OpenVuln Security Framework

A Complete Reference for your Information Security needs

Compiled by

RAJHESHWAR V

SHARAT N

VISHAL S

Introduction

Information Technology seeps its way through every part of our lives, businesses and organization. But the core aspect is information, data that drives.

The proposed framework tries to cover all aspects of information security which includes methodology, practices, strategies, analysis, and technical details becoming a wealthy resource for defining a policy or a framework in your own place to meet the information security needs

Index

|  |  |  |
| --- | --- | --- |
| **1** | **Part One - Foundations** |  |
|  | Information Security Overview |  |
|  | Risk Analysis |  |
|  | Compliance with Standards, Regulations, and Laws |  |
| 1.4) | Secure Design Principles |  |
| 1.5) | Security Policies, Standards, Procedures, and Guideline |  |
|  |  |  |
| **2** | **Part Two - Database Security** |  |
|  | Database Security |  |
|  |  |  |
| **3** | **Part Three - Network Security** |  |
| 3.1) | Secure Network Design |  |
| 3.2) | Securing Routers and Switches |  |

Part One

Fundamentals

* 1. Information Security Overview

What is information?

Information is a valuable resource. Information is frequently one of the most valuable assets a firm has. Information can occasionally give an organisation a competitive advantage that it can use to outperform its rivals.

Information can be categorised into groups such as

• *Unclassified information*, which is information that is not protected by a classification system and can be shared or distributed without restriction.

• *Controlled Unclassified Information (CUI)* is information that needs to be protected or made available under certain conditions in accordance with the laws, rules, and government-wide policies.

• *Confidential information* is data that must be kept private and accessible only to authorised staff members. Examples include research and development plans, manufacturing procedures, strategic corporate information, product roadmaps, process descriptions, customer lists and contact information, PII (Personal Identifiable Information), PHI (Personal Health Information), or even something as basic as your ATM login credentials.

• *Specialized/secret information* is data whose privacy must be strictly upheld, such as trade secrets, formulas, production information, and other intellectual property, as well as proprietary techniques and processes that specify how services are offered, encryption keys, etc. It may result in significant loss or harm to a company, government, or organisation if it is revealed or leaked.

**Building a Security Program**

Now that you know what information is, what kinds of information there are, and why information security is important. Learn what a security programme is and why an organisation would require one.

The security policies, methods, tools, and controls used by an organisation are listed in a document called a security programme. When it comes to any area of information technology and organisational security, it may be considered the "holy-grail."

When developing a solution, you need to answer the questions “What” and “Why?” In building a security program, you should begin with describing what is needed and why, and to proceed to define how it will be implemented, when, and using which particular methods.

The components in building a security program

* Authority
* Framework
* Assessment
* Planning
* Action
* Maintenance

Let’s look at each component in detail

**Authority**

A security programme establishes the goals, duties, and scope of the security organisation and grants authority for the programme. Information protection, risk management, monitoring, and response are often the purview of the security organisation. It might also be in charge of enforcement, which includes reprimanding or even firing employees or contract workers. Physical security, disaster recovery and business continuity planning, regulatory and internal compliance, and auditing may be added to the list of duties. Yet, the security programme is what grants the organisation the right to take such measures.

**Framework**

An organization's security is governed by its security policy. Regarding what must be done to comply with the business needs, the framework specifies the policies and processes around the implementation and administration of information security measures. The security framework should specify rules and regulations. It is ideal to have a security framework established before beginning any implementations.

**Assessment**

An assessment helps you discover and implement important security controls in apps with the help of an assessment. Additionally, it emphasizes avoiding application security flaws and vulnerabilities.

**Planning**

This stage entails creating a plan that outlines the significant events and milestones that will occur throughout the course of the subsequent time period. One component of the planning stage is designing the security architecture and how systems are organised inside the design.

**Action**

Actions explain how procedures are carried out continuously by individuals to deliver the desired results of the security programme in a repeatable, dependable manner. The incident response plan specifies the steps that should be done when a security event happens. Planning beforehand for what to do in the event of a security problem reduces reaction time and offers repeatable, dependable, and efficient steps to contain an incident's scope and harm.

**Maintenance**

As part of a typical lifecycle of planning, updating, reviewing, and improving, maintenance and support are part of supporting the continuing operations of the security programme and its associated technology.

In order to ensure that the management's intentions are carried out by the many individuals accountable for the behaviour and activities outlined in the security rules, policy enforcement is also a component of maintenance. This enforcement frequently involves the cooperation of Human Resources, business management, and security management.

Strategy and Tactics

A security strategy is a comprehensive plan for defence, detection, and deterrence that defines all the architectural and policy elements that go into it. The daily routines of the people and tools tasked with protecting assets are known as security techniques. To put it another way, tactics are frequently reactive whereas plans are typically proactive. Both are equally crucial, and a successful security programme must combine tactical and strategic elements.

**1.2) Risk Analysis**

Risk mtigiation is the goal of a security programme. Mitigating risks does not mean eliminating them; it means reducing them to an acceptable level. You must plan for the different types of incidents that can happen in order to ensure that your security controls are successfully reducing the risks in your environment. Also, you must specify what you are attempting to defend and who from. Risk analysis, threat definition, and vulnerability analysis are used in this situation.

Let’s look at some of the terms and definition,

*Threats* include anything that poses a risk or can do so. Risk analysis includes evaluating threats as a key component. By identifying threats, you can focus your security strategy and lessen the possibility of missing crucial risk areas that might otherwise go unprotected. Threats can come in many different forms, so a security strategy must be thorough enough to handle the biggest ones if it is to be effective.

You must take into account all potential threats in order to prevent missing significant threat sources. Threats should be considered in light of the following factors:

• Threat vectors

• Threat sources and targets

• Types of attacks

Threat Vectors

A threat's origin and route to its target are both described by the term "threat vector." An illustration of a threat vector is an email sent from outside the company to an internal employee that has a tempting subject line and an executable attachment that is actually a Trojan programme that, if opened, will compromise the recipient's computer.

There are numerous threat vectors. For instance, viruses and Trojan horses infect computers connected to a reliable internal network. Trojan programmes are pieces of software that are secretly installed and use the privileges of authorised users to carry out tasks.

Threat Sources and Targets

Threats can come from a variety of sources and have a range of targets within an organisation. It might enter the company through its Internet-facing public face, or it might even be a nefarious insider looking to steal or discredit the company in question. Speaking of the targets, they could be an employee of the company or the servers that power it.

Attack Types

Attacks can be carried out manually by an attacker or automatically by malicious, mobile code that roams networks looking for exploit opportunities. In some cases, an attacker will use an automated programme to identify vulnerable hosts before manually attacking the targets. Attacks that involve entirely automated programmes are always the most effective in terms of the number of computers they compromise. Any computer that can be accessed via the Internet is also vulnerable to attack. Attackers and malicious software will continuously probe it in an effort to find vulnerabilities.

1.3) Compliance with Standards, Regulations, and Laws

Standards, Laws, and Regulations

The fourth layer of security management has been described as information security governance. Technical issues were addressed in the first layer, management issues were addressed in the second layer, organisational issues were addressed in the third layer, and governance issues were addressed in the fourth layer. Information security governance must be a concern for everyone involved in information security, including the board of directors, chief executive officers, information technology and information security professionals, and organisation employees.

Information security professionals must contend with developing technologies, crafty and determined cybercriminals, a complex threat environment, and heightened compliance demands resulting from fresh corporate governance initiatives. Even security professionals who work in unregulated settings are expected to adhere to a common set of standards, guidelines, laws, and rules, and it is essential that they comprehend them.

Standards for Information Security

Information security frameworks, also referred to as standards, are a collection of best practises that have been created by and approved by the information security industry as a whole.

The most well-known of these are

• Control Objectives for Information and related Technology (COBIT)

• International Organization for Standardization (ISO) 27001 and 27002

• National Institute of Standards and Technology (NIST) standards

COBIT

ISACA, the Information Systems Audit and Control Association, is the publisher of COBIT. ISACA is a well-known independent IT governance group, and many organisations use its COBIT guidelines to define and oversee processes based on maturity models like the Capability Maturity Model (CMM). COBIT is a general IT standard that incorporates some information security best practises, but it is not just about information security. Compared to the ISO 27000 series, COBIT contains a higher-level set of information security recommendations.

The COBIT procedures undergo regular updates, and new versions are released by ISACA. COBIT 4.1 is divided into four domains, which are conceptual areas. These four domains are expanded upon in COBIT 5, which also adds a fifth domain for governance. Versions 4 and 5's domains are as follows:

Governance:

• (v5) Evaluate, Direct, and Monitor (EDM)

Management:

• (v4.1) Plan and Organize (PO) and (v5) Align, Plan, and Organize (APO)

• (v4.1) Acquire and Implement (AI) and (v5) Build, Acquire, and Implement (BAI) • (v4.1) Deliver and Support (DS) and (v5) Deliver, Service, and Support (DSS)

• (v4.1) Monitor and Evaluate (ME) and (v5) Monitor, Evaluate, and Assess (MEA)

Key information security–related components of COBIT 4 (which are carried forward into version 5) include

• PO2.3 Establish an information classification scheme based on the criticality and confidentiality of data, and include ownership information, protection, retention, and destruction requirements.

• PO4.8 Establish an IT security and risk management function at a senior level of an organization’s management.

• PO6, PO7.4 Implement a security awareness program along with formal security training for employees, service providers, and third parties.

PO9 Perform risk assessment and management via a risk management program that analyzes and communicates risks and their potential impact on business processes.

• PO10.12 Ensure that security requirements are embedded into the project management process.

• AI2.4 Include security requirements in the application development process to ensure security and availability in line with the organization’s objectives.

• AI3.2, AI3.3 Implement security in the configuration, integration, and maintenance of hardware and software to provide availability and integrity.

• AI5.2 Ensure that third-party suppliers of IT infrastructure, facilities, hardware, software, and services comply with the organization’s security requirements, and this is reflected in any contracts with those third parties.

• AI7.1–AI7.9 Follow a well-defined change control process that includes testing, production migration, and backout planning.

• DS1.3, DS2.2 Include security requirements in Service Level Agreements (SLAs).

• DS4.1–DS4.10 Perform Business Continuity Planning (BCP) with periodic testing, and ensure that backups are preserved in a safe offsite location.

• DS5.1–DS5.11 Manage security according to a specific plan, perform identity management and user account management, perform security testing and monitoring, perform incident detection and response, implement security protections, employ cryptographic key management, protect against malicious software, secure the network, and protect data exchanges.

• DS12.1–DS12.5 Control physical security and access to important assets with access controls, escorts, and monitoring of activities.

ISO 27000 Series

The ISO 27000 series of information security standards provides a set of frameworks for developing a security program from concept to maturity. It is divided into several manageable parts; each part, like COBIT, prescribes a set of activities that belong to phases similar to those in the Plan-Do-Check-Act (PDCA) cycle.

