procedures, design, implementation, or internal controls that could be accidentally triggered or intentionally exploited and a result in security breech or a violation of the systems 'security policy" [20]**.** An attacker probes the System for weaknesses using vulnerability detection tools. Each vulnerability is ranked by risk on a scale of 0 to 9 with 9 being highly critical. The computer will fail if any vulnerability has a risk of 4 or above.

A good vulnerability estimation system will point out holes which we could never have found our self and tell about password problems, programming errors and basic architecture issues without the high price tag of a security consultant. All security components are launched at each target when a test is initiated. Security Metrics reports contain instructions, security patch links, and helpful information needed to immediately repair identified issues. With the help of Security Metrics a Pass/Fail scoring system can be developed for Vulnerability Estimation. Each security issue is rated according to its risk to our security. If our computer or server passes our tests, we can be assured that we are protected from thousands of potential hacking attacks.

7 Conclusion

Over the last few years, information security has changed and matured, moving out of the shadow of government, the military and academia into fully fledged commercial field of its own. Although there can be no agreement on the actual figure and percentages, empirical evidence from a number of security Surveys over the past years (Comp TIA, 2010: Comp TIA 2011: PricewaterhouseCoopers, 2008; Richardson, 2004) shows similar trends and patterns of security breaches. Information security breaches are increasing year on year. The most common type of attack is from viruses and malware, followed by hacking or unauthorized access to networks resulting vandalism of websites and theft of equipment (mainly laptops). Denial-of-service attacks are less frequent relative to viruses, with financial fraud and theft of information being the lowest kind of security breach experienced. In this paper we have just tried to implement the security metrics in the educational institutions to overcome the invisible attacks which these institutions are facing along with the working of security metrics.

References

1. Ward, J., Peppard, J.: Strategic Planning for Information System, 3rd edn. John Wiley and Sans Ltd., Chichestor (2002)
2. http://net.edu0cause .edu/ir/library/pdf/eqmo337.pdf
3. Tonich, D.: An Overview of University Performance metrics and Rankings,12, http://www.My Universty.Australlia.org
4. Payne, S.C.: A guide to security metrics. SANS Institue (2006)
5. Jafari, S., Metenzi, F., Fitzpatrick, R., Shea, B.O.: Security metrics for e-health care Information Systems.A Domain soecific Metrics Approach. IJDS 1(4) (December 2010)
6. Cuilhong, W.: 2010 2nd International Conference on The problems in Campus network information security and its solutions in industrial and information system (IIS) (2010)
7. AI-Akhras, M.A.: Wireless Network Security Implementation in Universities. In: 2nd Information and Communication Technologies, ICTTA 2006 (2006)
8. Zhu, J., Liu, L.: University network security risk assesment based on fuzzy analytic hierarchy process. In: 2010 International Conference on Computer Application and System Modelling, ICCASM (2010)
9. Kvavik, R.B.: Information Techonology Security: Goverance, Strategy, and Practice in higher education. Educause Centre for Applied Research (October 2004)
10. Rathbun, D., Homsher, L.: Gathering Security Metrics and Repairing the Rewards. SANs Institute (2009)
11. Beres, Y., Mont, M.C., Griffin, J., Shin, S.: Using Security metrics Coupled with Predictive Modeling and Simulation to assess Security Process. Hewlett-Packard Development Company (2009)
12. Kyobe, M.: Towards a frame work to guide compliance with IS Security policies and Regulations in a university. IEEE (2010) 978-1-4244-5494-5
13. McCoy, J.: Are we ready for a chief Information Security Officers (2005), http://www.docstoc.com/docs/18364711/Are-we-ready-for-a-chief

14. Sckimkowitch, S.E.: Key components of information Security Metric Program plan (2009), http://webcache.googleusercontent.com/search?q=cache%3AJolzW7iux3
15. Lane, T.: Information Security management in Australian Universities: An Exploratory analysis (2007), http://eprints.qut.edu.au/16486//
16. Jones, H., Soltern, J.: Facebook:Threats to privacy (2005), http://swiss.ai.mit.edu/6095/student-papers/fall05-papers/facebook.pdf
17. Stango, A., Prasad, N.R., Kyriazanos, D.M.: A Threat Analysis Methodlogy for Security Evalution and Enhacement Planning.
18. Jonsson, E.: Towards an integrated conceptual model of security and dependability. In: The First International Conference on Availability, Reliability and Security, ARES 2006, p. 8 (April 2006)
19. Almgren, M., Fu, Z., Jonsson, E., Kleberger, P., Larsson, A., Moradi, F., Oovsson, T., Papatriantafilou, M., Pirzadeh, L., Tsigas, P.: Mapping Systems SecurityReasearch at Chalmers.
20. Cole, E.: Network Security Bible, p. 61