TO MAKE PMO THE SAFEST PLACE IN THE WORLD

[1] Ishan Anand
[1] Bachelor of Technology, Computer Science, BMIET Sonepat

Abstract

Artificial Intelligence, when used with desired hardware systems has proven to be effective and smart than human surveillance and CCTV's, the satellite is taking positions of watchmen and guardians for monitoring purposes with basic security concepts and development of AI aided security systems takes in use of what we have learned over the period of our course. The proposed network security model for the Prime Minister's office (PMO) includes both the conventional approach which is used by the government today as well as an upgradation of the traditional approach to fixing the various vulnerabilities that it proposes. In the paper, the researchers has given sets of detailed security policies governing a wide variety of topics such as the hardware to be used, emergency response, basic mail and file sharing policies etc. Apart from the defining these policies, approaches have implemented the database credentials policy based on a Role Based Access Control Measure that we made relating to the hierarchy of the PMO.

Introduction

Network planning and design is an iterative process, encompassing topological design, network-synthesis, and network-realization, and is aimed at ensuring that a new telecommunications network or service meets the needs of the subscriber and operator. Network Security, on the other hand, is the process of taking physical and software preventative measures to protect the underlying networking infrastructure from unauthorized access, misuse, malfunction, modification, destruction, or improper disclosure, thereby creating a secure platform for computers, users and programs to perform their permitted critical functions within a secure environment. It involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authentication means that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs; conducting transactions and communications among businesses, government agencies, and individuals. Networks can be private, such as within a company, and others which might be open to public access.

Network security starts with authentication, commonly with a username and a password. Since this requires just one detail for authentication by the user, i.e. the password, it is thus sometimes termed as one-factor authentication. With two-factor authentication, something the user 'has' is also used like a security token or 'dongle', an ATM card, smart card or a mobile phone; and with three-factor authentication, something the user 'is' also used like biometric (a fingerprint or retinal scan) etc. Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component may fail

to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS) helps us to detect and inhibit the action of such malware. An anomaly-based intrusion detection system may also monitor the network traffic and may be logged for audit purposes and for later high-level analysis.

The issue of security design can be broken down into three basic parts namely:

- Security Policy
- Security Standard
- Security Guideline

Security Policy

A policy is typically a document that outlines specific requirements or rules that must be met. In the information/network security realm, policies are usually point-specific, covering a single area. For example, an "Acceptable Use" policy would cover the rules and regulations for appropriate use of the computing facilities.

Security Standard

A standard is typically a collection of system-specific or procedural-specific requirements that must be met by everyone.

Security Guideline

A guideline is typically a collection of system specific or procedural specific "suggestions" for best practice. They are not requirements to be met but are strongly recommended. Effective security policies make frequent references to standards and guidelines that exist within an organization.

Related Work

A network security policy, or NSP, is a generic document that outlines rules for computer network access, determines how policies are enforced and lay out some of the basic architecture of the company security/ network security environment. It specifies these rules for individuals or groups of individuals throughout the company. While writing, the security document can be a major undertaking. A good start can be achieved by using a template. National Institute for Standards and Technology provides a security-policy guideline, but we referred to the SANS Security Policy Resource page for the policy templates we required for this project. It is a consensus research project of the SANS community that aims to offer everything one needs for the rapid development and implementation of information security policies.

In Security Guideline, the author presented a report on the principles of network security design that explains how the deployment of an effective and scalable network security system requires proper designing according to risk analysis results as well as security principles. The author further presents in detail, all the fundamental IT systems security principles should be taken into account, when designing the network security system, such as, defense-in-depth, compartmentalisation of information, principle of least privilege, weakest link in the chain, security zones, intrusion prevention, etc., which helped us a lot while designing our system.

Problem Statement

In the research, attempts have been made to develop an AI who can fulfill the design policies governing the complete network infrastructure, including the kind of hardware use, different authorization and access controls, different sharing rights policies, system administration policies, email and database access policies, password policies, policies for VPNs and Digital Signatures etc. and somehow the best suitable way has been

chosen. Through this research, it was the attempt to help design a better and more sophisticated network security measure for the PMO. Since the current system in place has issues like lack of proper division of security policies, Upgradation of systems and proper emergency response techniques. A small observation can be made from the simple fact that when a recent RTI was filed to the PMO to disclose the number of PCs hacked, it replied with the answer that the information was unavailable at the moment.

