Defense in Depth through Layered Security

Importance of Layered Security for Data Defense and Protection

Cyber Security is explained in terms of CIA Triad. The CIA Triad of Confidentiality, Integrity and Availability is considered as the core underpinnings of Information Security. The CIA triad forms the base unto which different approaches to security build upon. All security access controls and vulnerabilities can be viewed in the light of one or more of these key concepts.

Incidents of massive data breaches have become common and the cost of breaches have reached record high levels. The increase in frequency and sophistication of cyber-attacks becomes more relevant as Government Organizations and Enterprises are increasingly relying on networked computing architectures to maintain consistency of services. Breaches and downtime leading to network outage can impact profitability of businesses and availability of government services.

Confidentiality

Confidentiality measures protect information from unauthorized access and misuse. Most information systems house information that has varying degree of sensitivity. Confidential information often has value and systems are therefore under frequent attack as criminals hunt for vulnerabilities to exploit and subsequently gain access to information. Threat vectors include direct attacks such as stealing passwords and capturing network traffic, and more layered attacks such as social engineering and phishing.

Integrity

Integrity related measures protect information from unauthorized alteration. These measures provide assurance about the accuracy and completeness of data. In maintaining integrity, it is not only necessary to control access at the system level, but to further ensure that system users are only able to alter information that they are legitimately authorized to.

Availability

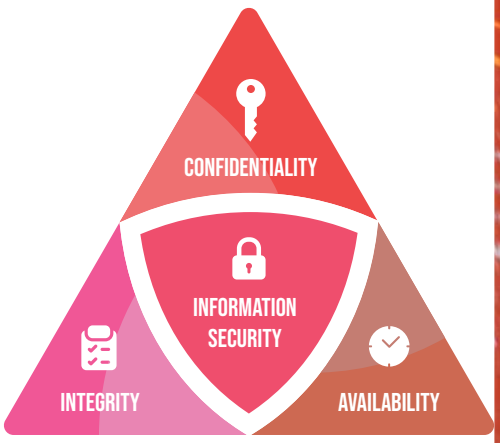
For an information system to be useful it must be available to authorized users. Availability measures provide timely and uninterrupted access to the system. Government, Businesses, Medical, Information and other types of infrastructure are based on the connectivity and availability of resources and services and unavailability can cause chaos and severe damage.

Concept of Layered Security

There are many approaches to deal with the conventional and emerging cyber-threats. Layered approach towards security is one of the most prominent among them.

Layered security is defined as:

Layered security refers to security systems that use multiple components to protect operations on multiple levels and protects the confidentiality, integrity, and availability of the information. The term "layered security" is related to the term "defense in depth", which is based on a slightly broader conception where multiple strategies and resources are used to slow, block, delay, or hinder a threat to subsequently neutralize it.



Abhishek Sisodia
Scientist - B
abhishek.sisodia@nic.in

Layered security is a network security approach that uses several components to protect an organization's operations with multiple levels of security measures. The purpose of layered security approach is to make sure to not leave any single point of failure in the security design. In many scenarios, layered security strategy mitigates the potential weakness of one layer by the strength of corresponding other layers.

Individual layers in a layered security approach focuses threats possessed to confidentiality, integrity and availability. These layers work together to tighten security and by minimizing potential threat surface area for intruders from breaching your network, making it much more robust than relying on a single layer security solution.

The terms "defence in depth" and "layered security" are often used interchangeably, however there is a subtle difference with a lot of overlap. The term "defence in depth" refers to an even more comprehensive security strategy approach than layered security. In fact, one might say that just as a firewall is only one component of a layered security strategy, layered security is only one component of a defence in depth strategy. Défense in depth strategies also include other security preparations which address concerns such as: monitoring, alerting, and emergency response, authorized personnel activity accounting, disaster recovery, criminal activity reporting, forensic analysis, etc. But nonetheless, layered security approach is one of most important components of Défense in Depth strategy.

Areas of Cyber Security Threats

Cyber security threats exist at all the OSI/ISO model layers starting at Layer 7 – the Application Layer because that's the place where users begin by interfacing to the network. For the purposes of creating the most comprehensive cyber security plan we must actually start the application layer and address perhaps the biggest vulnerability in the entire network – the user himself. Users are human and are far more subjected to making errors than computers which will perform the same function the same way every time. Threats at each layer of the ISO-OSI model include:

Application Layer Threats

Examples of application layer attacks include distributed denial-of-service attacks (DDoS) attacks, HTTP floods, SQL injections, cross-site scripting, parameter tampering, and slow-loris attacks. To combat these and more, most organizations have an arsenal of application layer security protections, such as web application firewalls (WAFs), secure web gateway services, and others. According to the experts "The application layer is the hardest to defend". The vulnerabilities encountered here often rely on complex user input scenarios that are hard to define with an intrusion detection signature. This layer is also the most accessible and the most exposed to the outside world because for the application to function, it must be accessible over Port 80 (HTTP) or Port 443 (HTTPS). Other possible exploits at the Application Layer include viruses, worms, phishing, key loggers, backdoors, program logic flaws, bugs, trojan horses and ransomware.