• ISO 27001 is a high-level specification for the management of an information security program. This is referred to as an information security management system (ISMS). High-level statements about management duties like goal-setting, performance evaluation, and compliance auditing are found in the ISO 27001 standard. It includes instructions for conducting a risk assessment first to identify which controls are most crucial for each organisation and how thoroughly they should be implemented. This is conceptually related to the COBIT "Plan and Organize" idea or the "Plan" phase of the PDCA cycle. Audits can be performed in accordance with this standard (voluntarily, for organisations that aspire to a high level of maturity)

ISO 27002 is a detailed set of information security controls that would ideally be driven by the output of the risk assessment performed as part of ISO 27001. This standard serves as a comprehensive reference for all potential organisational actions. You can think of it as a collection of best practises, and it's up to each organisation to choose which ones apply to their particular industry. This can be compared to the "Acquire and Implement" principle of COBIT or the "Do" phase of the PDCA cycle.

ISO 27003 is intended to offer suggestions and best practises for putting into practise the ISMS management controls outlined in ISO 27001, or how to deliver the security programme. This can be compared to the PDCA cycle's "Check" phase or the COBIT concept of "Deliver and Support."

ISO 27004 covers measuring the effectiveness of the ISMS put in place by the first three ISO 27000 standards using metrics and key performance indicators. This information is used to assess how well the information security controls are performing. This can be compared to the "Adjust" phase of the PDCA cycle or the "Monitor and Evaluate" concept of COBIT.

ISO 27005 defines a risk management framework for information security that can be used to inform the decisions within ISO 27001 that lead to selection of controls for ISO 27002.

• ISO 27006 is a standard that provides guidelines for professional organizations that provide certification to be properly accredited.

Some significant examples from ISO 27002 that most organisations would probably find interesting include

• 4.1, 4.2 Establish a formal risk management program to assess and treat risks to the organization’s assets.

• 5.1 Publish an information security policy that reflects senior management’s expectations with regard to security, and make sure it is available to all stakeholders.

• 6.1 Establish an internal security organization with appropriate, well-defined responsibilities and relationships with third parties.

• 6.2 Use confidentiality agreements to protect information when working with third parties, to protect access to confidential information.

• 7.1 Identify and document assets, assign ownership, classify according to criticality, and establish an acceptable use policy.

• 7.2 Establish an information classification scheme that includes labeling and handling guidance.

• 8.1–8.3 Perform background checks on employment candidates, communicate security responsibilities to all employees, provide information security awareness and training, and ensure that the correct security behaviors are enforced through a disciplinary process.

• 9.1, 9.2 Establish physical security controls, including perimeters, access controls, separation of critical areas, and protection of equipment.

• 10.1 Establish a change control process along with separation of duties to separate development and production environments and activities.

• 10.2 Manage third-party service delivery.

• 10.3 Perform capacity planning and resource monitoring for proactive allocation of resources.

• 10.4 Protect against malware.

• 10.5 Establish reliable backups.

• 10.6 Establish network security controls.

• 10.7 Manage the handling and disposal of data and the media it resides on, and transport data securely so it can’t be intercepted.

• 10.9 Protect online systems, data, and transactions and maintain accurate audit logs to identify issues.

• 11.2–11.6 Manage user access rights to control access to data.

• 12.2 Make sure that applications are correctly processing information and that they check their inputs to avoid misuse, and use encryption to protect that information.

• 12.5 Manage source code development and access, and use a formal change control process to promote code from development into the production environment.

• 12.6 Establish a vulnerability management program.

• 13.1, 13.2 Establish an incident response program.

• 14.1 Perform business continuity management, including regular testing.

• 15.1–15.3 Establish a compliance management program to comply with all legal and regulatory requirements. Perform audits to ensure compliance.

NIST

The National Institute of Standards and Technology (NIST) provides a set of “Special Publications” to assist industry, government, and academic organizations with following best practices.

With the exception of 800-53, the group of security-specific publications known as the "800 series" is very specific to individual technologies.To specify security control organisation and structure, security control baselines, common controls, security controls in external environments, security control assurance, risk management, information system categorization, security control selection, and monitoring of security controls, 800-53 was created primarily for the U.S. Federal Government.

800-53 is organized into 18 “security control families,” which are conceptual categories that represent important components of a complete security program.

1. Access Control

2. Awareness and Training

3. Audit and Accountability

4. Security Assessment and Authorization

5. Configuration Management

6. Contingency Planning

7. Identification and Authentication

8. Incident Response

9. Maintenance

10. Media Protection

11. Physical and Environmental Protection

12. Planning

13. Personnel Security

14. Risk Assessment

15. System and Services Acquisition

16. System and Communications Protection

17. System and Information Integrity

18. Program Management

Each remaining 800 series publication provides guidance on specific subject areas such as WLANs, public cloud, VPNs etc.

Regulations that affect Information Security Professionals

There are other regulations and standards that apply to specific kinds of information and technologies such as HIPAA that provides guidance on different areas such as protection, securing etc.

Health Insurance Portability and Accountability Act (HIPAA) and companion HITECH Act Applies to the healthcare sector, regarding the protection of patient information

Sarbanes-Oxley Act of 2002, Section 404 also known as SOX , applies to all publicly traded companies to guarantee data integrity against financial fraud

Gramm-Leach-Bliley Act (GLBA) Applies to the financial sector, including banks and lenders, for the protection of customer and financial information

Payment Card Industry (PCI) Data Security Standard (DSS) Applies to any organization that processes, transmits, or stores credit card information

The Need to Care

Information technology strategy is heavily influenced by information security regulations and the risk of liability that comes with not meeting industry standards for anticipating, preventing, and responding to security breaches. The majority of these new federal and state regulations are focused on protecting electronically stored, personally identifiable information, and they typically only apply to specific business sectors. The regulations lay the groundwork for accountability and liability for organisations that don't implement the necessary safeguards. An emerging duty of care for any entity that obtains or maintains personally identifiable information electronically has been created as a result of the cumulative impact of security breaches. A discussion of the existing regulations provides some shape and contour to the measures that organizations should now consider essential to secure their systems.

The Need for Laws that affect Information Security Professionals

Information security professionals need to be familiar with the components of the various computer crimes listed in state and federal statutes. This is not only because it enables information security professionals to lessen their organisations' liability for actions taken by their own employees, but also because it helps them protect their organisations' data, products, and communications from outside threats.

It assists in determining whether to alert other members of the organisation to a particular act. The likelihood of information security staff raising an alarm in response to unactionable events significantly decreases when they are aware of the essential characteristics of criminal behaviour.

Information security experts can use it to set up their businesses to make reliable criminal referrals (or to build solid civil cases). Computer crime laws are a bit special in that they place a lot of responsibility on the victim to take actions to prove that a cybercrime was committed, such as defining access permissions and documenting damage. Information security professionals can design their network defence posture and gather and document crucial evidence when responding to incidents by being aware of this responsibility. The majority of the time, information security managers will take the initiative to draught the information security policies for their organisations, and those policies can include recognition of the main components of computer crime.

It will help to prevent overly forceful responses to incidents that could make a system administrator liable.

1.3) Secure Design Principles

Security Models

Let’s compare some of the security models that were proposed previously and still have a significant place in the world of information security.

CIA triad -- Confidentiality, Integrity, and Availability is a venerable, well-established conceptual model that deals with the most important aspects of information protection. Security experts are well aware that information security is not just about information and that the CIA only concentrates on three aspects of information protection. Even though the model isn't perfect, it's still beneficial to be aware of it.

Confidentiality

Confidentiality refers to the restriction of access to data only to those who are authorized to use it. Generally speaking, this denotes that a particular set of data is only visible to one or more authorised users or systems. For instance, a password is private because it should only be known by one person, whereas a patient record is confidential because it can be accessed by several members of the patient's medical team.

Integrity

Integrity is the guarantee that the data has not been changed without authorization. It means that unauthorised parties shouldn't change, alter, or even completely delete the data.

Availability

It is the guarantee that a specific service, like network, storage, or compute, is always accessible when required. Implementing high-availability (or continuous-service) controls on computers, networks, and storage is typically done to protect service availability.

The Onion Model

Onion model is a defense security model which is a layered strategy that considers “security” as layered approach where the attacker has to break his way layer by layer just like how a onion is peeled away layer by layer. The better the protection against a failure of any one of those layers, the more layers of controls there are. The layered security approach can be used at any level where security controls are installed. It not only makes it harder for an attacker to get past the defences, but it also lowers the possibility of an unintended failure of a single technology. It is possible to layer authentication controls for systems, networks, and applications.

Zones of Trust

Different parts of a network have varying levels of mutual trust. Some regions, or what we refer to as "zones," have completely trustworthy services and communication, while others do not. Zones of trust are a term used to describe how trustworthy a network or computer system is. You can start dividing those functions into zones of trust once you have determined the risks and threats to your company and the necessary functions. You must do this by putting different levels of trust on each group of network resources. Zones of trust are interconnected, and as business needs change, communication between various dissimilar networks, systems, and other network entities is necessary. You can start to develop a plan for containing those systems into zones once you have an understanding of how systems on the network must communicate with one another. Certain areas enjoy greater levels of trust than others, and different areas have varying degrees of mutual respect. A crucial first step in minimising the vulnerabilities that could jeopardise a security implementation is to list these areas.

Separating the resources into zones of trust enables you to vary the levels of security for these resources according to their individual security needs. A more trusted resource can be shielded from attack by a less trusted one by using multiple zones, which allows access between two zones to be controlled.

Each zone (aside from perhaps a "untrusted" zone) requires that the devices in it have a specific, equivalent level of security; this level of security is determined by the technologies and procedures that are in place to check for attacks, intrusions, and security policy violations. This level of security is required to establish a minimum level of trust.

To keep trust zones apart from one another, network access control devices and technologies such as firewalls, routers, virtual LANs (VLANs), and others can be used (as the walls in the castle analogy did). Based on the authorization rules specified in the security architecture, access control lists (ACLs) and firewall rules can be used to regulate communication between these levels.

The perspective of a transaction can also be used to view trust. Several systems may communicate with one another during a specific transaction through different zones of trust. In a transaction-level trust model, systems can be classified into functional groups according to the kinds of transactions they handle rather than being divided into different trust zones based on where they are on the network.

Even though a transaction may cross multiple network boundaries, all systems involved in it must have equal trust in one another. As a result, security measures at the system and network levels should permit each of these systems to carry out the tasks for which they have been authorised while preventing access to these resources by systems not involved in the transaction.

Some network defense best practices

Physically securing the devices

PCs and laptops may need to be physically fastened to their desks depending on your environment. Lockdown devices come in a variety of forms, from thin rubber-coated wire lanyards to hardened metal jackets specifically designed to enclose a PC. Someone should secure their laptop if they plan to leave it on their desk over night.

UEFI/BIOS password protection

Since the CMOS/BIOS settings of a computer contain many potentially secure settings, such as boot order, remote wake-up, and antivirus boot-sector protection, the majority of CMOS/BIOSs allow you to set up a password to prevent unauthorised changes. It's best if the password is different from other administrative passwords. This is especially important for portable computers, such as laptops and smartphones. The most likely targets for theft are personal computers with small form factors. On a tablet or smartphone, resetting the boot-up password frequently necessitates erasing the data as well, guaranteeing confidentiality and privacy.

Disable booting from optical and USB drives

By preventing boot viruses from USB storage devices and optical drives, as well as attackers from installing a different operating system on the computer, operating system security can be bypassed.

Boost operating system security

Always ensure that the operating system is hardened by taking precautions such as allowing the installation of only secure software, patching and updating the system frequently, configuring the settings securely, limiting the number of administrators and their privileges, and bolstering the authentication processes.

