Cyber Security Vulnerabilities and Cyber Security Safeguards

Cyber Security Vulnerabilities - Overview

- In cybersecurity, a vulnerability is a weakness that can be exploited by cybercriminals to gain unauthorized access to a computer system. After exploiting a vulnerability, a cyber attack can run malicious code, install malware and even steal sensitive data.

What is a Zero-Day Exploit?

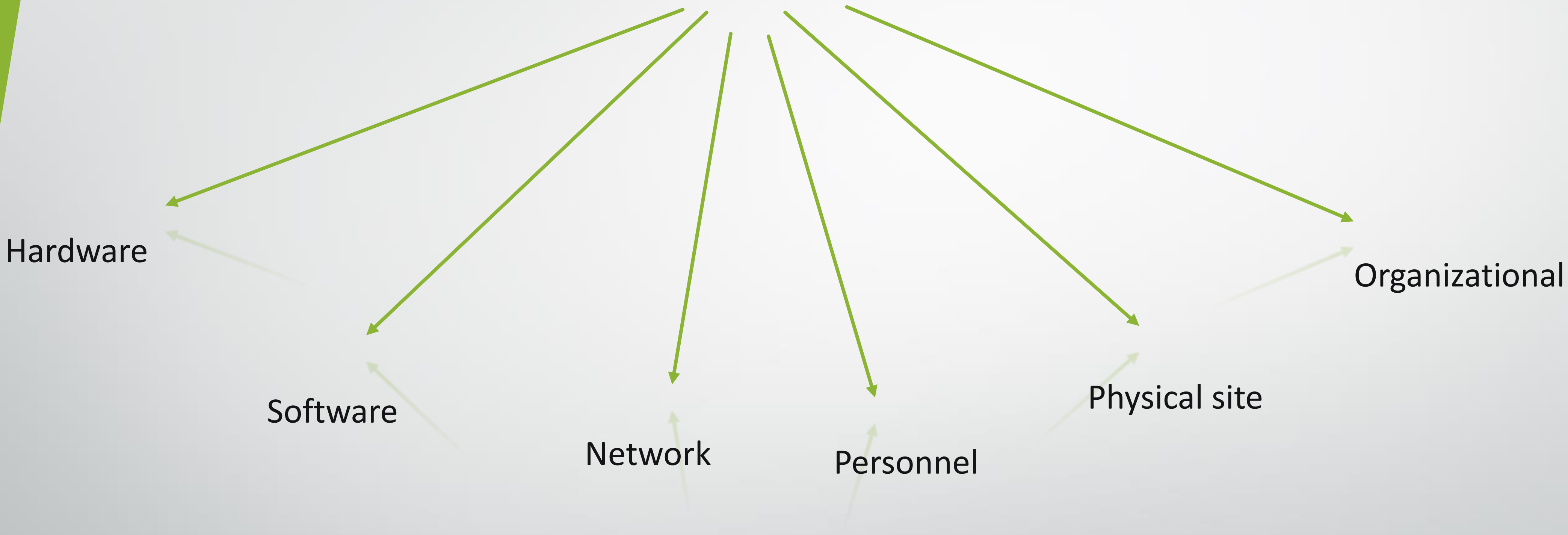
- A zero-day exploit (or zero-day) exploits a zero-day vulnerability. A zero-day (or 0-day) vulnerability is a vulnerability that is unknown to, or unaddressed by, those who want to patch the vulnerability.

What Causes Vulnerabilities?

There are many causes of vulnerabilities including:

- Complexity: Complex systems increase the probability of a flaw, misconfigurations or unintended access.
- Familiarity: Common code, software, operating systems and hardware increase the probability that an attacker can find or has information about known vulnerabilities.
- Connectivity
- Poor Password Management
- Operating System Flaws
- Internet Usage
- Software Bugs
- Unchecked User Input
- The biggest vulnerability in any organization is the human at the end of the system. Social engineering is the biggest threat to the majority of organizations.

Vulnerabilities can be classified into six broad categories:



Hardware

Software

Network

Personnel

Physical site

Organizational

Vulnerabilities in software

- Insufficient testing, lack of audit trail, design flaws, memory safety violations (buffer overflows, over-reads, dangling pointers), input validation errors (code injection, cross-site scripting (XSS), directory traversal, email injection, format string attacks, HTTP header injection, HTTP response splitting, SQL injection), privilege-confusion bugs (clickjacking, cross-site request forgery, FTP bounce attack), race conditions (symlink races, time-of-check-to-time-of-use bugs), side channel attacks, timing attacks and user interface failures (blaming the victim, race conditions, warning fatigue).

Hardware vulnerability

- Susceptibility to humidity, dust, soiling, natural disaster, poor encryption or firmware vulnerability.
-

Vulnerability in System administration

- **KNOWN VULNERABILITIES IN SYSTEM ADMINISTRATION**

Vulnerability in Complex Network Architectures

- Unprotected communication lines, man-in-the-middle attacks, insecure network architecture, lack of authentication or default authentication.