Presentation Layer Threats

The most prevalent threats at this layer are malformed SSL requests. Knowing that inspecting SSL encryption packets is resource intensive, attackers use SSL to tunnel HTTP attacks to target the server. Mitigation plans should include options like offloading the SSL and inspecting the encrypted application traffic for the signs of attacks traffic or violations of policy at an applications delivery platform and subsequently encrypting it after the process of inspection is complete.

Session Layer Threat

DDoS-attackers exploit a flaw in a Telnet server running on the networking devices like switches, rendering Telnet services unavailable. Thus, it becomes important that networking hardware is regularly patched for such vulnerabilities, proper access and session restriction policies are configured and firmware is kept up-to-date

Transport Layer Threats

Transport Layer Security (TLS) is used to secure all communications between their web servers and browsers regardless of whether sensitive data is being transmitted. TLS is a cryptographic protocol that provides end-to-end communications securely over networks and is widely used for internet communications and online transactions. It is intended to prevent eavesdropping, tampering and message forgery. Common applications that employ TLS include Web browsers, instant messaging, email such as Outlook and voice over IP.

Network Layer Threats

Routers make decisions based on layer 3 information, hence the most common network layer threats are generally router-related, including information gathering, sniffing, spoofing, and distributed denial of service (DDoS) attacks in which multiple hosts are enlisted to bombard a target router with requests to the point where it gets overloaded and cannot accept genuine requests.

The most effective protection is achieved by consistently observing best practices for router, firewall and switch configurations. At the router itself it is important to constantly assure that the router operating system is up to date on all security patches, packet filtering is kept enabled and any unused ports are blocked, unused services, and interfaces are disabled. Logging should be enabled, and regular auditing of any unusual activity should be conducted.

Data-Link Layer Threats

The data link layer provides reliable transit of data across a physical link. The data link layer is concerned with physical addressing, network topology, network access, error notification, ordered delivery of frames, and flow control. Frame-level exploits and vulnerabilities include sniffing, spoofing, broadcast storms, and insecure or absent virtual LANs (VLANs, or lack of VLANs). Network interface cards (NICs) that are misconfigured or malfunctioning can cause serious problems on a network segment or the entire network.

Port security is important to tackle Address Resolution Protocol (ARP) spoofing, Media Access Control (MAC) flooding or cloning, Port Stealing, Dynamic Host Configuration Protocol (DHCP) Attacks, layer 2-based broadcasting or Denial of Service Attacks. Switches should be configured to limit the ports that can respond to DHCP requests, static ARP should be implemented and Intrusion Detection Systems (IDS) should be installed.

Physical Layer Threats

The copper & fiber-optic cables that connect everything together create the actual network that everything else uses. Most threats at this layer involve interruption of the electrical signals that travel between network nodes including the physical cutting of cables, natural disasters that bring flood waters which can cause short-circuits, or other human vandalism. Many organizations mitigate these failures by bringing in multiple circuits to the internet.

A superior strategy is the placement of all network core elements such as servers and storage at multiple redundant cloud data centers so that services are available at all the times.

Functional Aspects

An analogy can be drawn between layered approach to security and physical security at an airport. Just like multiple checkpoints at an airport serve different purpose, different layers of security also prevent different type of cyber threats. What layers of security are used in practice may vary from implementation to implementation, but most common ones are:

Network Perimeter Defense

Perimeter defense involves firewalls, intrusion detection and prevention systems, and DMZs. Network Perimeter defence separates an organization's network from External network and prevents unauthorized access to this network. Its components include:

Firewall: Firewall is an essential part of any network security; a firewall stands as the main barrier between the organization's internal secured network and external network. While some firewalls are basic, others can be highly complex and sophisticated like Next Generation Firewalls and Unified Threat Management devices.

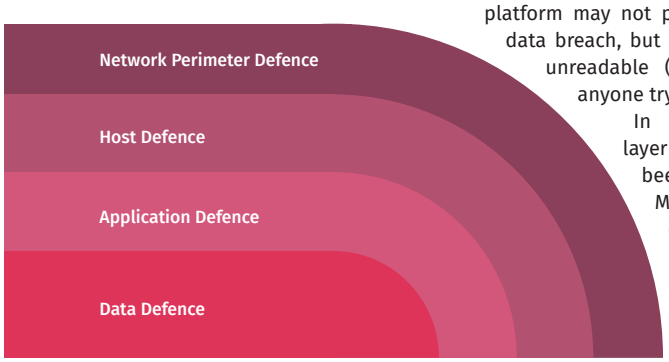
Intrusion Detection and Prevention: This system is designed to monitor intrusions and prevent threats from entering organisation network. The system monitors organisation network continuously and scans the traffic for possible risk to gather more information and

administer the proper preventative actions. This system can be used to identify violations against access rules and policies It is also capable of defending against zero-day attacks.