Antimalware programs should be used.

Anti-malware programs are crucial in the modern world. It ought to be installed on desktop computers with compelled automatic updates and enabled for real-time security.

Firewalls are essential.

Firewalls are capable of performing a wide range of security tasks, from straightforward port filtering to stateful inspection systems that can analyse threats occurring anywhere in layers three through seven with computer-based software.

Desktop firewall software, also referred to as host-based firewalls or personal firewall software, is used to protect individual PCs from external and internal threats. It typically has the added benefit of preventing unauthorised software programmes, like Trojans, from initiating outbound traffic.

Secure Network Share Permissions

A network share (like NetBIOS or SMB) with no password or a weak password is one of the most popular ways an attacker or worm gains access to a system. The principle of least privilege should be used to apply discretionary ACLs (DACLs) to folders and files that can be accessed remotely over a network, and strong passwords should be used.

Use encryption

Every opportunity should be taken to use encryption. SSH should be used by Linux and Unix administrators to manage their computers instead of Telnet or FTP. If you must use FTP, think about using an FTP service that encrypts traffic using SSL and digital certificates. Both the client and the server must support the same encryption mechanism for encrypted FTP to function. Windows includes the Encrypting File System (EFS) feature. It instantly encrypts and decrypts password-protected files and folders. EFS will automatically create public/private encryption key pairs for the user and the recovery agent once it has been activated by a user. Every encryption and decryption operation is carried out silently in the background. Unauthorized users will not be allowed access to files that are protected by EFS. In some cases, such as when a worm attack is rampantly corrupting every data file it can find on a file server, this could stop malicious activity (like the VBS.Newlove worm does). While the authorised user is logged in, EFS won't stop malware occurrences because it encrypts and decrypts data on the fly.

Securely Configure Applications

Applications should be set up with the recommended security settings from the vendors. However, in end-user PC environments, you want to maintain the applications while reducing the risk. To achieve this, make sure security settings are set at the vendor's suggested levels, if not higher, and apply security patches on a regular basis.

Blocking Dangerous File Types

Given that sending viruses and worms via e-mail is currently the preferred method for doing so, the best way to prevent exploits is to block dangerous file attachments. It is possible to block harmful file extensions at the Internet gateway device, email server, or email client. A plethora of commercial and open source programs exist to block file attachments at the gateway and e-mail server level. Additionally, the majority of antivirus suppliers provide an email server antivirus solution.

Lock Down Applications

The ability of an end user to install and run any software they desire poses one of the biggest risks to any environment. There are numerous tools available to restrict what a desktop user can and cannot run. In Windows, an administrator could set system policies to severely restrict the desktop, disable the user's Run command, and prevent the installation of new applications. Administrators can specify what software is permitted to run on a specific computer using Windows' Software Restriction Policies feature.

Secure P2P Services

Music sharing and other peer-to-peer (P2P) applications are likely to continue to be popular targets for attacks in the future. This is due to the fact that P2P applications frequently get installed in the corporate environment without the administrator's permission and have very little security, if any. Additionally, they are built to access files on the computer of the end user, which makes it much simpler to steal those files.

First, get rid of P2P if it isn't permitted in your corporate environment. Start by educating end users and establishing sanctions for unapproved software with management. Then locate the programmes and uninstall them. Finding them requires checking firewall logs for known P2P port attempts, sniffing P2P packets with an IDS on the local network, or using P2P auditing software.

Second, confirm that your firewall is set up to specifically block P2P traffic. It can be challenging to block P2P traffic by port number alone because P2P software frequently uses port 80 as a proxy port, but there are steps you can take. Block the destination at the firewall if P2P clients connect to servers with a specific IP address or in a specific domain. Some firewalls permit the use of wildcards in domain names that are blocked, such as \*irc\* or \*kaz\*. Last, if your end users insist on using P2P, and it is authorized by management, insist on a more secure P2P application, if at all possible.

Make Sure Developers Code Securely

SQL injection and buffer-overflow attacks can only be defeated by programmers using secure coding practices. Using double quotation marks in place of single quotes can help prevent SQL injection attacks. Input validation is necessary to prevent buffer-overflow attacks. If the programmer makes the application well-designed and secure, other attacks of this nature could be easily avoided.

Back up the system

The most frequent sign of malware damage is frequently altered, corrupted, or deleted files. Viruses and worms frequently destroy files, reformat hard drives, or purposely corrupt data. Malware can maliciously modify a system even if it doesn't intentionally alter any files on the host system. Security professionals sometimes are unable to undo the harm and restore the system to its pre-exploit state. Therefore, it's critical to maintain frequent, verified system backups.

. At the very least, all of your data files should be included in the backup, and a full system backup ensures a speedier recovery in the event of a serious exploit event. Additionally, you need to confirm that your backups weren't contaminated by the malware.

Implement ARP Poisoning Defenses

One of the most frequent and potent threats to network infrastructures is ARP poisoning attacks (especially wireless networks). They are a type of man-in-the-middle attack (MITM) that enables an attacker to covertly intercept and change network traffic. Therefore, these attacks require unique defences of their own. An organisation can protect itself from an ARP poisoning attack in a few different ways. Static ARP tables, port rate limiting, or DHCP snooping with dynamic ARP inspection are a few examples of defences (DAI). A mix of the latter two strategies is the best form of defence.

Configure Port Rate Limiting

Port Rate Limiting (PRL) restricts and tracks the volume of traffic that can pass through a port in a given period of time. When the configured threshold is tripped, the port automatically closes until it is manually enabled or until a predetermined amount of time has passed (usually 15 minutes).

It is simple to understand why PRL is a respectable line of defence when considering how an MITM attack with ARP poisoning operates. As previously mentioned, ARP poisoning operates by routing the victim system(s)' traffic through the attacker's tool. If an attack is launched against a port that has PRL, the volume of traffic should be sufficient to exceed the threshold and shut the port down. You have essentially prevented an attacker from performing ARP poisoning from that port if you make the port inaccessible to them.

If enabling the port requires manual intervention, this may serve as a warning to the organisation, especially if it occurs on several ports at once.

Use Dynamic ARP Inspection and DHCP Snooping

DHCP snooping combined with dynamic ARP inspection is the most efficient way to combat ARP poisoning (DAI). This defence is based on the fact that it discards any ARP reply requests that are not in its table. Similar to PRL, this defence necessitates some environment research on the part of the organisation before full implementation can take place. For two to three weeks, the organisation must run DHCP snooping in order to properly compile a table of IP addresses and MAC addresses. Once that table has been created, DAI can be used. DAI offers a strong defence against ARP poisoning attacks once it is implemented.

1.4) Security Policies, Standards, Procedures, and Guidelines

The four components of security documentation are policies, standards, procedures, and guidelines. Together, these form the complete definition of a mature security program.

Security Policy

A security policy is a document that outlines the security requirements of an organisation. A security policy outlines what must be done, not how to do it, and it doesn't name any particular tools or fixes. The security policy outlines a specific set of goals and requirements that will help safeguard an organization's resources and operational efficiency.

It serves as the fundamental framework for an efficient and thorough security programme. A strong security policy should be a high-level, succinct, formalised declaration of the security procedures that management anticipates staff members and other stakeholders will adhere to. A security policy should be succinct and simple to comprehend so that everyone can adhere to the instructions provided in it.

A security policy outlines clear guidelines for management, technical staff, and staff members. What an organisation does in response to a security violation will depend on its explicit and well-documented security policy. Organizations put themselves at risk and frequently struggle to respond to a violation when there is no clear policy in place.

For managers, a security policy outlines the senior management's expectations regarding the roles, responsibilities, and actions that management should take in relation to security controls.

• For technical staff, a security policy specifies which security measures should be applied to computer systems, physical infrastructure, and networks.

For all employees, a security policy describes how they should conduct themselves when using the computer systems, e-mail, phones, and voice mail

The security practitioner is given a road map for efficient, reliable policy production by using a top-down approach to security policy development. The person creating the policy must take the time to comprehend the regulatory environment, corporate goals, and risk management issues, as well as the general policy statements of the organization.

Security Policy Development

When developing a security policy for the first time, one useful approach is to focus on the why, who, where, and what during the policy development process: 1. Why should the policy address these particular concerns? (Purpose)

2. Who should the policy address? (Responsibilities)

3. Where should the policy be applied? (Scope)

4. What should the policy contain? (Content)

Security policy must be developed in the following phases,

1. Requirements gathering

• Regulatory requirements (industry specific)

• Advisory requirements (best practices)

• Informative requirements (organization specific)

2. Project definition and proposal based on requirements

3. Policy development

4. Review and approval

5. Publication and distribution

6. Ongoing maintenance (and revision)

To ensure a smooth implementation after the security policy has been approved, standards and procedures must be created.

Security Policy Contributors

The following contributor groups may be represented in a security policy:

• Human resources - When it comes to employee rewards and punishments, the HR department is typically in charge of enforcing the security policy. When the company's policies are broken, HR imposes sanctions, up to and including termination. Additionally, HR gets a signature from each employee confirming that they have read and comprehend the organization's policies, so there is no doubt about who is to blame when employees don't follow the rules.

Legal - A company with an internal legal department or outside legal counsel will frequently want to have those lawyers review and explain any legal points in the document and offer advice on specific matters of appropriateness and applicability, both in the organization's home country and abroad. When their policies are applied to specific employees, all organisations are advised to have some sort of legal review and advice.

Information Technology - Computer systems, and more specifically the security safeguards integrated into the computing infrastructure, are frequently the focus of security policy. The biggest users of the policy information are typically IT staff.

Physical Security - The physical security controls listed in the security policy are typically implemented by physical security (or facilities) departments. In some circumstances, the physical security system's information systems components may be managed by the IT department.

Security Policy Audience

The intended audience for the security policies is all the individuals who handle the organization’s information, such as:

• Employees

• Contractors and temporary workers

• Consultants, system integrators, and service providers

• Business partners and third-party vendors

• Employees of subsidiaries and affiliates

• Customers who use the organization’s information resources

Policy Categories

Three main categories can be used to further divide security policies:

Regulatory - It is helpful to include this particular category for audit and compliance purposes. Typically, the policy is filled with a number of legal declarations that explain what is required and why it is required. It is possible to include the findings of a regulatory requirements assessment in this kind of policy.

Advisory - This type of policy informs all parties who may be impacted of business-specific rules, which may include rules pertaining to computer systems and networks, people, and physical security. Typically, this kind of policy is based on security best practises.

Informative - To ensure that policies not covered under Regulatory and Advisory are taken into account, this kind of policy is available as a catch-all. Specific business units, business partners, vendors, and clients who use the organization's information systems may be subject to these policies.

The security policy should be concise and easy to read, in order to be effective. It should consist of a few straightforward declarations of the intentions of senior management.

The following elements can be used as an outline to represent the structure and organisation of security policies:

• Author The policy writer

• Sponsor The Executive champion

• Authorizer The Executive signer with ultimate authority

• Effective date When the policy is effective; generally when authorized

• Review date Subject to agreement by all parties; annually at least

• Purpose Why the policy exists; regulatory, advisory, or informative

• Scope Who the policy affects and where the policy is applied

• Policy What the policy is about

• Exceptions Who or what is not covered by the policy

• Enforcement How the policy will be enforced, and consequences for not following it

• Definitions Terms the reader may need to know

• References Links to other related policies and corporate documents

Additional Security Frameworks and Laws

There are numerous security frameworks that work well with specific information technology components.

