**ASSSIGNMENT - 2**

**Subject: Information Security (CS6404)**

**Guided by: Dr Bhaskar Mondal**

**NAME : Nikhil kumar**

**Roll – 1806055**

**Branch – CSE-I**

**CABLE TV**

**NETWORK SECURITY POLICY**

**Network Security Policy**

A network security policy is a set of standardized practices and procedures that outlines rules network access, the architecture of the network, and security environments, as well as determines how policies are enforced.

**1. Acquisition Assessment Policy**

The purpose of an Acquisition Assessment Policy is to establish Infosec responsibilities regarding corporate acquisitions, and define the minimum security requirements of an Infosec acquisition assessment.

**2. Bluetooth Baseline Requirements Policy**

The purpose of this policy is to provide a minimum baseline standard for connecting Bluetooth enabled devices to the company’s network or a company owned device. The intent of the minimum standard is to ensure sufficient protection Personally Identifiable Information (PII) and confidential company data.

**3. Database Credentials Policy**

The purpose of the Remote Access Policy is to define rules and requirements for connecting to the company’s network from any host. These rules and requirements are designed to minimize the potential exposure to the company from damages which may result from unauthorized use of company resources. Damages include the loss of sensitive or company confidential data, intellectual property, damage to public image, damage to critical company internal systems, and fines or other financial liabilities incurred as a result of those losses.

**4. Remote Access Tools Policy**

The Remote Access Tools Policy defines the requirements for remote access tools used at the company.

**5. Router and Switch Security Policy**

The purpose of the Router and Switch Security Policy is to describe a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity at or on behalf of the company.

**6. Wireless Communication Policy**

The purpose of the Wireless Communication Policy is to secure and protect the information assets owned by the company. The company provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. The company grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

**7. Wireless Communication Standard**

The Wireless Communication Standard Policy specifies the technical requirements that wireless infrastructure devices must satisfy to connect to a company network. Only those wireless infrastructure devices that meet the requirements specified in this standard or are granted an exception by the InfoSec Team are approved for connectivity to a company’s network.

**8. Remote Access Policy**

The Database Credentials Policy states the requirements for securely storing and retrieving database usernames and passwords (i.e., database credentials) for use by a program that will access a database running on one of the company’s networks.

**9. Technology Equipment Disposal Policy**

The purpose of the Technology Equipment Disposal Policy is to define the guidelines for the disposal of technology equipment and components owned by the company.

**10. Information Logging Standard**

The purpose of the Information Logging Standard Policy is to address this issue by identifying specific requirements that information systems must meet in order to generate appropriate audit logs and integrate with an enterprise’s log management function.

**12. Server Security Policy**

The purpose of the Sever Security Policy is to establish standards for the base configuration of internal server equipment that is owned and/or operated by the company. Effective implementation of this policy will minimize unauthorized access to the company’s proprietary information and technology.

**13. Software Installation Policy**

The purpose of the Software Installation Policy is to outline the requirements around the installation of software on company computing devices. To minimize the risk of loss of program functionality, the exposure of sensitive information contained within the Company’s computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.

**14. Workstation Security (For HIPAA) Policy**

The purpose of the Workstation Security (For HIPAA) Policy is to provide guidance for workstation security for company workstations in order to ensure the security of information on the workstation and information the workstation may have access to. Additionally, the policy provides guidance to ensure the requirements of the HIPAA Security Rule “Workstation Security” Standard 164.310(c) are met.

**Application security best practices for the cable industry**

Over the years, the cable television industry has endeavored to provide an ever-wider range of services to cable TV subscribers. The industry has ventured into digital video, voice and data to accommodate the growing demands of its client base. However, the launch of innovative solutions such as operating the set top box (STB) via a mobile phone; recording shows through click of a button; and, online payment using handheld devices, has also increased the application security attack surfaces for hackers to exploit.

There are thousands of websites related to cable modem hacking alone. Application security is a serious concern, and hackers focus on extracting personally identifiable information (PII) of users at the subscriber end, as well as on backend processing applications. To address these application security concerns, a cohesive solution around a robust information security policy is essential.

**Domain topology**

A typical cable eco-system has two major players – service providers and subscribers. If we hypothetically map the X.805 standard prescribed by the International Telecommunications Union to a cable network, the service provider spans the management and control plane, while subscribers can be placed at the end-user plane.

**Management plane**

The service provider network comprises various network components such as edge quadrature amplitude modulation (EQAM) and cable modem termination system (CMTS) that receive radio frequency signals. It interfaces with various underlying applications to deliver services. In the management plane mediation, billing, operational and business support systems, end-user portals and content processing applications are deployed.