De-Militarized Zones (DMZ): The purpose of DMZ is to enable access to resources from the untrusted network while keeping the system or host on an organization's internal private network secure. Resources that are commonly placed within the DMZ are Mail servers, FTP servers, Web servers, DNS servers and VoIP servers.

Host Defence

Host defence comprises of End Points and Anti-malware/Anti-virus solutions for End User Protection. Whether users use desktop PC's, laptops, iPads, tablets, or any other devices, it is critical to mitigate the risk of attacks which can find their way into an organisation's network by means of the end point/end user vector. Endpoint security controls protect the connection between devices and the internal network of the organisation. It also protects the user data and resources along with the protecting other hosts from the compromised ones by blocking lateral spread of malware within the organisation's secured network.



Application Defence

Application defence is the process of developing, adding, and testing security features within applications to prevent security vulnerabilities against threats such as unauthorized access and modification. It involves security measures at the application level that aim to prevent data or code within the app from being stolen, altered or hijacked. It encompasses the security considerations that happen during application development and design, but it also involves systems and approaches to protect apps after they get deployed like Authentication, Authorization, Encryption, Application security testing, etc.

Data Defence

Data defence include measures to protect the storage and transfer of data. Different methods include:

Email Filtering: Organisations communicate heavily through email, and cyber attackers make continuous efforts to exploit this dependency. Often, end point/end user protection is not enough to prevent someone from opening infected emails and attachments. Filtering emails at the gateway can reduce the risk of infections and data breaches.

Email Encryption: Once an email leaves server, it can be intercepted by attackers. If there is any sensitive information within the email, there can be a potential for a breach of data. With email encryption, the email and its data are altered into a non-readable and incomprehensible format.

Data Encryption: Like email encryption, data encryption protects information from unauthorized access even in the event of any type of breach. Using an effective data encryption platform may not prevent the occurrence of a data breach, but it virtually renders the data unreadable (and therefore useless) to anyone trying to access it.

In current times, one more layer of Mobile security has been added to the strategy. Mobile workplaces and virtual offices are becoming the norm, especially due to the growing work-from-home culture in the wake of the COVID pandemic. Mobile devices can increase the risk of security breaches which can lead to disruption of operations, data leaks, compromised information, financial losses, unavailability of services, etc. Thus, mobile device management becomes a necessity to ensure the safety and security of the equipment as well as the data and proprietary information for employees working from home and off-site locations. Organisations must make sure that they can encrypt, secure and remotely remove sensitive data and information that could fall into the wrong hands.

Benefits of Layered Security

The key benefit of layered security strategy is that it provides measures corresponding to protection, detection, and response. Layers are beneficial for many reasons. Each layer provides an additional level of defence so that with each extra layer of security that can be added, it becomes more challenging to find ways to infiltrate the system. While each layer in and of itself is not an adequate defence mechanism, layering them together improves each one's efficiency until the last layer nearly completely blocks out the hacker's ability to gain access. Instead of trying to rely on just one or two levels of defence, like access cards and two-step identification, multiple layers of security will lower the risk of a breach and make it easier to respond to legitimate inquiries and requests.

With a layered defence approach, several things happen. First, threats that are detected early are eliminated so that they won't pose a threat or be able to block authentic attempts to enter the system. The next thing to happen is that if a suspected data packet or email enters the system and is picked up as a threat, but clarification is needed, it is sent to an area where it can be easily verified. This rapid capture and validation process means less downtime and allows organisation to continue to be productive. It also eliminates the need for a security administrator to have to go into the system to sanitize an item. The right defence at the right time within a layered cyber security program offers an organization a chance to continue to work at full speed while defence mechanisms are in place and taking care of security.

Layered defence approach also reduces false positives that may prevent an organisation from maintaining interaction with legitimate contacts, while at the same time helping improve organisational visibility. By establishing a verified pathway that goes from the network to the server following a defined set of points that lie in between, any type of threat is detected much easier and eliminated without slowing down operations. The layered security concept creates an interwoven network of protection that prevents unwanted intruders from exploiting the existing vulnerabilities (or even lingering for long periods of time) within the system.

Layered approach provides multi-levels of defence that both identifies and eliminates threats on many different levels. With each added layer, it compounds level of protection until a wall of security is created that is almost impenetrable. The increased risk of loss associated with cyber-attacks cannot be denied, so it's vital that a security approach is followed which takes many different types of threats into consideration and deals with each one quickly and efficiently.

Conclusion

Strengthening the cyber security infrastructure of the country has become imperative with Government of India launching several initiatives for efficient delivery of services to citizens. The country is consistently improving the ranking in Global Cyber Security Index released by International Telecommunication Union (ITU). Continuous efforts are needed to further improve this posture. In a scenario where Governments and corporates are facing frequent data breaches, layered security has become the norm of the day to minimize the conventional as well as the emerging threats.

For further information, please contact:
Abhishek Sisodia
Scientist - B
National Informatics Centre, A-Block
CGO Complex, Lodhi Road
New Delhi - 110003
Email: abhishek.sisodia @nic.in, Phone: 011-24305865