Vulnerability in Open Access to Organizational Data

- Corporate systems using the Internet are especially vulnerable because **the Internet is designed to be an open system and makes internal corporate systems more vulnerable to actions from outsiders**. Hackers can unleash denial of service (DoS) attacks or penetrate corporate networks to cause serious system disruptions.

Vulnerability in Weak Authentication

- **The ability of a user to access any application feature or resource without having first authenticated** represents a Weak Authentication vulnerability.
- Authorization vulnerabilities **allow malicious users to perform unwanted actions or access resources that are deemed protected otherwise**. Authorization vulnerabilities are one of the most widely found vulnerabilities in web applications.

Vulnerability in Unprotected Broadband communications

- Free public Wi-Fi is available in a lot of places — airports, restaurants, coffee shops, libraries, public transit, hotel rooms, you name it.
- The best way to help protect your personal information is to avoid accessing sensitive information or performing sensitive transactions when connected to public Wi-Fi. And there are other safety measures that can help.
- An attacker’s rogue Wi-Fi hotspot can pretend to act as your home network or as a public network that you might come across at a coffee shop or airport, for example. Instead of connecting to a real public Wi-Fi hotspot, your device connects to the attacker’s fake hotspot. This means the attacker’s network is between your device and the actual Wi-Fi network, so they’re able to see your online traffic.

Cyber Security Awareness

- Poor recruiting policy, lack of security awareness and training, poor adherence to security training, poor password management or downloading malware via email attachments.
- Lack of audit, continuity plan, security or incident response plan.

Cyber Security Safeguards- Overview

- Cybersecurity is the protection of internet-connected systems such as hardware, software and data from cyberthreats. The practice is used by individuals and enterprises to protect against unauthorized access to data centers and other computerized systems.

Key Layers of Cyber Security Safeguards

Layer One: Web Application Firewall

Layer Two: Access Control

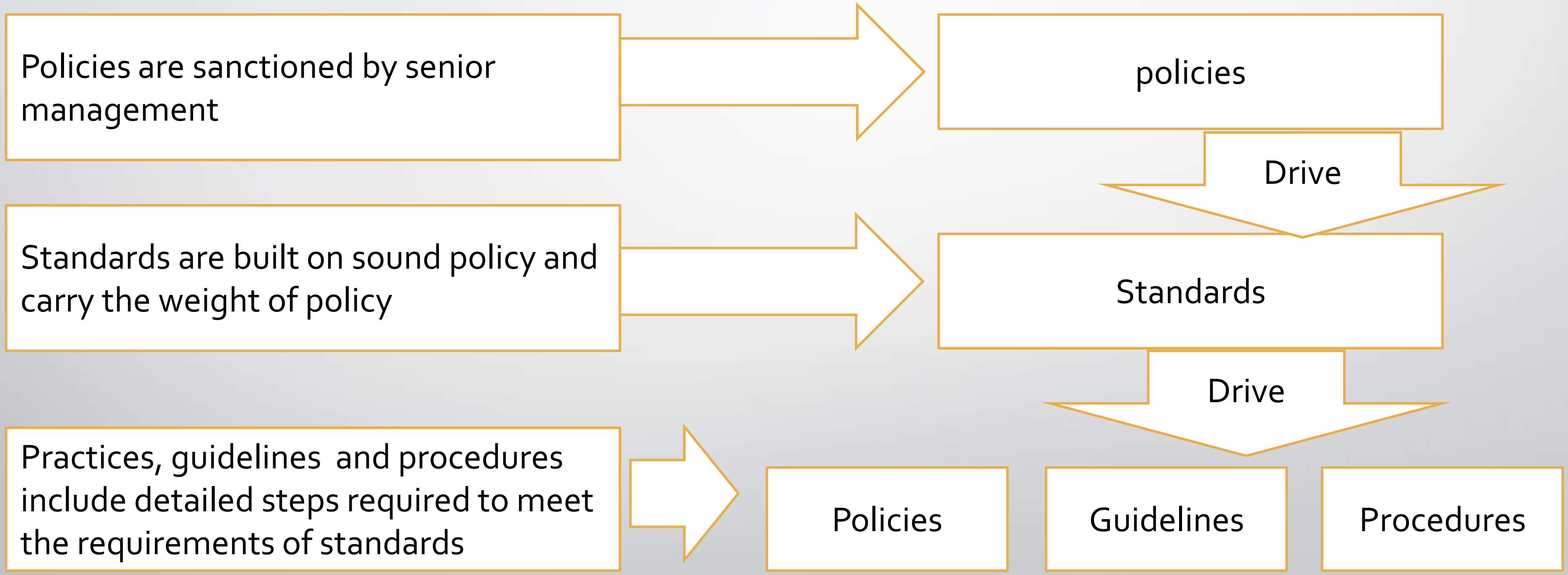
Layer Three: Bot Protection

Layer Four: Login

Layer Five: Behavioural Monitoring and Analytics

Security policies, standards and practices

Policies standards & practices



Policies are sanctioned by senior management

Standards are built on sound policy and carry the weight of policy

Practices, guidelines and procedures include detailed steps required to meet the requirements of standards

