UNIT IV

TECHNICAL SECURITY

Security Architecture-Malware Protection

SECURITY ARCHITECTURE:

A cyber security architecture combines security software and appliance solutions, providing the infrastructure for protecting an organization from cyber attacks. The cyber security architecture shouldbe able to adapt to the evolving cyber threat landscape as organizations engage in digital transformation initiatives and expand IT services beyond the traditional perimeter.

A cyber security architecture is the foundation of an organization's defense against cyber threats, and ensures that all components of its IT infrastructure are protected.

Environments that are secured by a cyber security architecture include:

- Cloud
- Networks
- IoT
- Endpoints
- Mobile

Security Architecture Components

According to Internal Auditors, effective and efficient cybersecurity architecture consists of threemajor components. Those are people, processes and tools that work together to protect your company's assets.
To align these components the architecture needs to be driven by your security policy by statingyour security architecture expectation, implementation plan, and enforcement process.

A security policy is a statement that outlines how each entity accesses each other, what operations various entities can carry out, the level of protection that is required for a system as.

The components listed below are part of an effective and carefully planned security architecture:

1. Direction in the area of incident response to threats, disaster recovery, systemsconfiguration, account creation and management, and cybersecurity monitoring.
2. Identity management.
3. Decided inclusion and exclusion of those subject to the domain of thesecurity architecture.
4. Access and border control.
5. Validation and adjustment of the architecture.
6. Training.

Features of Cyber security Architecture

The following are some of the features of cyber security architecture:

- **Network Elements**
- Network nodes like computers, NICs, repeaters, hubs, bridges, switches,routers, modems, gateways.
- Network communication protocols (TCP/IP, DHCP, DNS, FTP, HTTP, HTTPS, IMAP)
- Network connections between nodes using specific protocols
- Network topologies among nodes such as point-to-point, circular, chain, and hybrid.

MALWARE PROTECTION

Malware is a blanket term for viruses, Trojans, and other destructive computer programs threat actors use to infect systems and networks in order to gain access to sensitive information.

Malware *Definition*

Malware (short for "malicious software") is a file or code, typically delivered over a network, that infects, explores, steals or conducts virtually any behavior an attacker wants, because malware comes in so many variants, there are numerous methods to infect computer systems.

Provide remote control for an attacker to use an infected machine.

- Send spam from the infected machine to unsuspecting targets.
- Investigate the infected user's local network.
- Steal sensitive data.

Types of Malware:

Malware is an inclusive term for all types of malicious software. Malware examples, malwareattack definitions and methods for spreading malware include:

Adware – While some forms of adware may be considered legitimate, others make unauthorizedaccess to computer systems and greatly disrupt users.

Botnets – Short for "robot network," these are networks of infected computers under the controlof single attacking parties using command-and-control servers.

Cryptojacking – is malicious cryptomining (the process of using computing power to verify transactions on a blockchain network and earning cryptocurrency for providing that service) that happens when cybercriminals hack into both business and personal computers, laptops, andmobile devices to install software.

Malvertising – Malvertising is a portmanteau of "malware + advertising" describing thepractice of online advertising to spread malware.

Ransomware – Is a criminal business model that uses malicious software to hold valuablefiles, data or information for ransom. Victims of a ransomware attack may have their operations severely degraded or shut down entirely.

Remote Administration Tools (RATs) – Software that allows a remote operator to control a system. These tools were originally built for legitimate use, but are now used by threat actors.

RATs enable administrative control, allowing an attacker to do almost anything on an infectedcomputer. They are difficult to detect, as they don't typically show up in lists of running programs or tasks, and their actions are often mistaken for the actions of legitimate programs.

Rootkits – Programs that provide privileged (root-level) access to a computer. Rootkits varyand hide themselves in the operating system.

Spyware – Malware that collects information about the usage of the infected computer and communicates it back to the attacker. The term includes botnets, adware, backdoor behavior, keyloggers, data theft and net-worms.

Trojans Malware – Malware disguised in what appears to be legitimate software. Once activated, malware Trojans will conduct whatever action they have been programmed to carryout.

Virus Malware – Programs that copy themselves throughout a computer or network. Malware viruses piggyback on existing programs and can only be activated when a user opens the program. At their worst, viruses can corrupt or delete data, use the user's email tospread, or erase everything on a hard disk.

Worm Malware – Self-replicating viruses that exploit security vulnerabilities to automaticallyspread themselves across computers and networks. Unlike many viruses, malware worms do not attach to existing programs or alter files. They typically go unnoticed until replication reaches a scale that consumes significant system resources or network bandwidth.

Types of Malware Attacks

Malware also uses a variety of methods to spread itself to other computer systems beyond aninitial attack vector. Malware attack definitions can include:

- Email attachments containing malicious code can be opened, and therefore executed by unsuspecting users. If those emails are forwarded, the malware can spread even deeper into an organization, further compromising a network.
- File servers, such as those based on common Internet file system (SMB/CIFS) andnetwork file system (NFS), can enable malware to spread quickly as users access and download infected files.
- File-sharing software can allow malware to replicate itself onto removable mediaand then on to computer systems and networks.
- Peer to peer (P2P) file sharing can introduce malware by sharing files asseemingly harmless as music or pictures.
- Remotely exploitable vulnerabilities can enable a hacker to access systems

regardlessof geographic location with little or no need for involvement by a computer user.

How to Prevent Malware:

A variety of security solutions are used to detect and prevent malware. These include firewalls, next-generation firewalls, network intrusion prevention systems (IPS), deep packet inspection (DPI) capabilities, unified threat management systems, antivirus and anti-spam gateways, virtualprivate networks, content filtering and data leak prevention systems.

Malware Detection:

Advanced malware analysis and detection tools exist such as firewalls, Intrusion Prevention Systems (IPS), and sandboxing solutions. Some malware types are easier to detect, such as ransomware, which makes itself known immediately upon encrypting your files.

Other malware like spyware, may remain on a target system silently to allow an adversary tomaintain access to the system. Regardless of the malware type or malware meaning, its detectability or the person deploying it, the intent of malware use is always malicious.

When you enable behavioral threat protection in your endpoint security policy, the Cortex XDRagent can also continuously monitor endpoint activity for malicious event chains identified by Palo Alto Networks.

Malware Removal:

Antivirus software can remove standard infection types and many options exist for off-the-shelf solutions. Cortex XDR enables remediation on the endpoint following an alert or investigation giving administrators the option to begin a variety of mitigation steps starting withisolating endpoints by disabling all network access on compromised endpoints except for trafficto the Cortex XDR console, terminating processes to stop any running malware from continuingto perform malicious activity on the endpoint, and blocking additional executions, before quarantining malicious files and removing them from their working directories if the Cortex XDR agent has not already done so.

Malware Protection:

To protect your organization against malware, you need a holistic, enterprise-wide malware protection strategy. Commodity threats are exploits that are less sophisticated and more easily detected and prevented using a combination of antivirus, anti-spyware, and vulnerability protection features along with URL filtering and Application identification capabilities on thefirewall.