For instance, the HIPAA act clearly outlines how PHI (Personal Health Information) and other patient health-related data should be handled, transmitted, protected, and stored.

Therefore, it would be more beneficial if we took into account other similar frameworks when developing a security policy.

An organisation or a business entity may need to abide by a number of laws. Therefore, it is crucial to develop a security policy that complies with these laws and rules. The security policy's author and contributors must make sure that it complies with all applicable laws and regulations.

Security Awareness

Frequently, trusted internal staff members who have been given access to internal resources serve as the first line of defence against an organization's assets. The human element is, as with most things, the least predictable and most vulnerable to abuse. Trusted workers are either deceived or corrupted into unintentionally divulging useful information that helps burglars. Employees are the weakest link in any security chain because of the high level of trust that is placed in them.

Education is one of the best ways to stop employees from disclosing information, according to research. Employees are less likely to unintentionally assist an attacker in information gathering when they understand why they shouldn't disclose private information, are aware of the reasons why, and are aware that they will be held accountable. Social engineering and information leakage threats are lessened by education and training.

Importance of security awareness

Even the most meticulously designed security infrastructure is frequently compromised by employees either intentionally or unintentionally. This is due to the fact that in order to perform their duties, they are given trusted access to information resources through firewalls, access control mechanisms, structures, phone systems, and other private resources. End users have access to the system accounts and passwords required to copy, modify, delete, and print confidential information as well as alter its integrity level and prevent access by authorised users. Most organisations have common practises that put the information security programme at risk, including propping open doors, disclosing account and password information, and throwing away sensitive documents. A security awareness programme aims to change and stop these behaviours as well. Employees who are well-versed in security principles and practises can contain the damage a security breach causes quickly.

Implementing the Awareness Program

Once staff members are aware of security issues, they can start considering how to carry out their duties in accordance with the security policy and how to respond to security-related events and incidents. Following security policy and incident response typical topics include

- What to do about unauthorised or suspicious activity. How to report potential security events, including who should be notified, what to do during and after an incident, the timeframe for such reporting, and what to do about those events. When an employee is acting suspiciously, a computer system is being attacked, or email could be intercepted by an intruder, it may be necessary to communicate verbally rather than via email. These are just a few examples.

- Securing the use of information technology systems.

- How to handle email attachments, create and manage passwords, and transfer and download files securely.

The awareness campaign should make it clear that management places a high priority on security. It should be made clear that everyone in the company, from executive management to every employee, is accountable for security procedures. When executives set an example and employees can see that security procedures are important to the company rather than just another initiative, they will be more likely to take them seriously.

Enforcement

Perhaps the most crucial element of network security is enforcement. If policies, procedures, and security technologies are disregarded or used improperly, they will not function. Enforcing the security policy guarantees adherence to the values and procedures that the security infrastructure's designers intended.

There are numerous ways to enforce. Enforcement gives general employees the confidence that daily work activities adhere to the security policy. Enforcement ensures proper maintenance procedures are taken by system administrators and other privileged staff members and prevents abuse of the increased level of trust accorded to this group of employees. For managers, enforcement reduces the likelihood of conflicts of interest caused when managers give their employees orders that are against policy and prevents overriding of the security practices intended by the policy's authors.

Enforcement discourages people from inadvertently, deliberately, or casually breaking the law. Normally, Human Resources is directly responsible for enforcing the corporate security policy for employees and temporary workers. For egregious security policy violations, HR implements punitive measures, up to and including termination, and also makes an effort to change behaviour through warnings and evaluations. HR may also use financial incentives and other forms of positive reinforcement, such as bonuses. The same standards of policy enforcement should be applied to every employee, without exception. When enforcing policy, it is crucial to avoid prejudice or distinction between employees. In management, this is especially true. Senior managers and corporate executives, in particular, ought to be held to the same standards of accountability as regular employees, if not higher. Senior management ought to be a role model for ethical conduct for the rest of the company and maybe even held to a higher standard than those who report to them.

Software can occasionally be used to enforce policy compliance and stop behaviours that are against the rules. Controls for web browsing like website blockers are one illustration of this. Each time a user tries to access a website, these programmes consult a list of websites that are forbidden. The attempt is blocked if it is made to access one of the forbidden websites. The benefit of software-based enforcement is that staff members are physically unable to break the law. The operating system's Group Policy settings are among the others. This implies that, despite their best efforts, no one will be able to violate the policy. As a result, the organisation is guaranteed complete policy compliance. Software enforcement is the easiest and most reliable method of ensuring compliance with security policy.

The corporate security policy and acceptable use policy should be thoroughly documented, communicated to employees, and signed by them to show that they have read, understood, and agree to the terms, regardless of the corporate culture or how software-based enforcement is used in the organisation to control behaviour and promote compliance. Software-based enforcement should only be one step in a chain of enforcement techniques that includes other levels, including termination, when it is used.

For this reason, businesses shouldn't just rely on software; they also need levels of deterrence that are understood by all employees. Employees should be aware that they may lose their jobs if they act in ways that go against the employer's ethics or principles because employment is typically an at-will relationship between the employer and the employee. Instead of using software as an escape or a way to avoid the challenges and hardships of enforcement, use it to help the organisation reach its enforcement objectives.

Security Standards

A policy is less specific than a standard. Standards should be regarded as obligatory because they provide instructions on how to adhere to the policy and because they are connected to policies. Standards define specific technology settings, platforms, or behaviours and are the extension of policy into the real world. Typically, security managers who are in charge of the IT infrastructure spend more time writing standards than they do policy. Compared to policy, which anyone should be able to understand regardless of level of expertise, security standards are much more detailed.

Security Procedures

Security procedures are detailed instructions on how to carry out a particular task. The level of specificity is higher in security procedures than it is in policies and standards. A system administrator would follow the procedure while seated at the keyboard of the computer that is being built. This information is very specialised and only intended for system administrators, so the majority of people won't understand it. A security procedure will typically contain specialised information that is highly job-specific.

Security Guidelines

Guidelines provide guidance. They are only recommendations on how to abide by the policy; they are not requirements. The purpose of guidelines is to help people understand how to achieve the objectives set forth in the security policy, which should make life easier for both the end user and the security manager who wrote the policy.

Ongoing Maintenance

The security guidelines, policies, and standards are ever-evolving documents. They are not written once and then left unchanged for years, in other words. In response to evolving business conditions, technologies, customer requirements, etc., these documents should be updated on a regular basis. To manage this lifecycle process, some kind of document version control technology may be useful.

Finalizing the Implementation with Audits

An audit may be carried out by external organisations or internal divisions once the security policies, standards, procedures, and guidelines are in place, well-established, and in a position to direct day-to-day operations. An audit contrasts current procedures with the goals of the policy. A disinterested party (not the security organisation or the IT department) must conduct the audit in order to identify weaknesses or issues with the policy and its enforcement. This requires having an unbiased third-party perspective. Any frequency—monthly, quarterly, yearly, or at another interval—can be used for audits. Audits of security policy compliance should be performed at least once a year because longer time frames could allow for significant differences between the operations and the policy.

Part Two

Data Security

Information security professionals' first and foremost responsibility is to secure the data. Therefore, it's crucial to establish policies, adhere to processes, and practise some discipline when it comes to data security.

Difference between Structured and Unstructured Data

Data that complies with a rigid data model is said to be structured data. The majority of IT and security experts define structured data as data that is stored in a database and is arranged according to the database schema and any corresponding database rules. The structure of the data itself typically makes it possible to classify it quickly. For instance, you could locate a person's medical history in a database and implement security measures in line with that discovery. You have complete control over who can access structured data. Structured data can be easily defined and applied security controls using either the structure's inherent features or third-party tools created for that particular structure.

Unstructured data is much harder to secure and manage. Unstructured data is mobile across all networks, can exist anywhere, and can take any form. Think about a patient record being pulled from the database, displayed in a web page, copied into a spreadsheet, attached to an email, and then sent to a different address. There is no set format for unstructured data. The original structure of the data has been changed as it moves between formats.  
The key areas where unstructured data can reside can be broken down into the following categories:

• Databases

• Applications

• Networks

• Computers

• Storage

• Physical world (printed documents)

Databases

The hub of the data universe is the database. The majority of the data you are attempting to protect either exists in, was created and inserted into, or was retrieved from a database. You must protect the database's data while allowing authorised users and applications to access it for practical reasons. Databases were previously only used to store structured data, but new advancements in database technology have led to an increase in the amount of unstructured data being stored in databases. For instance, a content management system or application that stores pictures, videos, and other unstructured data can use a database as its storage component.

Encrypting Unstructured Data at Rest in the Database

Encryption is the most popular method for protecting the data in a database. There are several methods for encrypting data that is stored in a database:

• Encryption of the data itself, allowing it to be kept in an encrypted state in regular data files. The encrypted data is passed to the application to decrypt because the database may not be aware of (or care about) whether or how the data is encrypted.

• Partial encryption of the database schema, whereby only particular rows, columns, or records are encrypted depending on where the data will be stored. In this instance, the database manages data encryption and provides the application with the decrypted data.

• Full encryption of the database data files, ensuring that all data contained therein is encrypted.

Database exports and backups may be protected without additional technology depending on the type of encryption used. Data masking technologies are frequently used to declassify data that must be used in development environments. These technologies scramble or randomise real data to create fake information that retains many of the same properties as the original data.

Implementing Controls to Restrict Access to Unstructured Data

Restricting access to data is largely accomplished through database access controls. The strategies employed by various databases range from simple username and password authentication to a complex set of rules that specify who is permitted to access what from where, when, and with what application for various levels of data classification.

The credentials that are used to authenticate and grant access to data can either be kept on the database platform itself or in a separate identity directory. This makes it possible to link data security to the enterprise directory store, making it simpler to manage the access control model by utilizing the already-existing access control infrastructure.

The trust that the process that is permitted to access the data is legitimate or that the data remains secure after it leaves the database still underlies all the work put into configuring controls to restrict access to the database.

Securing Data Exports

The ability to bulk export data into other databases is a feature offered by many databases. There are security issues as a result. Encryption can be used at the export stage to solve this issue. This mechanism typically differs from those used for system-wide database backups or the encryption of data in the schema. It is typically possible to provide a passphrase when exporting data, which will be used as the key for the export's one-time encryption. Because the encrypted export and passphrase are shared separately when given to the user importing the data into their own system, this enables sets of data to be protected in transit.

Keeping Database Storage Secure

Databases and storage have a lot in common. Security of the storage becomes just as crucial as security of the databases. Although storage security solutions primarily deal with data at rest, sometimes stored data is also in use or in transit. The contents of a PDF file, which the operating system pages to the disc and stores in RAM as an illustration, are an example of this.

Storage Encryption

Encrypting these locations is an obvious solution because data in databases, network storage, content management systems, and computers ultimately end up being stored on storage gadgets like hard disc arrays or USB flash memory. There are two types of encryption techniques for storage devices:

• Hardware-based or software-based disc encryption

• File-system encryption

Hardware-based/software-based disk encryption

Disk encryption is the process of encrypting the disk(s) and its contents using software or hardware in a way that is transparent to the operating system, the application, or the content format. Before any data on the drive can be decrypted and read, some type of authentication must occur.

