A Study of Network Security Issues faced by the Corporate Sector in Pakistan with respect to Selected Organizations

AMINA SAID

MBA VIA

THE THESIS SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE DEGREE OF MBA (1 Year Program)

DEPARTMENT OF MANAGEMENT SCIENCES
BAHRIA INSTITUTE OF MANAGEMENT AND COMPUTER SCIENCES

BAHRIA UNIVERSITY ISLAMABAD

Abstract

This research aims to study the different types and levels of network security issues faced by selected companies in terms of factors that relate to the authenticity, integrity and confidentiality of information. The reason for this is the sudden expansion in connectivity between organizations and the increasing methods of communication. The intent is to discover how the Pakistan Telecommunications Company (Ltd) has used network security mechanisms to improve the performance of its Internet Service Providers and strengthen its IT infrastructure. The study also covers the technological opportunities and solutions that are available to individual Internet Service Providers as well as the general users of the Internet.

The research follows a descriptive style of study. Descriptive data collection methods have been used in acquiring information regarding Pakistan Telecommunications Company that is providing the infrastructure for networks operating in Pakistan. It's objective is to study the security issues faced by the controller of ISP's (i.e. PTCL) as well as the security issues being faced by a single ISP (Paknet). Paknet has been selected as a means of illustrating the hypothesis and its specific security threats are then analyzed.

Research instruments used consist mainly of primary and secondary research, unstructured interviews and observation. The range of topics covered and the responses were not constrained by any detailed interview guide (except for the unstructured interview format placed at

annex B). This flexible approach means that the order and wording of questions in each interview has varied from respondent to respondent. Sampling procedure selected was simple random sampling and the total sample size consisted of 2 organizations. First the DG IT was contacted for an unstructured interview at PTCL. Then regular visits to PAKNET determined that ISP's security needs. Specific security issues faced have been uncovered by the questionnaire(placed at annex C).

Findings show that the Pakistan Internet Exchange has been facing a type of DoS/DDoS attacks for about three months in 2003. The highest intensity of these attacks were observed in April 2003. DoS attacks fall under the broader category of hacking activities. These attacks are typically aimed at servers connected to the Internet with the intent of degrading or disabling the systems to the extent that the services become unavailable to legitimate users. Instead of attempting to hack into the target systems to access confidential data, DoS attacks focus on overwhelming the systems with bogus and/or defective traffic that undermines their ability to function normally. (Details are mentioned in the literature review). Since PIE supports Pakistan's Government websites, break down of these had been devastating.

Another attack was the YAHA Worm that choked all the ISP's downstream activity . Hence, the capability available both from infrastructure and skills point of view were not enough to handle these attacks.

Finally results suggest two types of strategic options that are available; to the Government in terms of improving the overall infrastructure, and the ISP's improving their performance.

Firstly, the government needs to set up a purpose-built facility to host government websites and portals. The suggested facility could centralize the hosting of all government portals and ensure that the breakdown of one link would not break vital Government communications. Initiative could also be taken to employ security specialists and administrators who can find ways of bridging 'loopholes', thus acting on the principle that 'prevention is better than cure'. In order to limit attacks such as DoS, the PIE network can be divided into access layers each having its own set of routing, switching and management devices to minimize chances of virus spreading. Proper hardware and software can be installed to safeguard attacks, the suggested are Network Intrusion Detection Systems.

Secondly, at the ISP level, administrators of corporate firewalls can install anti-spoofing measures to prevent hosts on the Internet from assuming the addresses of internal hosts and thus reducing the risk of invaders. ISPs can inform and educate their customers to use anti-virus software and keeping the software updated. It was noted during the research period that COMSATS is providing its customers with extended information regarding existing and upcoming viruses and how to avoid them. Proper firewalls can also be applied to protect the authentication, integrity and confidentiality of information. The suggested software is **Remote Authentication Dial-In User Service.**

Overall, the thesis covers the basic networking security issues being faced and suggests remedies that the Government can follow to improve its Pakistan Internet Exchange and the options available to Internet Service Providers to curb communications against intruder attacks.

TABLE OF CONTENTS

Title Page No.

I. INTRODUCTION ... 1

- Broad Problem Area / Background
- Rational of the Study
- Problem Statement
- Objectives of Study
- Definition of the terms

II. LITERATURE REVIEW ... 13

III. RESEARCH METHODOLOGY ... 96

- Type of Study
- Research Instruments
- Respondents of Study
- Sampling Procedure

IV. RESULTS & DISCUSSION ... 101

V. CONCLUSION & RECOMMENDATIONS ... 106

REFERENCES

APPENDICES