Examples

- Well-written policies should spell out who's responsible for security what needs to be protected and what is an acceptable level of risk.
  - All email communication must be strongly encrypted.
- Standards are much more specific than policies. Standards are tactical documents because they lay out specific steps or processes required to meet a certain requirement enforced by the policy. They are guidelines of how to go about implementing a policy.
  - Use an encryption that is not yet proven to be breakable in less than 30 minutes
- Practices are procedures that implement the policies with the desired standards.
  - Provide Wi-Fi router with AES encryption connected to a manageable switch. How to comply with the policy?

Introduction to Policy

- □ Security Policies are the foundation of your security infrastructure.
- □ Without them you can not protect your company from possible lawsuits, lost revenue bad publicity and not to mention basic security attack.
- □ A security policy is a document or a set of documents that describe, at a high level, the security control that will be implemented by the company.

Role of Security Policy

- Suggests the safety measures to be allowed in an organisation.
- Reduce or eliminate legal liabilities to employee and the third party.
- Protect priority or confidential information from theft, misuse, unauthorized disclosure and modification.
- Prevent waste of company computing resources.

Key Elements

- **A security policy should have these characteristics-**

  - ✓ Clear communication
  - ✓ Brief and clear communication
  - ✓ Define scope and applicability
  - ✓ Enforceable by law
  - ✓ Recognizes area of responsibility
  - ✓ Sufficient guidance
  - ✓ Top management involvement

Goals of security policies

- **Protection** of organizations computing resources
- **Elimination** of strong legal liability from employees or third parties
- Ensuring customers integrity and **preventing unauthorized modifications** of the data.

Types and responsible people for security policies

- Two basic type of security policy
  - Technical Security Policy : Includes how technology should be configured and use
  - Administrative Security Policy : Include people (both end user and management) should behave/respond to security policy
- Persons responsible for implementation of security policies are
  - Director of Information Security
  - Chief Security Officer
  - Director of Information Technology
  - Chief Information Officer

Classification of security policy

- User policy
  - Defines what kind of user is using the network
  - Defines the limitations that are applied on users to secure the network
  - Password management policy
  - Protects the user account with a secure password

Cont..

- IT policy
  - Designed for IT department to keep the network secure and stable
  - Following are the three different IT policies-
    - Backup policies
    - Server configuration, patch update, and modification policies
    - Firewall policies

Cont..

- General policy
    - Defines the responsibility for general business purposes]
    - The following are different general policies-
        - High level program policies \business continuity plans
        - Crisis management
        - Disaster recovery
- Partner policy
    - Policy that is defined among a group of partners.

Cont…

- Issue specific polices
  - Recognize specific areas of concern and describe the organization’s status for top level management
  - Involve revision and up gradation of policies from time to time, as changes in technology and related activities take place frequently.
- Components
  - Issue statement
  - Statement of the organizations position
  - Applicability
  - Roles and responsibility
  - Personnel security
  - Communication security
  - Risk management
  - Administrative security

Design of security policy

- Guidelines should cover the following points as policy structure-
  - Detailed description of the policy issues
  - Description about the status of the policy
  - Applicability of the policy to the environment
  - Functionalities of those affected by the policy
  - Compatibility level of the policy is necessary
  - End consequences of non-compliance

Contents of security policy

High level security requirements

- This statement features the requirements of a system to implement security policies that include discipline security, safeguard security, procedural security and assurance security.

Policy description based on requirement

- Focuses on security disciplines, safeguards, procedures, continuity of operations and documentation