End user plane

On the end-user plane, STBs and cable modems receive signals from the service provider and deliver them to subscribers. Cable services are then accessed via digital TVs, smart phones, tablets, laptops, or desktops. This is facilitated by applications such as embedded operating systems, CAS/DRM applications for encryption and decryption or mobile applications for live TV, payment processing and other features.

**Mitigating controls**

Application security threats can be alleviated to a certain level with implementation of security measures such as firewalls, intrusion prevention systems, and so on. However, a holistic approach to addressing application security threats is desirable, by designing and implementing appropriate information security controls that work in unison. The recommended best practices to address application security threats are:

**Content security:**

**.** Implement content protection systems such as CAS and DRM.

**.** Design applications on terminal devices such that they do not transmit decrypted content through user-accessible bus, storage or memory, and require permission of the content-protection solution deployed.

**.** Store content protection keys used for decryption in a safe location accessible only by a built-in device cryptographic module.

**Device security:**

**.** Provision terminal devices to detect, isolate and remove malicious codes or viruses.

**.** Make applications on terminal devices tamper-proof using code obfuscation or HSM to store content keys.

**.** Follow a secure image download process (DOSCIS specification) and validate software images using digital signatures during installation.

**.** Harden cable modems being used as wireless access points.

**End-user security:**

**.** Use secure communication channels such as HTTPS/SSL for applications deployed

**.** Use FIPS compliant encryption libraries such as Bouncy Castle and B-SAFE.

**.** Implement step-up authentication for financial transactions.

**.** In addition to the above controls to mitigate application security threats specific to the cable industry, following are the overall security recommendations to address security at a holistic level:

**.** Follow secure SDLC as an institutionalized process.

**.** Implement access control solutions to identify, authenticate, authorize and provide accountability.

**.**  Adopt application security assurance testing to provide actionable data for vulnerability validation and remediation efficiency.

**.** Operate a secure computing infrastructure to ensure confidentiality, integrity and availability of information.

**.** Enforce regular application security audits to ensure compliance sustenance.

**Scope**

The cable industry does more than just provide internet connectivity for millions of customers: it also plays an active role in driving security in the broader internet ecosystem. Cable operators have a long history of successfully defending against attackers seeking to steal service, customer data and video content. The cable industry has been protecting the delivery of high-value video content for over 30 years through technology that has never been breached in a successful, scalable manner. Moreover, the industry has been setting fundamental broadband security features through cable internet access standards for over 20 years to ensure the confidentiality, integrity and availability of cable broadband services globally. As the details and motivations of attacks continue to evolve, so does the security incorporated by cable operators.

Of particular focus for CableLabs is the urgent need to address the risks associated with insecure internet-connected devices (“Internet of Things” or “IoT”). IoT represents the next major axis of growth for the internet. But, without a significant change in how IoT providers approach security, the explosion of connected devices increases the risk to consumers and to the basic functionality of the internet. The consensus forecast has the number of devices connected to the internet doubling (or more) between 2016 and 2020. To the extent these devices do not contain sufficient security, the number of potential attack vectors will multiply rapidly as IoT proliferates.

**Account Policies**

**Password Policy**

* If a service is trivial enough to be provided by an unprivileged account then a root account should not be used.
* Administrator, root, or other superuser account rights will only be granted to the servers when the use of non-privileged system accounts will not serve the same purpose. As with other user accounts, these accounts will be approved, inventoried, and utilized in accordance with this organization's Account and Identity Management Policy.
* Only authorized user accounts shall be configured and utilized on each of the organization's servers in accordance with the inventory approved for each server and the organization's Account and Identity Management Policy.
* Remote administration shall only be performed on systems or servers where it has been authorized by the system's data owner. All approved remote administration shall be performed over properly encrypted channels using non-generic user accounts in accordance with this organization's Account and Identity Management Policy.
* Database passwords must be securely stored in the form of hash (with proper salting) and should be secured physically by the CEO.
* If there are some unexpected requests from the user to the server, then their accounts should be locked after a certain number of requests. The locking period could range from few hours to few days, based on the number of requests and after analysis of any potential threat.
* If some threat or hacking probability is sensed from some account, then the account should be blocked immediately and the registered numbers and emails should be blacklisted in the database. Further investigation should be initiated and vulnerability testing should be done.
* If a Data Owner or a member of Operation Group leaves the organization, then his/her accounts should be shut. Moreover, the passwords and other information of the system he/she had been working on should be reset as soon as possible.
* If a customer discontinues the services of the organization, their accounts should be shut and information should be deleted after a certain period of time.