File-System Encryption

When data is encrypted at the file system level, it is said to be file system encryption. This implies that the approaches could change based on the operating system being used. The primary distinction between file and folder encryption and metadata encryption is that the former only secures files and folders. In other words, without the cryptographic keys, an unauthorised person can list the files, view their names, and determine who owns them. However, they cannot actually access the files. Like disc encryption, file-system encryption only takes effect when the content is stored in an encrypted location. The data is no longer secure if it is transferred from the encrypted disc to an unencrypted disc.

Data Loss Prevention (DLP)

Data loss prevention (DLP) is the name given to a group of relatively recent technologies used to track, find, and safeguard data. Three categories of DLP technologies exist.

• Network DLP - Typically a network appliance serving as a bridge between significant network perimeters (most commonly between your corporate network and the Internet). Network DLP keeps an eye on the traffic that enters the gateway in an effort to spot sensitive information and take appropriate action, usually blocking it from leaving the network.

• Storage DLP: Software that performs the same tasks as network DLP, running either on an appliance or directly on the file server. Searching for sensitive data, storage DLP scans storage systems. Once discovered, it has the ability to remove it, place it in quarantine, or simply alert the administrator.

• Endpoint DLP- Endpoint systems run software that keeps track of operating system and application activity, keeps an eye on memory usage, and scans network traffic for the unauthorised use of sensitive data.

Information Rights Management (IRM)

Regardless of where data files are stored, transmitted, or used, information rights management (IRM), a relatively new technology, incorporates protection right into the data files. To permit authorised users to open files and to block unauthorised users, IRM uses a combination of encryption and access controls. IRM encrypts files using advanced encryption methods. Software is needed to check with a central authentication server (typically located somewhere on the Internet) and determine whether the requesting user is authorised to unlock the data when a request is made to open, copy, modify, or decrypt the file and the data.

Security risks related to storage

Malfunctions

Data integrity is harmed by computer and storage malfunctions that corrupt data. Make sure the storage infrastructure you choose has appropriate RAID redundancy built in and that important data archives are part of the service to avoid malfunctions. You can also use integrity checking software that verifies data using checksums or other methods.

Data Deletion and Data Loss

Due to malfunctions in computer systems or improper handling, data can be destroyed on purpose or accidentally. Financial, organisational, individual, and audit trail data are some examples of this type of data. If such important data can't be recovered, it's lost forever once it's lost. To prevent data deletion and data loss,

• Make sure your critical data is redundantly stored and housed in multiple locations to prevent data loss and deletion.

• Keep track of and analyse audit logs for data deletion.

• Continue to offer programmes that educate and inform those who access and manage data. Make sure to assign data owners who will be in charge of the data, bear responsibility for its loss, and have authority over it.

Data Corruption and Data Tampering

Data that is invalid or damaged can have serious consequences because valid, trustworthy data is the basis of every computing system. The integrity of data can be harmed by alterations brought on by faulty computer or storage systems, malicious individuals, or malware. A person who alters data with the intention of defrauding another party can harm integrity. To avoid data tampering and corruption,

• Maintain archive copies of important data before it is modified by using version control software. Make sure antivirus software is protecting all data. Maintain least privilege, role-based access control over all data in accordance with job function and need to know.

• Use integrity-checking software to track and notify changes to important data.

• Continue to offer programmes that educate and inform those who access and manage data. Make sure to assign data owners who will be in charge of the data, bear responsibility for its loss, and have authority over it.

Denial of Service (DoS) attacks

A denial of service (DoS) attack or distributed denial of service (DDoS) attack aims to prevent the intended users from accessing a computer resource. This type of attack typically entails overwhelming the target machine with too many communications requests, rendering it ineffectively unavailable or unable to respond to legitimate traffic. The majority of DoS and DDoS attacks use compromised systems all over the world, making them difficult to track and vulnerable to defences because they flood system and network resources. To prevent DoS attacks,

• Pick a storage platform with strong defences against network intrusions. At the storage network's edge, install firewalls, an IPS, and network filtering to prevent attacks.

• Always keep an eye on intrusion detection systems.

• Collaborate with your legal team to find and bring charges against the attackers.

Outage

Any unplanned downtime or unavailability of a computer system or network is referred to as an outage. Storage infrastructures may be unavailable for as long as it takes to switch to the disaster recovery environment because unexpected outages can happen even when every device and network path is fully redundant.

• Redundancy is the main safeguard against any service interruption. Make sure that each system, piece of hardware, and network link is clustered or configured to use high availability. Calculate the cost of downtime and use that figure to support investing in the extra equipment required for redundancy. Use a reliable disaster recovery plan as well to make sure you are prepared for prolonged outages and to enable automatic switching of storage environments to alternative locations in the event of an outage.

• Utilize monitoring tools to continuously keep an eye on the storage environment's availability and response times. Little can be done to prevent outages because they typically result from software issues, making them difficult to prevent.

Instability and Application Failure

Applications may freeze, lock up, crash, or become unresponsive due to issues with software or firmware, which can also cause a computer or network to completely fail or lose functionality. To prevent instability and application failure,

• Ensure that all software updates are regularly applied to the infrastructure in order to prevent instability and application failure.

• Use service monitoring to find and notify you when an application is not responding as it should.

Slowness

When the response time of a computer or network or storage is considered unacceptably slow, its availability is affected. Slowness can continue and cause efficiency loss and useful downtime. To prevent slowness of storage,

• Configure the architecture using redundant storage and network connections so that application access will automatically switch to the fastest environment. Make sure you've also implemented high-capacity services with demand-driven resource expansion.

• Constantly check the applications' response times, and make sure alerts are delivered to support staff outside of the system to prevent delivery issues.

• Write clauses into contracts with storage manufacturers that offer rewards for late responses.

• Despite best efforts, slowness can continue, leading to lost efficiency and ineffective downtime.

High Availability

When a device has a problem, a service that is supposed to switch over to other, working devices might not actually switch over properly. This might occur, for instance, if a primary device gradually becomes less responsive to the point where it is effectively unresponsive, but the HA software doesn't actually recognise this as a "down" state. To prevent HA failure,

• Run recurring failover tests

• Monitor the health of backup systems or all the systems in a HA cluster.

• There isn't much that can be done to ensure that systems will switch over when they should.

Backup Failure

Data loss occurs when you realise the backups you were counting on aren't actually any good, either because the backup media is damaged or the backup data is corrupted or missing. Backups fail, but multiple paths to recovery can reduce the risk to a large extent. Data backups are one of the most dependable security practises because they have been done for a long time. Data can last an eternity if it is properly replicated. In order to stop backup failures,

• Use storage elasticity to avoid using conventional offline backups (on tape or in optical form).

• Repeat recovery tests frequently to confirm the data's resilience.

• Include a data-loss clause in the agreement with the storage manufacturer so that they will be motivated to assist with an unexpected data loss.

Few Things to Remember­

Last but not least, it's critical to make sure that the server environment itself is under control and observation. Security of the storage infrastructure alone is insufficient. Any server that is accessed could be dangerously exposed, as could the storage environment. Server configuration must be secure, and the equipment must be kept in a facility that is monitored and secure with access control. The security of the storage environment should be taken into consideration when performing change management and activity monitoring to keep track of system changes and the actions of administrators on the server. Not only on the servers hosting the data, but also on the management servers used to manage the arrays and switches, these actions must be taken.

Solid understanding of storage security procedures should be part of the required skill set when hiring people to manage and secure the storage environment. An important requirement should be to have knowledge of computer security, networking, and storage techniques.

A crucial step in any organization's business continuity process is offsite (secure) data storage. To guarantee accountability for all data sent offsite, these facilities should undergo regular audits. Whether on disc or tape, the data should be encrypted for security reasons. End-to-end encryption should be used for all forms of online data backup.

1.2) Database Security

Databases play an important role in businesses as organizations typically deal with humongous amount of data that gets stored in databases either in a simple row-column format or complex non-relational format.

There are many uses for databases, including:

• Application support

Relational databases are the most widely used method for storing data, and can be used to store anything from basic employee lists to enterprise-level tracking software.

• Secure storage of sensitive information

One of the safest ways to store crucial data centrally is with relational databases. In regulated industries, these techniques can be used to comply with legislative requirements.

• Online transaction processing (OLTP)

Client applications and other servers access information that is stored and processed by OLTP systems. High levels of data modification are a defining characteristic of OLTP databases (inserting, updating, and deleting rows). As a result, they are enhanced to support dynamic data. They typically hold large amounts of data, which if not properly managed, can quickly grow.

• Data Warehousing

Platforms for relational databases can act as a central repository for data gathered from a variety of internal data sources. Then, "decision support" systems and centralised reporting can both use this database.

Database Security Layers

Database Server-Level Security

A database application's security depends entirely on the server it is installed on. Therefore, whether the servers are located locally or off-site, it is crucial to secure the servers on which your databases will be hosted.

- Choose which programs and users should have access to it.

- Make sure the databases are physically secure to prevent unauthorized individuals from accessing database files and data backups.

- Direct physical access to a database is rarely necessary because modern database platforms can be managed remotely.

Database Network Security Layer

Database security at the network layer is also crucial. These are a few best, typical practices

- Implement routing rules and packet filtering to make sure that only specific users on the internal network will even be able to communicate with a server.

- Modify the server's default port of listening.

Database Encryption Layer

Since databases store numerous types of information, including credit card numbers and passwords, which may or may not be sensitive and confidential, data encryption is a crucial security feature in areas outside of the network layer.

- A database can make effective use of data encryption

- Only the calling application will be able to decipher and make use of the encrypted values that are obscured in the data to allow authorised users to access and modify the data as needed.

On the majority of platforms, operating system security and database security are mutually exclusive. Database security can be affected by a variety of factors, including operating system encryption capabilities, file system permissions, network configuration settings, and authentication procedures. It's crucial for systems administrators to keep permissions settings current and to make sure that unused accounts are promptly deactivated.

Database-level security

Users have various types of permissions based on their job functions, and databases are frequently used to host a wide variety of databases and applications. Although any user may be able to connect to a database, each user will only be given the permissions they need.

In most cases, which databases a user has access to is determined by the first type of database-level security. Database administrators can specify whether or not a user login is required to access a particular database. Additional permissions must be assigned after a user has been given access to a database in order to specify the actions that user is permitted to perform there.

Database Roles and Permissions

Choosing the database(s) to which a login may connect is the first step in the general process. The database must then be assigned permissions. Typically, "groups" or "roles" are created by database administrators, and each of these contains users. The roles each have a set of permissions. Database administrators can easily manage which users have which permissions by using roles.

Object-level security

Relational databases can store a wide variety of objects. But the fundamental unit for storing data is a table. In general, each table is made to refer to a specific kind of entity. Information about each of these items is stored in columns within these tables. The ability to use one or more of the most popular SQL commands is granted. These commands are

• SELECT Retrieves information from databases. SELECT statements can obtain and combine data from many different tables, and can also be used for performing complex aggregate calculations.

• INSERT Adds a new row to a table.

• UPDATE Changes the values in an existing row or rows.

• DELETE Deletes rows from a table.