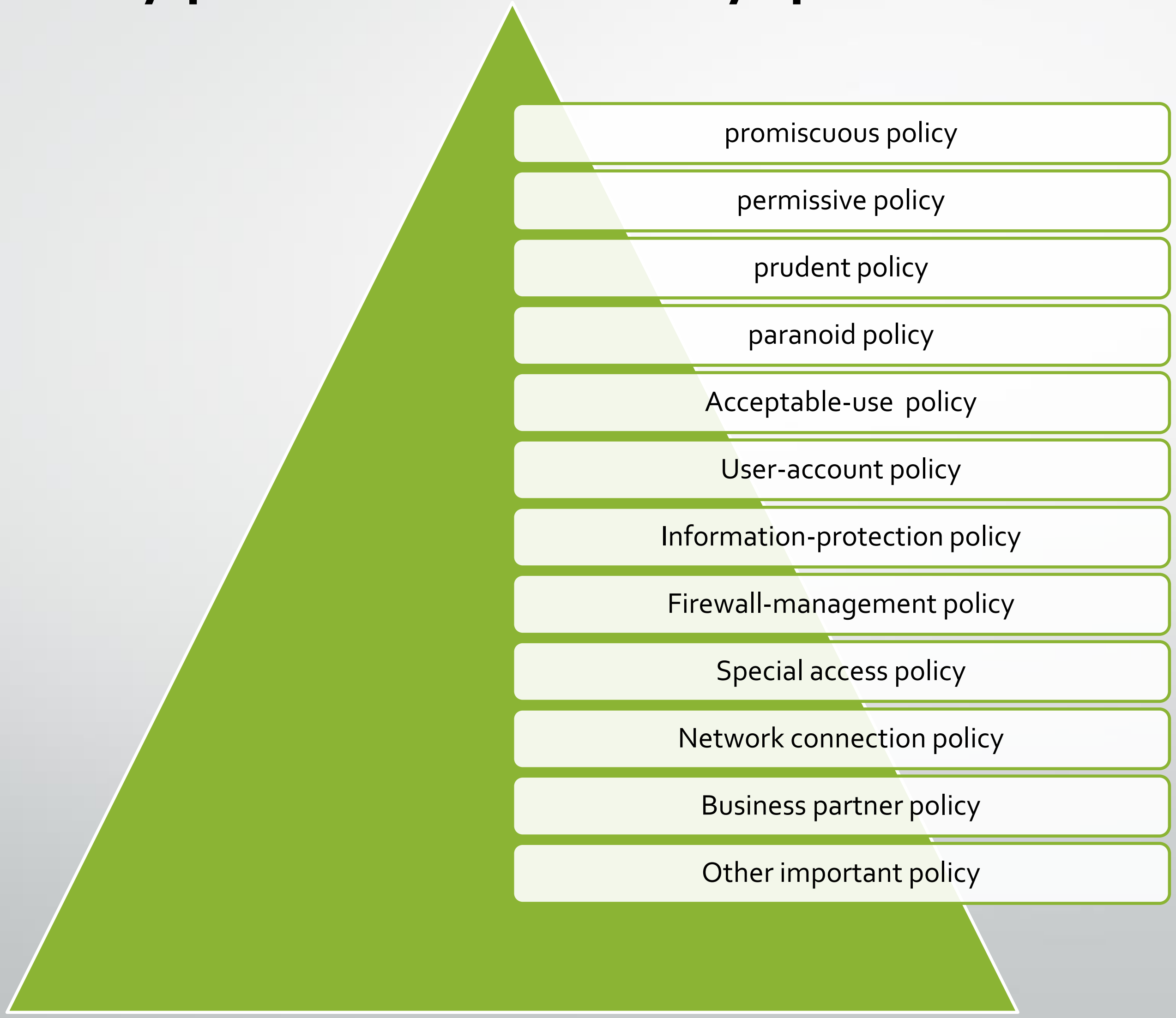
Security concept of operation

- Defines the roles, responsibilities and functions of a security policy

Allocation of security enforcement to architecture elements

- Provides a computer system architecture allocation to each system of the program

Types of security policies



- promiscuous policy
- permissive policy
- prudent policy
- paranoid policy
- Acceptable-use policy
- User-account policy
- Information-protection policy
- Firewall-management policy
- Special access policy
- Network connection policy
- Business partner policy
- Other important policy

Promiscuous policy

- Casual policy
- No restrictions on internet/remote access

Permissive policy

- Known dangerous services/attacks blocked
- Policy begins wide open
- Known holes plugged, known dangers stopped
- Impossible to keep up with current exploits; administrators always play catch-up.

Prudent policy

- Provides maximum security while allowing known but necessary dangers
- All services are blocked, nothing is allowed
- Safe/necessary services are enabled individually
- Nonessential services/procedures that can not be made safe are not allowed.
- Everything is logged.

Paranoid policy

- Everything is forbidden
- No internet connection or severely limited internet usage
- Users find ways around overly severe restrictions

Acceptable use policy

- Should users read and copy files that are not their own but are accessible to them?
- Should users modify files that they have write access to but are not their own?
- Should users make copies of system configuration files(for example, /etc/passwd and SAM) for their own personal use or to provide to other people?
- Should users be allowed to use .rhosts files? Which entries are acceptable?
- Should users be allowed to share accounts?
- Should users have the ability to make copies of copyrighted software?

User account policy

- Who has the authority to approve account requests?
- Who(employees, spouses, children, company visitors, for instance) are allowed to use the computing resources?
- May users have multiple accounts on a single system?
- May users share accounts?
- What are the users rights and responsibilities?
- When should an account be disabled and archived?

Remote access policy

- Who is allowed to have remote access?
- What specific methods(such as cable modem/DSL or dial-up) does the company support?
- Are dial up modems allowed on the internal network?
- Are there any extra requirements, such as mandatory anti-virus and security software. On the remote system?
- May the other members of a household use the company network?
- Do any restrictions exist on what data may be accessed remotely?

