Chapter 55
Pragmatic Solutions to Cyber Security Threat in Indian Context

Cosmena Mahapatra
VIPS, GGSIPU, India

ABSTRACT

Recent attacks on Indian Bank customers have exposed the vulnerability of banking networks in India and the ignorance that prevails in the system. Unlike their foreign counterparts Indian banking networks are not aware of solutions easily available in market to counter cyber theft and cyber terrorism. SIEM or Security Information and Event Management is one such solution which could have easily negated these attacks. This chapter focuses on studying various cyber security mechanisms including SIEM for implementation of cyber defense effectively.

INTRODUCTION

Cyber security must be the foremost concern of all government and private organizations including banks now days. Although there are various advantages of digitization, yet it makes the data & networks vulnerable to cyber attacks from hackers and cyber terrorists. In foreign domain Organizations like CIS, NIST, etc (NIST, 2015) have set up various methods to secure the networks but their implementation ultimately depends on the understanding and risk assessment capabilities of people managing these digitized resources. In Indian context still much is left to be done. Although in recent time since the inception of “Digital India” the government bodies are actively involved in cyber security yet the recent Debit Card/ Credit Card related thefts from Hitachi’s owned ATM’s have put a question mark on the readiness of Indian Networks to more such attacks.

FRAMING OF EFFECTIVE CYBER THREAT MANAGEMENT POLICIES

India is new to cyber security threats. Its networks are not conditioned to fight off threats which may originate on the network and target its users. Although the recent government led by Prime Minister

DOI: 10.4018/978-1-5225-5634-3.ch055

Modi has shown remarkable interest in guarding Indian computer networks. However recent credit card/debit card frauds show that there is an immediate need in Indian context to frame strict policies against cyber threats. They may be framed around the following crucial points (CIS, 2015):

1. **Cyber Attack Analytics:** Use the knowledge gained from actual attacks that have already taken place to build effective and pragmatic defenses. Here, care must be taken to study and review data from known compromised systems only. Indian Banks and Government departments currently do not have a routine system of cyber threat sharing, this is the reason why multiple networks fail because of same type of attacks originating from same source IP addresses.
2. **Universal Metrics for Measurement of Security Measures:** Standardization has to be implemented via cooperation among various cyber defense organizations within India and abroad for agreeing on common and effective metrics for measurement of security measures so that changes to the security controls can be made in a smooth and fast mannerism.

   It also means that the people working in different levels of the security architecture must use the same names and procedures for implementation of the security measures. Any redundancy in these measures me lead to major losses during a cyber attack.
3. **Prioritize Risks through Hierarchical Structure:** This step requires building priority based architecture of all risks, putting the most dangerous of them at the top. The next step requires implementation of security controls that will solve the first layer, thereby proceeding to underlying layers thus strengthening the whole security architecture (Tomsitpro/guide.html, 2016).
4. **Continuous Revaluation of Security Measures:** The organization must carry out continuous measures to test and validate the effectiveness of current security mechanisms and metrics to help stay ahead of the trouble makers.
5. **Automation of Defenses:** All security measures must be automated and monitored round the clock so that organizations can get measureable, reliable and continuous feedback of the security measures involved.

VARIOUS MEASURES OF CYBER DEFENCES

It is important for a bank, organization as well as country to build various measures via which cyber defenses may be implemented seamlessly. These may be implemented by following steps (Robert, 2015):

1. **Building List of Authorized and Unauthorized Devices:** For the safety of the organization at physical layer, a list of authorized and unauthorized devices must be made and kept in the inventory for continuous and future analytics. This may be done via the use of various network sweeping tools or fingerprinting mechanisms (e.g. to read the OS being used) for identifying and storing the identity of all devices attached to the network.
2. **Building List of Authorized and Unauthorized Software:** It is important to keep a list of authorized software and unauthorized software in the security control so that unauthorized or malicious software may be timely detected and nullified.
3. **Customise Configuration of Hardware and Software on Laptops, Client Computers, Servers, and Mobile Devices:** A secure cyber network can be further strengthened by customizing the ports, software etc configuration as per the security requirements of the network. This is because the