The ANSI Standard SQL language provides for the ability to use three commands for administering permissions to tables and other database objects:

• GRANT - Specifies that a particular user or role will have access to perform a specific action.

• REVOKE - Removes any current permissions settings for the specified users or roles.

• DENY - Prevents a user or role from performing a specific action.

Improvising Database Security

It's wise to refrain from granting permissions directly on database tables as a general rule. Instead, you should give users access to other database objects by giving them permissions so they can access the data they require. We'll take a broad look at the three frequently used database objects in this section and discuss how they can be used to more effectively manage security settings.

Views

A view is a logical relational database object that actually refers to one or more underlying database tables. In general, views are defined as the output of a SELECT query. This query can then retrieve data from numerous different tables and process the data using standard mathematical operations. One of the most popular techniques for limiting access to data is the use of views. Database administrators now have a way to define granular permissions settings that were previously impossible. After a view has been created, it can be given object-level permissions. The view will then allow database users to access any necessary information. A chain of objects based on business rules can be created by views by querying other views.

Stored Procedures

Database stored procedures allow different users to carry out common tasks. By using objects called stored procedures, databases allow developers to write and reuse SQL code. Any operation that can be carried out with the aid of common SQL commands can be performed using stored procedures. They can also consider arguments (much like functions and in other programming languages). Regarding security, stored procedures let users make changes to data kept in tables without granting direct access.

Triggers

Triggers are intended to be activated automatically whenever certain actions occur within a database. Triggers can be applied in various ways in terms of security. To start, you can conduct thorough auditing using triggers. For instance, you might want to alert a senior manager whenever certain information in a table is changed, or you might write a row logging this action to another table. Triggers can also be used to enforce complex database-related rules. For instance, if you want to guarantee that a particular set of actions is always performed whenever data is changed, you can create the necessary trigger to accomplish this.

In addition, you can customise the permissions that each web application has on the database by creating multiple accounts for each web application that tries to access the databases.

Securing databases from internet based applications

Web servers are used by many internet-based applications to access databases. It is crucial to protect the web applications that are running on these web servers so that they don't offer a route for attacking the databases. Some of the preventive measures that you could take against such risks,

- Prevent direct access to the databases from all but the most trusted servers (or, sometimes, networks)

- Web and standard-client applications often use a “connection string” to store authentication information. For administration purposes, this information is often stored in configuration files that can be modified, as needed. Ensure that these files are properly protected (through the use of encryption and file system permissions)

- To prevent errors, data corruption, or system crashes and attacks such as SQL injection, data validation must be done.

Database Backup and Recovery

Database Recovery and Backup

Accidental human error, flawed application logic, flaws in the database or operating system platform, and, of course, malicious users who are able to get around security measures are all potential causes of data loss. The only real way to recover data in the event that it is incorrectly altered or completely destroyed is from backups.

Choose the databases and tables you want to backup first. It's time to consider how to implement a data protection strategy once you have a good idea of what your company needs to back up. Prior to looking at the technical requirements for any type of data protection solution, it is imperative that you define your business requirements. You might also have a preliminary budget cap that can be used as a benchmark for comparing solutions in addition to these requirements. Additionally, you should start considering your staff and the kinds of expertise you'll need to have on hand in order to implement a solution.

Additionally, it's critical to remember that the goal of data protection is not to produce backups. The ability to recover information in the event that it is lost is the true goal. To that end, it's a good idea to start designing a backup solution based on the data you need to recover. The cost of downtime, the worth of the data, and the maximum amount of allowable data loss in the worst-case scenario should all be considered. Also consider the likelihood of specific catastrophes.

Auditing and Monitoring Databases

When it comes to network and database security, the concept of accountability is crucial. Keeping track of data changes and permission usage is part of the auditing process. Before much harm is done, users who are attempting to violate their security permissions (or users who are not authorised at all) can frequently be identified and dealt with; alternatively, once data has been altered, auditing can provide information about the extent of loss or changes. Users may be less likely to try to snoop around your databases if they are aware that certain actions are being tracked. This method can therefore act as a deterrent.

Unfortunately, auditing often goes unnoticed in settings. You can track particular actions based on user roles or actions on particular database objects in the majority of relational databases. Too much information auditing frequently has a negative impact on system performance. Audit logs may also consume a sizable amount of disc space. Therefore, auditing systems need to be properly configured.

Most database administrators ought to configure logging of both successful and unsuccessful database login attempts, at the very least. This measure will provide some level of accountability even though it will only provide limited information on its own.

Reviewing Database Audit Logs

System and database administrators should routinely review the data gathered in order for auditing to be truly useful. Only by engaging in this activity can potential security settings issues be identified before they worsen. As a result, you might want to check the audit logs and establish specific responses to unusual activity that is logged. Additionally, reading through logs can be overwhelming; therefore, any techniques for filtering the gathered data can be useful.

Monitoring Databases

Sometimes all you need is a quick snapshot of the server's users and their activities. The majority of databases offer simple ways to view this data. Starting with the most recent activity information may not be the best way to discover potential security breaches, but it can give you a better understanding of how your database is being used. You will be able to quickly spot any potential system abuse by creating a performance and usage baseline. Additionally, based on typical activity, you can set up alerts that can be used to alert you when performance or other statistics are "out of bounds."

Part III

Network Security

3.1) Secure Network Design

Network design frequently overlooks the importance of security. When the security of an existing network needs to be upgraded, it becomes even harder and more likely to be disregarded.

Budgets, availability requirements, network size and scope, anticipated future growth, capacity needs, and management's risk tolerance are all factors in network design.

Each component of a network carries out unique tasks and houses data with unique security needs. Some devices hold extremely sensitive data that, if disclosed to unauthorised parties, could harm a company. Depending on where they are on the network, other devices are more exposed. Internal file servers, for instance, will be protected differently than web servers that are accessible to the general public. It is useful to recognise key security controls and be aware of the repercussions of a failure in those controls when designing and implementing security in network and system architectures.

For example, by restricting which services users can connect to on a given system, firewalls safeguard hosts. It's critical to secure the network as a whole in addition to its individual components. The network perimeter is a definite inner boundary within the electronic security perimeter and consists of all the external-most points of the internal network. Every connection to another network, including the Internet and any external third parties (such as business partners, data providers, and so on), creates a point of entry into the perimeter that needs to be protected. Implementing firewalls to allow only the communications necessary for conducting business and conducting periodic audits of the external networks are both good practices for reducing risks.

Impact of Wireless Networks on Network Security

Companies using wireless solutions must be aware of and take precautions against the risk of an unauthorised person connecting to the corporate LAN through wireless signal leakage outside of corporate-controlled premises. While the wireless access point signals quickly deteriorate when travelling over distance and through walls, more potent and specialised directional antennas like Yagi antennas can pick up signals at considerable distances. In addition to issues with signal leakage, weaknesses in the encryption techniques used to secure wireless traffic have been found.

As a result, there is a big chance that unauthorised parties could intercept and monitor network communications on wireless networks. Segregating wireless connectivity from the rest of the corporate LAN has become standard practise to reduce the risks brought on by inadequate encryption and signal monitoring. VPN solutions can provide strong wireless traffic encryption and authentication as a temporary fix.

Network design must also take into account the impact of the explosion of mobile devices on wireless networks, the ways in which wireless designs must support and accommodate a greater variety of devices, and the ways in which this is driving the development of technologies like mobile device fingerprinting and identity management. The sheer number of mobile devices has led to unexpected risks for the wireless network as well as significant security challenges, creating a new dynamic that has expanded the network beyond its conventional boundaries.

Setting up Remote Access

The majority of corporate networks enable remote user access to internal resources. In the past, this was accomplished through a dial-up connection, but today, remote access is typically offered via a VPN solution. In contrast to a site-to-site or LAN-to-LAN VPN, which connects two networks together, a remote access VPN (also known as RA VPNs) connects people who are physically located outside of the organization to its network. VPNs affect the corporate network perimeter significantly despite being useful. Depending on how they are set up, VPNs can allow remote workstations to connect as if they were physically connected to the local network, even though they are not under the corporate security infrastructure's umbrella of protection. The security of the corporate network as a whole is dependent on the security of the employee's remote PC when VPN peers are remote users connecting to the corporate network via the Internet. The VPN may be used to tunnel traffic around corporate firewalls and the security they offer if a hacker manages to access an unprotected PC.

Security administrators need to make sure that adequate endpoint security is in place when VPNs are used for remote user access to the corporate network. The majority of significant firewall and VPN vendors integrate firewalling capabilities into their clients. When using their external email and the Internet, home users are not covered by the most recent corporate antivirus infrastructure. When deploying VPNs, these risks should be taken into account and minimised. Before allowing a remote system to connect to the network, posture validation, a feature of many remote access VPN products, performs a security software and configuration check on the system. It's an effective way to lessen the danger of vulnerable, infected, or compromised systems introducing threats to the company's network.

Internal Network Security Practices

Internally initiated attacks, which are currently the most prevalent threats, are vulnerable to organisations that only use firewalls to protect the perimeter of their networks. In order to add additional security for particularly sensitive resources like research networks, repositories for intellectual property, and databases used for payroll and human resources, internal controls like firewalls and early detection systems like IDS, IPS, and SIEM should be placed at strategic points within the internal network.

If there is no reason for two specific networks to communicate with one another when designing internal network zones, explicitly configure the network to block traffic between those networks, and track any attempts that hosts make to communicate between them. This can be difficult with modern VoIP networks because VoIP streams are typically endpoint to endpoint, but you should think about only allowing traffic that you are certain is legitimate between any two networks. Targeting a less secure area of the network and then slowly gaining access by "jumping" from one area of the network to another is a common tactic used by hackers. By blocking and logging the communication attempts between those networks, such threats can be avoided.

Intranets, Extranets, and DMZs

Organizations divide the networks into three categories for the purpose of applying security policies, practices and rules to the devices within these “nets”. Let’s take a deeper look into these network categories.

Intranets

Giving internal users access to applications and information is the main goal of an intranet. Internal applications, such as knowledge bases, organisation bulletin boards, and time and expense tracking systems, are housed on intranets where they are typically inaccessible to outside parties. An intranet's primary function is to facilitate employee sharing of company data and computing resources. Intranet systems are combined into one or more dedicated subnets and firewalled to increase security.

Extranets

Extranets are application networks that are under the control of a company and made accessible to reliable outside parties like partners, clients, and vendors. Extranets, however, require additional security processes and procedures beyond those of intranets because these users are external to the company and the security of their networks is beyond the company's control.

DMZs’

A company might decide to make some of its systems publicly accessible via the Internet. For instance, the email server needs to be accessible from the Internet in order for an organisation to receive Internet mail. Deploying these systems on a specific subnet, also known as a demilitarised zone (DMZ) or screened subnet, apart from internal systems, is a good idea. These systems can and will be attacked by malicious users because they are publicly accessible. A successful attack against these systems still leaves a firewall between the successful attacker and more sensitive internal resources because they are housed on a separate network.

A single application system's components can be divided using a number of DMZs. For instance, a business that separates its web servers and email system into separate DMZs shields each system from a flaw in the other. Even if a hacker is successful in exploiting a web server vulnerability, a firewall still prevents them from accessing the email system.

Web Access Considerations

Proxy servers can be set up to prevent connections to URLs that are thought to be potentially harmful or not required for normal operation, such as those that contain specific scripts or other executable files. Proxy services are fortified procedures that can be offered independently by a dedicated server or internally on a firewall. When regulating user traffic, a company has a number of extra options when using a proxy service. For instance, the business might want to check downloaded files for viruses before sending them to the end user. Additionally, a proxy server can log, record, and compile information about user Internet activity, which can discourage workers from wasting their time browsing websites or going to pages that are irrelevant to their line of work. For example, high-bandwidth music and video downloads can quickly saturate an organization’s Internet link, slowing other critical business systems that share the connection.

Outbound Filtering

By allowing users to access services that do not adhere to corporate security policies or that do not have valid business purposes, users run a number of serious risks to the company and its infrastructure if outbound access is not restricted.

Securing Routers and Switches

In this sub-topic, we will be learning on how to secure network devices especially routers and switches that constitute a major part of the network.

Switches

The network hub's evolved offspring are switches. Switches are layer two devices, despite some layer 3 features like QoS and basic routing being implemented in the newest switches.

Switches are more intelligent devices that learn the various MAC addresses of connected devices and transmit packets only to the devices they are specifically addressed to. In addition, switches provide a security benefit by reducing the ability to monitor or “sniff” another workstation’s traffic. A switched network cannot absolutely eliminate the ability to sniff traffic. By means of ARP poisoning and gratuitous ARP attacks. To reduce a network’s exposure to ARP poisoning attacks, segregate sensitive hosts between layer three devices or use virtual LAN (VLAN) functionality on switches. For highly sensitive hosts, administrators may wish to statically define important MAC entries, such as the default gateway.

ARP-learned MAC entries will be subordinate to statically defined MAC entries. Although it is time-consuming and does not scale well, statically defining ARP entries can safeguard small networks that demand high security. Make sure to first ascertain whether any of the devices on your network use ARP spoofing for any HA functionality or for other valid functional reasons, such as new host redirection to a captive portal.

Routers

Routers operate at layer three, the network layer of the OSI model, and Internet Protocol version 4 is the most popular layer three protocol today (IPv4). Routers are primarily used to transfer traffic among networks and between different parts of a single network. Routers can locate various networks either manually or dynamically using administratively defined static routes or routing protocols. To ensure reliable connectivity between all required networks, networks typically combine the two.

Additionally, there may be a risk with dynamic routes. An important security concern is regulating which devices can advertise routes for your network. Network rogue or malicious routes can stop legitimate communications or reroute sensitive data to unauthorised parties. The Border Gateway Protocol (BGP) and a number of other routing protocols, including RIPv2, OSPF, and Open Shortest Path First (SSPF), can all perform authentication; however, a typical solution is to block or filter routing protocol updates on essential router interfaces.

Hardening the devices

Patching

Patches and updates that the product vendor releases should be applied promptly. The distinction between a minor inconvenience and a serious security incident can be made by prompt detection of potential issues and the installation of patches to address recently discovered security vulnerabilities. Subscribe to your vendor's email notification services as well as mailing lists for general security to make sure you are promptly informed of such vulnerabilities. Keep a close eye out for knowledge base (KB) articles and release notes that detail changes in device behaviour and default settings from one code version to the next, as well as any vulnerabilities or bugs that were fixed. By invalidating prior measures you've taken to secure your devices, ignoring these details can result in potential security issues on your network.

Switch Security Practices

Hosts cannot send traffic directly to switches because they do not keep track of layer three IP addresses. The ARP poisoning attack is the main strategy used against switches. Switches can still be used as security control devices despite the threat of an ARP attack. When physical access over the network port cannot be trusted, such as in public kiosks, switches can be configured to allow only certain MAC addresses to send traffic through a particular port on the switch. This feature is known as port security.

With port security, a malicious person cannot unplug the kiosk, plug in a laptop, and use the switch port because the switch would deny the traffic because the laptop's MAC would not match the kiosk's MAC. Even though a MAC address can be faked, locking a port to a particular MAC makes it more difficult for a potential intruder. Virtual local area networks (VLANs), layer two broadcast domains that are used to further divide LANs, can also be built using switches. VLAN boundaries are generally useful for controlling and managing network segmentation as well as providing a foundation for applying various security levels to various networks depending on the particular security requirements.

Access Control Lists

Filtering IP packets is a function of routers. The source or destination address, or both, as well as other factors like the TCP or UDP port numbers present in a packet, can be used to permit or deny TCP, UDP, or other types of traffic using access control lists (ACLs). ACLs on routers placed carefully can greatly improve network security. ACLs, for instance, can be used on edge or border routers to filter out traffic that is obviously unwanted (like RFC 1918 traffic coming from an Internet source), relieving the load on border firewalls. Additionally, WAN links can use ACLs to filter out broadcast and other unnecessary traffic, thereby consuming less bandwidth. ACLs are frequently used for other more sophisticated purposes as well as for protecting the router itself. The best practise is to use an ACL to restrict access to the administrative services (like Telnet, SSH, or HTTP) on a router to the management stations or hosts on a network used by administrative staff members who are permitted to log in to the network devices. The ACL engines in many vendors' products have special features built in.

Disabling Unused Services

Proxy ARP

One host can respond to ARP requests on behalf of the real host using proxy ARP. This is frequently employed on a firewall when traffic for protected hosts is being proxied. Proxy ARP is enabled by default on Cisco routers, which may make it possible for an attacker to launch an ARP poisoning attack against a host that is not connected to the local subnet or VLAN.

Network Discovery Protocols

There are a number of automatic discovery protocols; some are vendor-specific, like Cisco Discovery Protocol (CDP), while others are open standards, like Link Layer Discovery Protocol (LLDP). In all cases, even though they might make network administration a little easier, they also give anyone sniffing the network the chance to discover a lot of information about the network topology. When not in use, these protocols should be disabled, and when they are, special care should be taken to keep them as secure as possible.

Other Extra Unnecessary Services

These extra services can be secured or altogether disabled if unused.

Diagnostic Services

For some UDP/TCP services, routers have a number of diagnostic services enabled, including ICMP echo request, reply, and discard. When not in use for diagnostic testing or troubleshooting, these services ought to be turned off. These services may expose a vulnerability for a denial of service (DoS) condition by accessing a compromised router and activating a debug process that uses all of the device's resources. The same way, an administrator could unintentionally cause an outage.

BOOTP Server

DHCP addresses can be distributed to clients via the BOOTP service using BOOTP Server Routers. The router frequently serves as the DHCP server in residential and small office/home office (SOHO) configurations, but this is less common in enterprise settings. Disable the unnecessary service if it's not in use.

TFTP Server

To transfer configuration files and software updates to and from the router, use a trivial file transfer protocol (TFTP) server. However, TFTP doesn't offer services for authorization or authentication. Most administrators keep a TFTP server running outside of the router and turn it on as necessary.

Web Server

A web server is offered by many vendors so that configuration changes can be made. The web server can be disabled if the router won't be managed in this way. While they are active, these services, along with a number of others, put the router's regular operation at risk for security breaches. Many times, security breaches can be prevented by simply becoming aware of and adhering to a manufacturer's best practise recommendations regarding its equipment. If in doubt, disable the services until you need them.

Administrative Practices

There are several techniques for managing routers. Telnet or the Secure Shell protocol can be used to remotely access a command-line interface from a console (SSH). Telnet is sent over the network in cleartext, so SSH is advised. In addition, a browser can access a web interface, and the Simple Network Management Protocol can be used to monitor and control the router (SNMP). Configuring a login banner or message-of-the-day (MOTD) banner, which is shown whenever a connection is established as part of the login process, is another crucial step in hardening network devices.

. A warning message about unauthorised use of the device should be included in the banner in addition to making sure that it doesn't contain any vital information that could reveal the device's type or operating system. This makes it impossible for someone to claim that they were unaware that their use was prohibited. Along with following these best practises, it's a good idea to omit information about the device's location or the organisation it belongs to. Essentially, you want the banner to be a strong warning while remaining as generic as possible.

Remote Command Line

SSH is a protocol that is supported by the majority of routers. The same access and interface are offered by SSH as by Telnet, but all communications are encrypted. It is possible for an attacker to intercept sensitive data, including passwords and configuration parameters, while it is being transmitted over the network if administrative connections to network routers are not encrypted. The configuration of host and domain names on the router, the creation of an encryption key, the configuration of accounts, and the setting of necessary SSH parameters are all required on many network devices in order to enable SSH.

Many network devices keep two passwords by default—one for device access and another for configuration commands, also known as "privileged" or "enable" access. It can usually be configured even if this is not the default behaviour.

Individual user accounts can and should be created to provide granular authorization and full accountability, though not always locally on the device; the method and choice to use named accounts on an individual basis is much more crucial than where the accounts are created and stored. Another vital factor to take into account is how these passwords will be stored—locally or in a central authentication server.

Centralizing Account Management (AAA)

It is difficult to synchronise and maintain separate user accounts on each network switch, router, and device in large-scale environments. The majority of network devices can be set up to use authentication, authorization, and accounting to verify their identity against a central account repository (AAA). The removal of usernames and passwords from local configurations is facilitated by this. While AAA is the mechanism, a sound methodology for administrative device account creation and use policy is equally important. As you can take extra precautions like more frequent password rotation for admin accounts or more stringent password complexity requirements, requiring administrators to have a separate account specifically for administrative purposes will help protect crucial network equipment.

The only real drawback to the strategy is that if one of these accounts with elevated privileges is compromised, an attacker would gain access to resources they might not otherwise have.

RADIUS and TACACS (now TACACS+) are the two most widely used protocols for these access devices to conduct device-level AAA communication. Some devices can directly query an LDAP or Active Directory service in addition to those that use RADIUS and TACACS+. Administrative control can be precisely tailored for particular needs using the granular controls and variables provided by these protocols.

A remote authentication server shouldn't be used for all aspects of network device authentication. No one could log in if the server was down or unavailable. Consequently, maintaining a local backup account is a wise preventative measure.

Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP), which offers a centralised mechanism for monitoring and configuration, can also be used to monitor and manage network devices. Through the use of Management Information Base Object Identifiers (MIB OIDs), a structured format database that describes objects within a device that can be monitored or managed by SNMP or another management protocol, SNMP can be used to monitor things like link operation, port status and statistics, and CPU load. By configuring an ACL on each device to regulate who is permitted to query the device via SNMP and what they are permitted to do, it is possible to protect SNMP communications. RW SNMP should only be used if a particular automation or functionality needs read-write access. If not, use RO for node managers that are only collecting statistics.

Internet Control Message Protocol (ICMP)

Protocol for Internet Control Messages (ICMP)

TCP/IP communication issues can be reported using the Internet Control Message Protocol (ICMP), which also offers tools for evaluating IP layer connectivity. When analysing network issues, it is a crucial tool. ICMP, however, can also be used to gather crucial data about network topologies and accessible host services. Messages are a general term for a wide range of defined ICMP communication types. When used maliciously, the following ICMP functions pose a number of risks.

ECHO and Traceroute

Pings, also known as echo requests and replies, are used to check whether a host is available and reachable over the network. One host's ability to successfully ping another host indicates that the hosts' networks are functioning properly up to and including layer three of the OSI model. This does not ensure that there are no additional restrictions or barriers in place, but it does show reachability. However, there are occasionally exceptions to this rule.

Attackers with more experience avoid ping and employ more covert techniques for host identification. However, an attacker can use ping to scan publicly accessible networks to find available hosts. Because it is believed that nothing bad can be contained in an ICMP packet, ICMP echo and echo reply have also been used to make covert channels through firewalls that permit malicious traffic to pass through unchecked. At the network perimeter, ICMP echo requests and responses should be dropped. TTL packets can be used by an attacker to find open ports in perimeter firewalls.

Attackers have developed a technique for scanning networks using UDP, TCP, and ICMP packets that expire one hop past the perimeter firewall using this method. Dropping TTL Exceeded packets can prevent such attacks since they rely on receiving ICMP TTL Exceeded messages from firewalled hosts.

Unreachable Messages

A Type 3 Destination Unreachable message is another classification of ICMP message. When a router is unable to forward a packet because the specified destination address or service is unavailable, it will respond with an ICMP Type 3 message. Dropping all messages marked as Destination Unreachable has a significant impact. For a network to function properly, the message Code 4, "Fragmentation Needed," is crucial. If hosts are not informed that the amount of data they are transmitting into the network exceeds its maximum transmission unit (MTU), disruptions may result.

Directed Broadcasts

A packet sent to a network's first and last addresses is equivalent to sending a separate packet to every host connected to that network. A class of attacks known as bandwidth amplification attacks are based on this functionality. In such attacks, the attacker inserts the victim's source address into UDP ECHO packets or ICMP traffic sent to a number of large networks' broadcast addresses. This is done to ensure that the victim and not the attacker receives the ICMP responses. Due to the way that some services that use the UDP protocol behave, these packets will elicit responses from every system that is reachable and responding within the network range. Modern firewalls are capable of spotting and preventing these attacks, but frequently rely on being configured to do so.

Redirects

In the normal course of network operation, ICMP redirects are used to inform hosts of a more effective route to a destination network. On networks where several routers are present on the same subnet, this is typical. Redirects on router interfaces to untrusted and external networks should be disabled because a malicious user may be able to manipulate routing paths.

Anti-Spoofing and Source Routing

Attackers spoof or insert information into TCP/IP packet headers in an effort to pass for a more reputable host. Internal packets should obviously not be arriving inbound on border routers, as address spoofing is an attempt to get past external defences by posing as an internal host. Inbound packets with source IP addresses that match the internal network can be dropped by border routers to protect the network from such attacks. Additionally, broadcast packets and packets with source addresses that match RFC 1918 "private" IP addresses should be dropped by routers. Routers should be set up to reject packets that contain source routing information in addition to spoofed packets.

The route a packet should take through a network is determined by source routing. By forcing a lot of traffic through one router and overloading it, such information could be used to circumvent known filters or create a denial of service situation. An administrator might occasionally want to use source routing. In these circumstances, source routing may be enabled solely for that goal.

Logging

Both system-related and ACL activity-related information can be logged by routers. Although the majority of routers lack large discs for locally logging data about network and system activity, they do offer the ability to log remotely to a syslog server. A single repository can be created by centralising and aggregating all of the scattered network logs using the syslog facilities. Syslog can play a crucial role in conducting forensic investigations or in troubleshooting network-related issues. Choosing the appropriate level of logging and the duration of log retention gives you a window into the past and enables you to look back at what was happening in various locations throughout the network at a specific time. Security Information and Event Management (SIEM) is a cutting-edge security technology that gathers, examines, and correlates logs before either taking action or recommending action based on the event information.

Firewalls

The first line of defence between a company's internal network and unsecured networks like the Internet is a firewall. For layer three traffic, first-generation firewalls were merely permit/deny engines, operating similarly to an appliance with an access control list. They were only able to "allow or deny" traffic from "this predefined source IP address to this predefined destination IP address on these predefined TCP and UDP ports." They were unable to perform any other "intelligent" operations on the traffic. By keeping track of running network sessions, second-generation firewalls effectively operated at layer four. Stateful firewalls or, less frequently, circuit gateways were the names given to these devices.

By being able to monitor network sessions, the firewall was able to prevent man-in-the-middle (MITM) attacks coming from other IP addresses. In some sophisticated firewalls, a high-availability (HA) pair could swap session tables, allowing a network session to continue through the other firewall in the event that one failed. The application layer, or layer 7, was first entered by the third generation of firewalls. Some well-defined, preconfigured applications, like HTTP, DNS, and older, computer-to-computer protocols like FTP and Telnet, could be decoded by these "application firewalls," which could also decode data inside network traffic streams for other applications. They were created with the World Wide Web in mind, which made them well suited to identifying and preventing web site attacks like cross-site scripting and SQL injection, which were causing a lot of concern at the time.

Additionally, advanced application-layer firewalling capabilities, antivirus, intrusion detection and prevention, network content filtering, and other security features have been combined in unified threat management (UTM) devices. These are genuine devices at layer seven. Application-layer gateways, which are specifically created to comprehend how a specific application should function and how its traffic should be constructed and patterned, can be run on fourth-generation firewalls.

The majority of network appliances you will find today fall under the commonly accepted definition of a fourth-generation firewall. Fifth generation firewalls are internal to hosts and protect the operating system kernel. Some sixth generation firewalls (meta firewalls) have also been described.

Firewall Features

Application Awareness

At the very least, traffic from OSI layers three through seven must be able to be processed and interpreted by the firewall. In order to effectively manage communications between applications, it should be able to filter at layer three by IP address, layer four by port, layer five by network sessions, layer six by data type, and, most importantly, layer seven.

Accurate Application Fingerprinting

Applications should be correctly identified by the firewall not only based on their external appearance but also by the internal contents of their network communications. To guarantee that all applications are properly covered by the firewall policy configuration, accurate application identification is required.

Granular Application Control

The firewall must be able to recognize and classify the features of applications in order to manage them effectively, in addition to allowing or blocking communication between applications. Examples of potentially undesirable features that the firewall should be able to control include file transfer, desktop sharing, voice and video, and in-application gaming.

Bandwidth Management (QoS)

The firewall can control the Quality of Service (QoS) of preferred applications, such as Voice over IP (VoIP), based on the current network bandwidth availability. To guarantee the highest level of availability for the most important services, the firewall should integrate with other network devices.

Core Firewall Functions

Network Address Translation (NAT)

RFC 1918 designates specific network ranges as "private" networks that will never be used on the Internet in order to conserve IPv4 addresses. As a result, businesses can use these blocks for their internal corporate networks without having to worry about tripping over an Internet network. But in order for these networks to be routable when they are connected to the Internet, they must translate their private IP network addresses into public IP addresses (NAT). This allows a large number of hosts protected by a firewall to access the Internet alternately or by sharing a small number of public addresses. In a firewall, NAT is typically implemented independently of the policy or rule set. It is important to keep in mind that just because a NAT has been set up to translate addresses between two hosts, it does not guarantee that the hosts can talk to one another. The policy specified in the firewall rule set governs this.

Static NAT

The address translation that results from a static NAT configuration is constant. The host is defined with a fixed 1:1 relationship between a single local address and a corresponding global address. As each packet passes through the firewall, the static NAT translation rewrites the source and destination IP addresses as necessary. Nothing else in the packet is impacted. This is typically used for internal servers that require a stable IP address so they can be accessed from the Internet. This straightforward strategy will enable most protocols to pass through a static NAT without incident. Static NAT is most frequently used to give a trusted host inside the firewall perimeter access to the Internet or to grant inbound access to a particular host, like a web server that needs to be reachable via a public IP address.

Dynamic NAT

A group of internal local addresses can be mapped to one or more external addresses using dynamic NAT. From the standpoint of an Internet-based attacker, dynamic NAT has the advantage of offering a constantly changing set of IP addresses, which makes it more challenging to target specific systems. The limitation on the number of concurrent internal users who can access external resources at once is dynamic NAT's biggest drawback. Simply put, the firewall will exhaust its supply of global addresses and won't be able to assign new ones until the idle timers begin releasing global addresses.

Port Address Translation

The entire inside local address space can be translated to a single global address using port address translation (PAT). In addition to changing the source and destination IP addresses, this is accomplished by altering the communication port addresses. Due to the firewall's ability to keep track of which ports correspond to which sessions, multiple communications can use a single IP address. PAT offers a higher level of security because incoming connections cannot be made using it. PAT has the drawback of restricting connection-oriented protocols like TCP.

Auditing and Logging

A firewall makes a great auditor. They have the ability to record any traffic that passes through them if given enough disc space or remote logging capabilities. Attack attempts will leave traces in the logs, and if administrators are vigilantly monitoring the systems, attacks can be stopped before they succeed. Firewalls should keep track of both successful and unsuccessful system events. In order to assist the network and security administrators, it is best to send the logs to a Security Information and Event Management (SIEM) system, which can filter, analyse, and perform heuristic behaviour detection.

Firewall Design

Software-based firewalls are an option, but purpose-built appliances are far more prevalent. Sometimes a group of various devices work together to perform the firewalling duties. One of the most important aspects of securing a network is the design of the network where the firewall resides and its specific features. Firewalls must be properly configured and installed in the appropriate places on the network for them to be effective. Best practices include

* All communications must pass through the firewall. The effectiveness of the firewall is greatly reduced if an alternative network routing path is available; unauthorized traffic can be sent through a different network path, bypassing the control of the firewall
* The firewall permits only traffic that is authorized. If the firewall cannot be relied upon to differentiate between authorized and unauthorized traffic, or if it is configured to permit dangerous or unneeded communications, its usefulness is also diminished.
* In a failure or overload situation, a firewall must always fail into a “deny” or closed state, under the principle that it is better to interrupt communications than to leave systems unprotected.
* The firewall must be designed and configured to withstand attacks upon itself. Because the firewall is relied upon to stop attacks, and nothing else is deployed to protect the firewall itself against such attacks, it must be hardened and capable of withstanding attacks directly upon itself.

Firewall Strengths

• Firewalls are excellent at enforcing security policies. They should be configured to restrict communications to what management has determined and agreed with the business to be acceptable.

• Firewalls are used to restrict access to specific services.

• Firewalls are transparent on the network—no software is needed on end-user workstations.

• Firewalls can provide auditing. Given plenty of disk space or remote logging capabilities, they can log interesting traffic that passes through them.

• Firewalls can alert appropriate people of specified events.

Firewall Positioning

A firewall is typically placed at the edge of the network, directly in front of any external connections. However, more firewalls can be installed inside the network perimeter to protect specific hosts with higher security needs with a more focused defence.

Firewall Configuration

When building a rule set on a firewall, consider the following practices:

- Develop rules in descending order of specificity. The majority of firewalls run through their rule sets in order, stopping once a match is found. A general rule cannot obscure a specific rule further down the rule set by being placed above it.

- A rule set's most active rules should be placed near the top. Screening packets requires a lot of processing power, and as was already mentioned, a firewall will stop processing a packet after it matches a rule. CPU savings could be significant in situations where millions of packets are being processed and rule sets can have thousands of entries.

- All firewalls should be set up to reject "impossible" or "unroutable" Internet packets, such as broadcast packets, packets coming from an external interface whose source addresses match those of the internal network, and packets with RFC 1918 "private" IP addresses. All of these represent unwanted traffic, such as that created by attackers, because none of them would be anticipated from the Internet.

l

l

l