Information protection policy

- What are the sensitivity levels of information?
- Who may have access to sensitive information?
- How is sensitive information stored and transmitted?
- What levels of sensitive information may be printed in public printers?
- How should sensitive information be deleted form storage media(paper shredding, scrubbing hard drives and degaussing disks) ?

Firewall management policy

- Who has access to the firewall systems?
- Who should receive requests to make a change to the firewall configuration?
- Who may approve requests to make a change to the firewall configuration?
- Who may see the firewall configuration rules and access lists?’
- How often should the firewall configuration be reviewed?

Special access policy

- Who should receive requests for special access?
- Who may approve requests for special access?
- What are the passwords rules for special access accounts?
- How often are passwords changed?
- What are the reasons or situations that would lead to revocation of special access privileges?

Network connection policy

- Who may install new resources on the network?
- Who must approve the installation of new devices?
- Who must be notified that new devices are being added to the network?
- Who should document network changes?
- Are there any security requirements for the new devices being added to the network?

Business partner policy

- is it mandatory for a company required to have a written security policy?
- Should each company have a firewall or other perimeter security devices?
- How will one communicate(virtual private network over the internet, leased line or so forth)?
- How will access to the partners resources be requested?

Other

- A wireless network policy, which helps to secure wireless networks, includes which devices are allowed to be connected,, what security measures should be followed and so forth
- A lab policy discusses how to protect the internal network from the insecurities of a test lab
- The best option is to keep the test lab on a completely separate internet and without connecting it in any way to the internal corporate network

Basic document set of information security policies

Policy	Description
Information classification	Describes how information should be classified . Should include a data ownership policy and a data treatment table.
Data protection	Covers data protection. How the company will manage personal data and precautions employees should take to avoid infringing on others rights.
Host access control	Describe the- •logon process •Login banners •Password rules •Audit rules •Data roles
Internet usage	Describe acceptable “Netiquette”.

Cont….

Email usage	**Warns users about the dangers of email**
Virus control	Describe the rules for virus protection and tells users what to do if their computers are infected
Backup and data disposal	The backup policy mandates that the system should be backed up when they are in use and that these backups should be tested and protected according to the need of the business. The disposal policy will mandate that; •Disks should be destroyed before disposal •CDs should be sanded and snapped •Tapes should be degaussed
Remote access	How to access the network remotely.
Physical protection	Describes physical portection
Encryption	Describes confidentiality

Cont…

Software lincesing	**Describes use of legal software's**
Acceptable use policy	This document is little different from the rest because it should be educational in its nature. It exemplifies acceptable use of company facilities and IT equipment and describes forbidden activities. Banned behavior tends to include: •Using illegal software •Viewing offensive material •Hacking or virus distribution or otherwise infringing on an individuals right. The big question here is whether to allow or disallow personal use; the latter is becoming increasingly difficult In some legal jurisdictions.

Summary

- Security policy is a set of objectives and rules of behavior for users and administrators
- Prudent policy provides maximum security while allowing know but necessary dangers
- Security policy suggest the safety measures to be followed in an organization
- Security policy implementation follows after building, revision and updating of the security policy.
- A wireless network policy helps to secure wireless networks, including which devices are allowed to be connected, what security measures should be followed
- An email security policy is created to govern the proper usage of corporate emails.

Access control

- Access control is **a data security process that enables organizations to manage who is authorized to access corporate data and resources**. Secure access control uses policies that verify users are who they claim to be and ensures appropriate control access levels are granted to users.

Mandatory access control (MAC). This is a security model in which **access rights are regulated by a central authority** based on multiple levels of security. Often used in government and military environments, classifications are assigned to system resources and the operating system or security kernel.

Discretionary access control (DAC). This is an access control method in which owners or administrators of the protected system, data or resource set the policies defining **who or what is authorized to access the resource**. Many of these systems enable administrators to limit the propagation of access rights

Role-based access control (RBAC). This is a widely used access control mechanism that restricts access to computer resources based on individuals or groups with defined business functions -- e.g., executive level, engineer level 1, etc. -- rather than the identities of individual users. The role-based security model relies on a complex structure of role assignments, role authorizations and role permissions developed using role engineering to regulate employee access to systems.

Rule-based access control. This is a security model in which the **system administrator defines the rules** that govern access to resource objects. These rules are often based on conditions, such as time of day or location. It is not uncommon to use some form of both rule-based access control and RBAC to enforce access policies and procedures.

Attribute-based access control. This is a methodology that manages access rights by evaluating **a set of rules, policies and relationships using the attributes of users, systems and environmental conditions.**

Cybersecurity Audit

- A cybersecurity audit involves a comprehensive analysis and review of the IT infrastructure of your business.
- It detects vulnerabilities and threats, displaying weak links, and high-risk practices.
- It is a primary method for examining compliance.
- It is designed to evaluate something (a company, system, product, etc.) against a specific standard to validate that the exact needs are met.