**Account Lockout Policy**

* If a user forgets his password for his system, then there are the following measures to retrieve back the account:
* Using two step authentication via sending One Time Password (OTP) to the user’s registered email or mobile number.
* Answering the security question correctly. This security question is set by the user during allotment of the system.
* For the servers that are being accessed remotely, if their password is lost then the concerned Data Owner or the Operation Group should be contacted physically or on a secure channel.

**Local Policy**

**Backup/ Security options**

* Backups of each system will be performed on a regular basis in accordance with the organization's Data Retention, Backup, Archive Policy. These backups shall be performed of each server's operating system, application code, system and application configurations, and business data.
* All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:
* Daily incremental tape backups will be retained for at least 1 month.
* Weekly full tape backups of logs will be retained for at least 1 month.
* Monthly full backups will be retained for a minimum of 2 years.
* Security-related events will be reported to InfoSec, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
* Port-scan attacks.
* Evidence of unauthorized access to privileged accounts.
* Anomalous occurrences that are not related to the specific applications on a host
* Security policies help to protect a company's network from both external and internal threats. For example, 91% of cyber attacks start with a phishing email. While employees may not be intentionally compromising a network, bad actions such as clicking on malicious links or downloading documents containing malicious code create security vulnerabilities. Therefore, implementing a security awareness training program to educate employees on security threats and how to identify them help to reduce this risk.

**Audit policy**

* Audits will be performed on a regular basis by authorized organizations within the organization.
* All the decisions related to auditing will be reviewed by the Auditing Committee in their regular meetings.
* Audits will be managed by the internal audit group. InfoSec will filter findings not related to a specific Operation group and then present the findings to the appropriate support staff for remediation or justification.
* Every effort will be made to prevent audits from causing operational failures or disruptions.
* Any internal auditing issues determined by the committee should be immediately reported to the Board.
* Risk based internal audit annual plan will be reviewed and approved.

External auditing may be done at times for better understanding and learning.

**User Rights**

* Users can send their grievances, feedback to the organization using emails, social media or any other medium. These should be monitored actively and their problems should be solved within a fixed stipulated time.
* Users have the right to inquire about the organization, it’s working and the legitimacy of the service being provided to them. Hence, such information should be made public via some booklet, website and proper certifications should be shown.
* Users can discontinue the services of the organization anytime but only after paying for the dues (if any) for any of the paid service.
* Data of a user is sensitive. If the user feels their data is being compromised, then the organization is answerable to them. Demand for proper proof can be sought from the user and the organization in extreme cases.

**General Configuration Guidelines / Recommendations**

. • Servers must be registered within the corporate Enterprise Management System. At a minimum, the following information is required to positively identify the point of contact:

* Year of installation
* Hardware and Operating System/Version
* Main functions and applications, if applicable
* Place of operation (that is concerned with which branch)
* Working condition
* Server contact(s)
* Expected expiry period
* Backup status and contact
* Information in the corporate enterprise management system must be kept up to date. This includes deletion of obsolete records, creation of new records concerned with the installation of new equipment and update of any change that has been made in the equipment.
* Configuration changes for production servers must follow the appropriate change management procedures. This ensures that the configuration changes must be recorded and stored properly whilst keeping up to date.
* Each server system must complete the organization's certification and accreditation process prior to being allowed on the production business network in accordance with the organization's Certification and Accreditation Policy that includes the guidelines and procedures needed to be followed for the certification.
* Operating System configuration should be in accordance with approved company’s guidelines. Use of open source operating systems that are popular and are in use by different companies are encouraged but only after passing the security guidelines and procedures of the company in accordance with the organization’s Software Update Policy.
* An approved device configuration standard will be created and maintained that will contain the documentation for all security configurations for each server (and other backend equipment, if any) along with the version and the type of service provided by any server.
* Services and applications that will not be used must be disabled where practical. Their records should be updated accordingly followed by analysis for the reason for stopping the services or any reason of failure. The analysis should come up with an efficient and practical solution to any discrepancy that is found and should be followed by the immediate implementation of the solution.
* A secure system image shall be created, maintained, and deployed for each of the organization's servers that include all necessary and approved software and configuration settings. This organization will attempt to maintain as few system images as necessary in order to maintain as much consistency between systems as possible.
* When a service is being provided by the server or alternately if a customer is accessing some service, if possible, the operations should be recorded/ logged and protected through access control methods such as TCP Wrappers.
* All server systems that are visible to any untrusted network, including the internet, will routinely be re-evaluated for business purposes and gradually they will be moved to a trusted and secured network as soon as possible.
* A test server system, which is a mirror of the production server system, will exist for each of the organization's servers. This test version of the system must be kept in a trusted state of this organization's production network
* The most recent security patches must be installed on the system as soon as practical. This should not be followed immediately only when some application or service would interfere with requirements and goals of the business.
* Procedures shall be maintained which detail the specific server security configuration standards necessary to protect each system. These procedures shall be based on the classification levels defined in this organization's Data Protection and Classification Policy.
* Trust relationships between systems are a security risk, and their use should be discouraged. Using a trust relationship when some other method of communication will suffice is discouraged.
* At least one data owner will be defined for each of the organization's servers located at different locations. Data owners will work with Operating groups and lead them to define the classification levels, provide necessary resources for the system, and maintain the system in accordance with the organization’s Data Protection and Classification Policy and Risk Management Policy.
* Each of the organization's servers will have appropriate and approved file and access control lists (based on network) inventoried and configured and file integrity assessment controls in accordance with the organization's Access Control and Authorization Policy, Account and Identity Management Policy, and Network Security Policy.
* Always use standard security principles of least required access to perform a function.
* An up-to-date inventory of all production and test server systems will be maintained at all times in accordance with this organization's Risk Management Policy. This inventory will include, at a minimum, information regarding the following:
* The system's hardware configuration;
* All approved software installations;
* All authorized system user accounts;
* All file access controls and user right assignments;
* All access control lists based on network;
* All authorized running services; and
* All listening network ports.
* Each system on the company’s local network will run the latest, tested, approved and updated system software for both the server's operating system and all applications installed on the system in accordance with this organization's Software Update Policy.
* If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH).
* Vulnerability scans will be performed on a regular basis on each of the organization's servers in accordance with this organization's Vulnerability Management Policy and the classification level of the server being scanned. It is required as vulnerabilities are often untraceable which leads to risk in the security of the data.
* Servers should be physically located in an access-controlled environment. They should be physically protected using latest security measures like Biometric access and should be guarded 24x7 in accordance with the organization’s Access Control and Authorization Policy and Physical Security Policy.
* Servers are specifically prohibited from operating from uncontrolled and unauthorized cubicle areas.
* The organization believes in Sustainable Development and is cautious not to harm the environment due to any of its business or technological operations. Hence, physical and environmental security controls will be implemented for each of this organization's servers in accordance with the organization's Physical Security Policy and Environmental Security Policy.
* Penetration tests shall be performed on a regular basis on each of the organization's servers in accordance with the organization's Penetration Testing Policy and the classification level of the server being scanned.
* All server administrative tasks will be conducted on a secured system exclusively for that purpose. Common business tasks such as word processing, internet access, and email will be done from a standard business system in accordance with the organization's Access Control and Authorization Policy.

**Firewall configurations**

* An application firewall will be installed in front of all critical servers and logging of critical events and alerts will be completed in accordance with the organization's Logging and Monitoring Policy.
* Each device regardless of the location on the network, will utilize a host-based firewall. Host-based firewall rules will be linked to authorized running processes whenever possible. These firewalls will only allow documented and approved services and ports and they will include a default-deny file that drops all traffic that is not explicitly allowed.
* Application firewalls will be maintained in front of all critical applications in order to limit the effectiveness of attacks against the application. This system will be updated on a regular basis with signatures of new or emerging attacks and will be configured to both block and alert this organization when attempts are made to attack the web applications being protected by the system. This will be completed in accordance with the organization's Network Security Policy.
* It is recommended to use the screened subnet firewall configuration as it is the most secure type of firewall till now and has three layers of defence.

**Protection against attacks**

* **Port Scan attack**

A port scan attack is a very common attack these days. An intruder/ hacker can note the TCP/ UDP port numbers while some system is running and use them for future attacks. To this, the Firewall should be able to counter this by tracking down the connection of multiple ports by a remote computer and prohibiting it.

* **IP address spoofing**

An intruder from outside may try to send a packet towards the internal corporate network with the source IP address equal to the IP address of the internal users of the company. To prevent this, the firewall must be able to reject those packets where source IP is equal to the IP of some internal users.

* **Fragmentation attack**

An attacker may at times send packets in the form of fragments and then get those fragments assembled at the victim computer/system. Thus, the firewall should discard the packets which use the TCP protocol and is fragmented.

**Administrative**

The Chief Executive Officer (CEO) of this organization has the responsibility for the overall administration of this policy. Establishment of the administrative procedures for the compliance with Corporate Policies is the responsibility of the officers and the managers of this organization and its business units.

**Enforcement**

Any employee found to have violated this policy may be subject to disciplinary, up to and including termination of employment. In extreme cases, legal action will be initiated.