Components Of Cyber Threat Management In An Organization

While the need for digital communication is increasing exponentially and is evolving continuously, there is a necessity to secure the data and privacy of networks in this world of cyberspace. This position paper is a summary of presentation on cyber threat management by EIR.

Introduction

In this digital age the use of computers is constantly being applied in every sphere of human interaction and business world. The interconnection of network in cyberspace constantly connects with computers, phones and digital devices which is an open access to all users. Cyber Threats are on the rise as there is continuous growth in requirement of data in this digital era. Cyber threat management is very much required for providing advanced threat research tactics and internal policies which are quite proactive in nature

What is Cyber Threat Management

Framework

Cyber Threat Management means protection of millions of digital devices from thefts or damage to their hardware, software or electronic data as well as disruption or misdirection of its services and its management by following steps and guidelines.

Observations:

Guidance and Control: Each company must make a call on the critical decisions on the amount of time and money that will be spent on protecting their technology and services. Organizations had to deal with dangers throughout history, but its observed that systematic anticipation of risks and to control it can avoid potential attacks significantly.

Threat Indicators: The possibility of an attack which is malicious in nature in order to damage, destruct or infiltrate files or data which is being gathered to cause harm to the business or user. The various cyber threats are as follows:

- Social Engineering: Malware creators use various ways to create links or apps which are then send to users to attract them to open this links and apps which ultimately infests their system with trojans that steal data and cause system abnormalities.
- Unpatched Software: Vulnerabilities like errors in programs or codes that can provide backdoor to malware creators and hackers to gain access in to system causing potential damage.
- Phishing: Fraudulent attempt to get usernames passwords or credit card details often for maliciously stealing money and cause damage.
- Network Travelling Worms: A computer program or code that could copy itself between machines.
- Advanced Persistent Threat: In this type of threat an attacker does a prolonged cyberattack by gaining access to a network and remains undetected for an extended period. E. g. Cuckoo's Egg, which documents the discovery and hunt for a hacker who had broken into Lawrence Berkeley National Laboratory.

Real-time Big Data Driven Situational Awareness: The concept of Big Data allows us to gather and do analysis on millions of petabytes of data, this data includes past attack, the process how that attack occurred, the weakness in network that gave hackers backdoor to penetrate the system, logs etc. which can be further analyzed and processed to predict and tackle any future possible attacks. All this is real-time to make more accurate decisions in given time.

Network Architecture: Blueprint of network that shows complete details of interconnected devices and security encryption to get general idea of network.

Honey-pot Development: A computer system that is set up to act as a decoy to lure hackers which in turn helps to detect, deflect or study attempts of unauthorized access to information system.

Analysis of logs: There are various activities and potential brute forcing happening on a network. This can be identified by network log analysis on various layers of transmission, devices and firewall.

Orient

To properly analyze the risk and take necessary actions proper orientation of task is required with proactive approach.

Security data science: Data science is required in cybersecurity with various challenges as follows:

In large organizations when you use SIEM or other security or traffic monitoring tools through this we have big data of security events, of which on small part are security incidents.

During monitoring of internet, or suspicious websites, you need dynamic data analysis to identify such activities.

Intelligence Gathering: Relevant information gathered which can be used to protect an organization from external and inside threats either by using SIEM or other tools like open source intelligence (OSIT), social media intelligence (SOCMINT). This can be implemented by following PCPAI methodology

Intelligence Data Mining: By identifying patterns in large datasets data mining can be used to analyze the complete network for possible flaws and abnormalities.

Risk Assessment: The goal of risk assessment in an organization is to understand and evaluate level of cybersecurity risks to organization assets and data.

Control Assessment: To meet the security requirements of the system correctly, the management, operational and technical security controls will be evaluated.

Behavior Modelling: The behavior of users and application networks are structurally modelled with normal operation traffic such that any signs of malicious activities would be detected as either:

- Anomaly: Any irregularity or deviation from normal network operating traffic.
- Misuse: Similar signatures of already known network threats are matched against the audit data stream.

Context Enrichment: Valuable insights to data and information in computer networks enables focus on items that indicate a security threat, create vulnerability, weaken security posture or violate security policy and compliance requirements.

Threat Data Warehousing: Information being stored in a single place will be used for creating and analyzing security reports. Most companies have operational databases that are used in the efficient use of data and information storage.

Decide:

To properly resolve the security risk and take precautions, a choice is to me made on the several possibilities of potential threats. This is further explained as:

Situational Awareness: The cognizance of a potential threat to computer system and networks.

Automated Triage: This is a highly sensitive system for the complete detection and diagnosis of possible threats to computer systems.

Security Analyst: In relation to the physical human presence needed for investigating computer security breaches, installing protective software measures, debugging to an ensure error-free system, a security analyst researched and documents current technology threats.

Act:

It is essential to act on the measures and initiatives put in place to handle possible threats to bring about security control in a system.

Incident Responses: An organization should have a clear guided process put in place for handling cyber threat attacks and effectively to manage the consequences of such attacks.

Security Operations Centre (SOC): The location of a unit in an organization where trained staff are assigned to supervise, monitor and control security issues.

Response Operations: Every organization needs to be able to strategize the implementation of quick response activities to potential cyber threats and in emergency situations.

Malware Analysis: Malicious program or software can be analyzed to gain full understanding of its origin, functionality and potential impact.

Automatic Responses: The technology of time conscious spontaneous identification and addressing of anomalous behavioral patterns of an organization's network.

Conclusion

Any reasonably likely scenario producing severe consequences would clearly demand action to reduce or eliminate the possible outcome. The business decision comes at the moderate and low severity ratings and low likelihood rankings. A risk-averse organization would probably address risks with moderate, and maybe even low, consequences. Risk assessment also requires assembling previously developed scenarios and ranking them by a combination of their consequence rating and likelihood rating. Point 'd' shows how this could be organized; scenarios with severe consequences and a high likelihood of occurring would be the top priority for implementing counter measures. Few points to keep a note of are: -

1. The cost of data breach is very high and costly affair.
2. Proper Team orientation, decision and action to be done
3. Regular log collection and analyzing the logs for any malicious activity should be thoroughly checked
4. Incident responses should be properly recorded and communicated to respective authorities (SOC) on time.
5. Intelligent Data mining and Context enrichment are very much important for planning according to intensity of attack.
6. Lessons learned from attacks must be recorded and used for future responses to avoid any mishaps due to negligence.
7. Upgradation of patch is very essential for every device in network.