The Scope of a Cybersecurity Audit

- **Data Security** – involves a review of network access control, encryption use, data security at rest, and transmissions
- **Operational Security** – involves a review of security policies, procedures, and controls
- **Network Security** – a review of network & security controls, SOC, anti-virus configurations, security monitoring capabilities, etc.
- **System Security** – This review covers hardening processes, patching processes, privileged account management, role-based access, etc.
- **Physical Security** – a review that covers disk encryption, role-based access controls, biometric data, multifactor authentication, etc.

Internal vs External Cybersecurity Audit

- External cybersecurity audits are performed by experienced professionals and equipped with appropriate software and tools to perform a thorough audit. The auditors possess an adequate understanding of all security protocols as well as well-trained to detect flaws in your cybersecurity risk management.
- External cybersecurity audits are performed by experienced professionals and equipped with appropriate software and tools to perform a thorough audit. The auditors possess an adequate understanding of all security protocols as well as well-trained to detect flaws in your cybersecurity risk management.
- Outsourcing security audit to the cybersecurity services company has significant value, though it is quite expensive for smaller companies.

What is Authentication?

- Authentication is a term that refers to the process of proving that some fact or some document is genuine. In computer science, this term is typically associated with proving a user’s identity. Usually, a user proves their identity by providing their **credentials**, that is, an agreed piece of information shared between the user and the system.

- **Authentication with Username and Password**
- **Authentication Factors: Something you know, Something you have, Something you are**

-password, OTP, biometric authentication etc

- **From Single to Multi-Factor Authentication**
- **Passwordless Authentication**

- facial recognition

- **Authentication at Auth0**

Biometrics

- Biometrics are body measurements and calculations related to human characteristics. Biometric authentication is used in computer science as a form of identification and access control.

There are two types of biometric systems: Physical biometrics and Behavioral biometrics

- **Physical Biometrics:** With the help of special devices (scanners, sensors, and other readers), a person's biometric data is stored in a database.
- **Behavioral Biometrics:** Handwriting and signature dynamics, voice and speech rhythms, gesture recognition, electronic device usage characteristics through typing speed, the way a person holds a smartphone or tablet, and even the way they walk.

Five Types of Biometric Identification

- **Fingerprint Scanning:** Converting a fingerprint into a digital code with an optical sensor, saving conversion using a linear thermal sensor, and converting a fingerprint with a capacitive authentication sensor.

Advantages of Fingerprint Scanning:

- Fingerprints are unique identifiers specific to the individual.
- Most people are familiar with this authentication method.
- No need to remember complex passwords.
- Fingerprint scanners are relatively cheap and can even be bought on Amazon.

Disadvantages of Fingerprint Scanning:

- Injuries, temporary or permanent, can interfere with scans.
- It is a technology that can be bypassed with methods that copy and replicate fingerprints. It’s hard to copy one’s fingerprint, but it’s not impossible.
- It can be bypassed by using someone else’s finger while they are asleep or unconscious.

Voice Recognition

- Voice biometric authentication technology is widely used in several areas directly related to processing users' voices, such as in call centers.
- Adoption of this biometric technology allows for speeding up of the service, making the work of agents easier, and helping them become more efficient.
- This technology can have many different use cases such as security systems, credit card verification, forensic analysis, and teleconferencing, etc.
- In larger projects, especially when the need to protect confidential information is great, voice identification can be applied with another authentication method such as fingerprint scanning.

Advantages of Voice Recognition:

- No need to remember and then use a password while being authenticated.
- Voice is a natural way of communication and interaction between people.
- It saves time for both users and agents, especially when using passive voice biometrics.
- The voice is a unique feature that is extremely hard to falsify.
- It’s a widely used method that is familiar to users.

Disadvantages of Voice Recognition:

- Users may not understand how their data is stored and have privacy-related concerns.
- Noisy places may prevent successful authentication.
- Severe respiratory illness may decrease the success rate of authentication.

Iris Recognition

- This is how the technology works: First, the pupil is located, followed by detecting the iris and eyelids.
- Next, unnecessary parts such as eyelids and eyelashes are excluded to leave only the iris part, which is divided into blocks and converted into numerical values representing the image.
- Finally, matching with previously collected data is performed using the same methods to verify identity.

Advantages of Iris Recognition:

- Iris is an internal organ that is well protected against damage by a highly transparent and sensitive membrane. Thus, it’s unlikely for minor injuries to influence scanning devices.
- The iris is an invariant organ with a high level of randomness between individuals.
- No need to memorize complicated passwords.

Disadvantages of Iris Recognition:

- Still requires improvements.
- It is a method that requires a short distance between the device and the user's eye.
- In low light conditions, the chances of iris recognition are really poor.