Approach

In our project, we chose the hierarchy to create an RBAC structure which we later implemented in our database which is a toned-down version of the actual hierarchical system present at the PMO.Prime Minister at top of the hierarchy with an unhindered access to documents and resources. After that comes the System Administrator, NSA and the Principal Secretary to the Prime Minister. The System Administrator himself cannot access the documents and in case of emergency or break down, works on a token generation system to gain a higher clearance. In this period, he is granted a special access permission by the Prime Minister and his work is audited by the Principal Secretary. The next tier is of the Private Secretary and the Assistant to the NSA. Up till here, the resources such as printers, scanners, Internet access etc. has been individually divided in abundance. The 4^{th} tier forms the Joint Secretary and the staff below. Here the resources are shared. Instead of individual access points, the staff uses a common WiFi, printer etc. The entire hierarchy can be divided into two blocks with tiers one to three in block one and tier four and below in block two depending on the sharing of resources. We shall only be taking the following five tiers in the domain of this project.

Based on the above classification and the research done by the group members on the PMO, we came up with the following security policies related to various aspects of the Network design, AI architecture and implementation.

Device Hardware and Network Hardware

Based on our research, the following is the list of permissible hardware devices with their respective specifications to be used in the PMO:

Desktop Computers

- To be used by the officials listed in Annexure 1
- No unauthorized external device is allowed to install or connect to the network or to the computers.
- The installation and the removal or repair of faulty sets will be authorized by the TCO and the Head of the maintenance.

Laptop

- To be used by the officials listed in Annexure 1
- No unauthorized external device is allowed to install or connect to the network or to the computers.
- The installation and the removal or repair of faulty sets will be authorized by the TCO and the Head of the maintenance.

Mobile

- To be used by the officials listed in Annexure 1

- No unauthorized external device is allowed to install or connect to the network or to the computers.
- The installation and the removal or repair of faulty sets will be authorized by the TCO and the Head of the maintenance.

Printer

- A common Machine will be installed in the offices of the officials
- Officials listed in Annexure 1 will receive a separate machine which cannot be used by their sub-officials of any other official of his/her rank.
- The installation and the removal or repair of faulty sets will be authorized by the TCO and the Head of the maintenance.

Television Set

- To be installed in the emergency room, the control room, private meeting room of the PM.
- The installation and the removal or repair of faulty sets will be authorized by the TCO and the Head of the maintenance.

Projector

- To be installed in the emergency room, the control room, private meeting room of the PM.
- The installation and the removal or repair of faulty sets will be authorized by the TCO and the Head of the maintenance.

Server

- Only the system admin and the server admin can operate on it with a clause of no external device which is not issued by the NSA.
- The installation and the removal or repair of faulty sets will be authorized by the TCO and the Head of the maintenance and NSA.

Routers

- Only the system admin and the server admin can operate on it with a clause of no external device which is not issued by the NSA.
- The installation and the removal or repair of faulty sets will be authorized by the TCO and the Head of the maintenance and NSA.

Switches

- Only the system admin and the server admin can operate on it with a clause of no external device which is not issued by the NSA.
- The installation and the removal or repair of faulty sets will be authorized by the TCO and the Head of the maintenance and NSA.

AI Policy

Artificial Intelligence is an essential component of the PM Office information systems security infrastructure. AI is defined as a security that controls and restrict network connectivity and network services. They establish a control point where access controls may be enforced. Connectivity which is pre-defined is permitted to exchange information. A service is sometimes called an application, and it refers to the way for information to flow through the system.

This policy applies to all system in the PM Office network, which is managed by the network administrator. No changes can be made in this policy until they are approved by the Network Administrator with proper application approval. All the systems in the network are playing the role of secured

machines, as the rules are defined according to different levels in the office. These systems are managed according to the rules defined in the policy.

Specifications of the Artificial Intelligence

For surveillance of all the Hardware components, an AI in terms of software would be developed who can take control of everything with maximum efficiency. The required specification for the AI to be assigned at PMO would be:

- Required Documentation – Prior to the deployment of every command, a diagram of permissible paths with a justification for each, and a description of permissible services accompanied by a justification for each must be submitted to the Network Administrator. Permission to enable such paths or services will be granted by the Network Administrator. The deployment of the firewall provided will be periodically checked by the Software Engineer and Network Administrator. Any changes to path or services must go throw the same process as described below.
- Default to Denial - Every connectivity path and service that is not specifically permitted by this policy and supporting documents issued by the Network department must be blocked by the security features of the AI. The list of currently approved paths and services must be documented and distributed to all system administrators with a need to know by the Network department. An inventory of all access paths into and out of PM Office internal networks must be maintained by the Network department.
- Connections Between Machines - Real-time connections between two or more computer systems must not be established or enabled unless the Network department has determined that such connections will not unduly jeopardize information security.
- Regular Testing - Because AI provides such an important control measure for networks, their strength and proper configuration must be tested on a regular basis. Where vendor software supports it, this testing must include the use of software agents that automatically check to determine whether firewalls remain configured and running in a manner that is consistent with both security policies and the Network Architectural plan.
- Logs - All changes to security configuration parameters, enabled services and permitted connectivity paths must be logged. All suspicious activity that might be an indication of either unauthorized usage or an attempt to compromise security measures also must be logged. The integrity of these logs must be protected with checksums, digital signatures, encryption, or similar measures.
- Intrusion Detection - All firewalls must include intrusion detection systems approved by the Network department. Each of these intrusion detection systems must be configured according to the specifications defined by the Network department. Among other potential problems, these intrusion detection systems must detect unauthorized modifications to system files, and detect denial of service attacks in progress.
- External Connections - All in-bound real-time Internet connections of PM office internal networks or multi-user

computer systems must pass through a security check before users can reach a login banner. No personal computers are allowed for usage.

- Virtual Private Networks - To prevent unauthorized disclosure of sensitive and valuable information, all inbound traffic, with the exception of Internet mail, approved news services, and push broadcasts, that accesses PM Office networks must be encrypted with the products approved by the Network department. These connections are often called virtual private networks (VPNs).
- Firewall Access Mechanisms - All PM Office firewalls must have unique passwords or other access control mechanisms. The same password or access control code must not be used on more than one firewall.
- Settings Access Privileges - Privileges to modify the functionality, connectivity, and services supported by settings must be restricted to a few technically-trained individuals. Unless permission from the Network Services Director has been obtained, these privileges must be granted only to individuals who are full-time permanent employees of PM Office, and not to temporaries, contractors, consultants, or outsourcing personnel.
- Secured Subnets - Portions of the PM office internal network that contain sensitive or valuable information, such as the computers used by the Human Resources department, should employ a secured subnet. Access to this and other subnets should be restricted with firewalls and other access control measures. Based on periodic risk assessments, the Network department will define the secured subnets required in the Network Architecture.
- Demilitarized Zones - All Internet commerce servers including payment servers, database servers, and web servers must be protected by firewalls, and be located within a demilitarized zone (DMZ), a subnet that is protected from the Internet by one or more firewalls. An internal network, such as an intranet, is also protected from the DMZ subnet by one or more firewalls.
- Network Management Systems - AI must be configured so that they are visible to internal network management systems. They should also be configured so that they permit the use of remote automatic auditing tools to be used by authorized staff members. Unless deliberately intended as a test, such automatic auditing tools must not trigger a response sequence through firewall-connected intrusion detection systems.
- Server Dedicated Functionality - AI software must run on dedicated machines that perform no other services, such as acting as a mail server. Sensitive or critical PM Office information must never be stored on a firewall.
- Monitoring Vulnerabilities – PM Office staff members responsible for managing system should stay current with information about system vulnerabilities. Any vulnerability that appears to affect networks and systems must promptly be brought to the attention of the Network Director.
- System Security - Every bit of code of the AI software must be encrypted in a shell with 'X'-type encryption. Besides this, all master computers must be

located in locked rooms accessible only to those who perform authorized firewall management and maintenance tasks approved by the Network Director.

Conclusion and Future Work

In our project, we have tried to put together both the traditional as well as modern security concepts which can work in the correlation with the expected security standards of the PMO. We have given both the hardware specifications and AI requirements and created various security policies to govern them. In our implementation of the research, we can also use some of these policies to create an RBAC structure file access control system via using a database. Over here we have defined various roles for the users and specified a security clearance for each of the roles along with their read and write specifications and special privileges if any.

Currently, due to lack of hardware, we are unable to implement any other policies and therefore we would try to our best of abilities to procure the required hardware and software to implement our security policies on them.

References

- https://en.wikipedia.org/wiki/Network_security_policy
- https://www.sans.org/security-resources/policies
- Stawowski, Mariusz. "The Principles of Network Security Design." ISSA Journal (2007): 29-31.
- Woodall, Stephen. "Firewall Design Principles." Computer Networks and Computer Security. Coursework paper, North Carolina State University, USA (2004).
- Michalos, Michail. "Design and implementation of Firewall security policies." (2014).
- Daya, Bhavya. "Network security: History, importance, and future." University of Florida Department of Electrical and Computer Engineering (2013).
- Stawowski, Mariusz. "Network Security Architecture." ISSA Journal (2009): 34-38.

Annexure 1

List of officials to get their separate devices

- PM
- Private Secretary to the PM
- Principal Secretary to the PM
- NSA
- Directors of sub-departments like RTI, PRO etc.
- Reference Officer