Facial Recognition

- Facial recognition is the automatic localization of a human face in an image or video.
- If necessary, facial recognition technology can be used to confirm a person's identity based on the available data - an image of someone’s face stored in a database as mathematical code. Interest in this technology is high because this method can be applied in videoconferencing.

Advantages of Facial Recognition:

- Requires little interaction with the device.
- It is widely used and people are used to this type of technology.
- Highly effective when combined with other biometric methods.
- No need to memorize complex passwords.

Disadvantages of Facial Recognition:

- Lighting changes can affect the system's performance.
- Facial expressions may change the system's perception of the face.
- The use of facial accessories may make it difficult to recognize the user.
- It may cause embarrassment for some users to have to look at their phone often to unlock it.

Handwriting Recognition

- Dynamic signature verification can be applied in areas requiring workflow automation, such as banking or judicial systems.
- Signature recognition is based on pattern recognition algorithms or mathematical methods of curve analysis, since a set of points can represent a signature.
- Therefore, these systems often use time series decomposition or curve approximation.

Advantages of Handwriting Recognition:

- Signatures were used to confirm identities for centuries. Thus, this technology evokes trust.
- The technology doesn’t require advanced devices to work (touchscreen devices are common these days).
- It’s intuitive and natural and doesn't require much explanation.

Disadvantages of Handwriting Recognition:

- Many people have inconsistent signatures.
- Injuries like broken arms or fingers may make it impossible to use this technology.
- This method is suitable only for low-level security operations.

What Is Deception Technology?

- Deception technology is a cybersecurity defense practice that aims to deceive attackers by distributing a collection of traps and decoys across a system's infrastructure to imitate genuine assets.
- If an intruder triggers a decoy, then the server will log and monitor the attack vectors utilized throughout the duration of the engagement.

Denial of Service (DoS)

- Denial of Service (DoS) is a cyber-attack on an individual Computer or Website with the intent to deny services to intended users.
- Their purpose is to disrupt an organization's network operations by denying access to its users. Denial of service is typically accomplished by flooding the targeted machine or resource with surplus requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.
- For example, if a bank website can handle 10 people a second clicking the Login button, an attacker only has to send 10 fake requests per second to make it so no legitimate users can login.

Ethical Hacking

- Ethical hacking involves an authorized attempt to gain unauthorized access to a computer system, application, or data. Carrying out an ethical hack involves duplicating strategies and actions of malicious attackers.
- This practice helps to identify security vulnerabilities which can then be resolved before a malicious attacker has the opportunity to exploit them.

What is an ethical hacker?

- Also known as “white hats,” ethical hackers are security experts that perform these security assessments.
- The proactive work they do helps to improve an organization’s security posture.
- With prior approval from the organization or owner of the IT asset, the mission of ethical hacking is opposite from malicious hacking.

What are the key concepts of ethical hacking?

- **Stay legal.** Obtain proper approval before accessing and performing a security assessment.
- **Define the scope.** Determine the scope of the assessment so that the ethical hacker's work remains legal and within the organization's approved boundaries.
- **Report vulnerabilities.** Notify the organization of all vulnerabilities discovered during the assessment. Provide remediation advice for resolving these vulnerabilities.
- **Respect data sensitivity.** Depending on the data sensitivity, ethical hackers may have to agree to a non-disclosure agreement, in addition to other terms and conditions required by the assessed organization.

Firewall

- A Firewall is **a network security device that monitors, and filters incoming and outgoing network traffic based on an organization's previously established security policies**.
- At its most basic, a firewall is essentially the barrier that sits between a private internal network and the public Internet.

Five main types of firewall include the following:

1. PACKET FILTERING FIREWALL
2. CIRCUIT-LEVEL GATEWAY
3. APPLICATION-LEVEL GATEWAY (AKA PROXY FIREWALL)
4. STATEFUL INSPECTION FIREWALL
5. NEXT-GENERATION FIREWALL (NGFW)

Packet-filtering Firewalls

- A packet filtering firewall is the most basic type of firewall. It acts like a management program that **monitors network traffic and filters incoming packets** based on configured security rules.
- These firewalls are designed to **block network traffic** IP protocols, an IP address, and a port number **if a data packet does not match the established rule-set.**

Circuit-level Gateways

- Circuit-level gateways are another simplified type of firewall that can be easily configured to allow or block traffic without consuming significant computing resources. These types of firewalls typically operate at the **session-level** of the OSI model by verifying **TCP (Transmission Control Protocol)** connections and sessions. Circuit-level gateways are designed to **ensure that the established sessions are protected.**
- Typically, circuit-level firewalls are implemented as security software or pre-existing firewalls. Like packet-filtering firewalls, these firewalls **do not check for actual data**, although they inspect information about transactions. Therefore, if a data contains malware, but follows the correct TCP connection, it will pass through the gateway. That is why circuit-level gateways are not considered safe enough to protect our systems.

Stateful Multi-layer Inspection (SMLI) Firewalls

- Stateful multi-layer inspection firewalls include both packet inspection technology and TCP handshake verification, making SMLI firewalls **superior to packet-filtering firewalls or circuit-level gateways**. Additionally, these types of firewalls keep track of the status of established connections.
- In simple words, when a user establishes a connection and requests data, the SMLI firewall creates a database (state table). The database is used to store session information such as source IP address, port number, destination IP address, destination port number, etc. Connection information is stored for each session in the state table. Using stateful inspection technology, these firewalls create security rules to allow anticipated traffic.
- In most cases, SMLI firewalls are implemented as additional security levels. These types of firewalls implement more checks and are considered more secure than stateless firewalls. This is why stateful packet inspection is implemented along with many other firewalls to track statistics for all internal traffic. Doing so increases the load and puts more pressure on computing resources. This can give rise to a slower transfer rate for data packets than other solutions.

Application-level Gateways (Proxy Firewalls)

- Proxy firewalls operate at the application layer as an intermediate device to filter **incoming traffic between two end systems** (e.g., network and traffic systems). That is why these firewalls are called **'Application-level Gateways'**.
- Unlike basic firewalls, these firewalls transfer requests from clients pretending to be original clients on the web-server. This protects the client's identity and other suspicious information, keeping the network safe from potential attacks.
- Once the connection is established, the proxy firewall inspects data packets coming from the source. If the contents of the incoming data packet are protected, the proxy firewall transfers it to the client. This approach creates an additional layer of security between the client and many different sources on the network.

Next-generation Firewalls (NGFW)

- Many of the latest released firewalls are usually defined as **'next-generation firewalls'**. However, there is no specific definition for next-generation firewalls. This type of firewall is usually defined as a security device combining the features and functionalities of other firewalls. These firewalls include **deep-packet inspection (DPI),** surface-level packet inspection, and TCP handshake testing, etc.
- NGFW includes higher levels of security than packet-filtering and stateful inspection firewalls. Unlike traditional firewalls, NGFW monitors the entire transaction of data, including packet headers, packet contents, and sources. NGFWs are designed in such a way that they can prevent more sophisticated and evolving security threats such as malware attacks, external threats, and advance intrusion.

Intrusion Detection Systems

- An Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for the harmful activity or policy breaching.
- Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.

Network Intrusion Detection System (NIDS):

Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network. It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks.

Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator. An example of a NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying to crack the firewall.

Host Intrusion Detection System (HIDS):

Host intrusion detection systems (HIDS) run on independent hosts or devices on the network. A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected. It takes a snapshot of existing system files and compares it with the previous snapshot.

If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate. An example of HIDS usage can be seen on mission-critical machines, which are not expected to change their layout.

Protocol-based Intrusion Detection System (PIDS):

Protocol-based intrusion detection system (PIDS) comprises a system or agent that would consistently resides at the front end of a server, controlling and interpreting the protocol between a user/device and the server.

It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accept the related HTTP protocol. As HTTPS is un-encrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.

Application Protocol-based Intrusion Detection System (APIDS):

Application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers.

It identifies the intrusions by monitoring and interpreting the communication on application-specific protocols.

For example, this would monitor the SQL protocol explicit to the middleware as it transacts with the database in the web server.

Hybrid Intrusion Detection System :

Hybrid intrusion detection system is made by the combination of two or more approaches of the intrusion detection system. In the hybrid intrusion detection system, host agent or system data is combined with network information to develop a complete view of the network system.

Hybrid intrusion detection system is more effective in comparison to the other intrusion detection system. Prelude is an example of Hybrid IDS.

Detection Method of IDS:

1. Signature-based Method:

Signature-based IDS detects the attacks on the basis of the specific patterns such as number of bytes or number of 1’s or number of 0’s in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware.

The detected patterns in the IDS are known as signatures. Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system but it is quite difficult to detect the new malware attacks as their pattern (signature) is not known.

2. Anomaly-based Method:

Anomaly-based IDS was introduced to detect unknown malware attacks as new malware are developed rapidly.

In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model.

Machine learning-based method has a better-generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

What is Scanning?

- Scanning is a set of procedures for identifying live hosts, ports, and services, discovering Operating system and architecture of target system, Identifying vulnerabilities and threats in the network. Network scanning is used to create a profile of the target organization.

- Scanning refers to collecting more information using complex and aggressive reconnaissance techniques.

- The attacker has gained valuable insights about the target. But this is not enough, as deeper insights are required.
- Scanning helps in getting more specific information about the target. Web scanners help attackers understand the vulnerabilities in a website, while application scanners look at the application code and the lists of potential vulnerabilities and issues.
- Network scanners help the attacker to perform host discovery, identify ports and services and gain

Incident response

- Incident response is **an organized approach to addressing and managing the aftermath of a security breach or cyberattack**, also known as an IT incident, computer incident or security incident. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs.