Introduction to Cyber Security

Review

- Vulnerability
- Threat
- Attack
- Risk
- Malwares
- Security functional requirements

Module 2

Security Layers

Topics

- Human factors in cyber security,
- Perimeter Security,
- Network Security,
- Endpoint Security,
- Application Security,
- Data Security,
- Privacy.

Introduction

- The increased frequency of high-profile breaches and the corresponding rise of new and expanded regulatory compliance requirements is putting enormous pressure on IT departments to assure their corporate executives that business-critical systems and data are secure.
- Improving confidence in one's IT security posture requires a solid understanding of all potential vulnerabilities as well as the most effective best practices and technologies in order to minimize the possibility of a breach.

What is Layered Security?

- Reports of massive data breaches have become common-place, and the average cost of breaches have reached record levels.
- In fact, 60% of SMBs who were victims of cyber attacks did not recover and shut down within 6 months.
- Keeping your business protected against cyber attacks is a challenge, but we can alleviate a lot of risk by adopting a layered security approach.
- According to Techopedia, layered security is defined as:

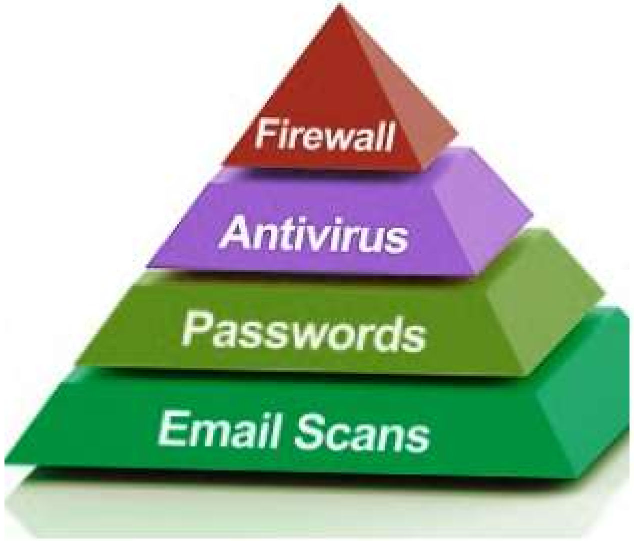
Layered security refers to security systems that use multiple components to protect operations on multiple levels or layers.

Contd…

- The purpose of a layered security approach is to make sure that every individual defense component has a backup to counter any flaws or gaps in other defenses of security.
- Individual layers in a multi-layered security approach focuses on a specific area where malware could attack. These layers work together to tighten security.

The Importance of Layered Security Architecture

- The need to guarantee the security of different network architectures becomes predominant.
- In today’s environment, breaches, bottlenecks or downtime leading to the slowing or stopping of network activity can mean the difference between economic prosperity and collapse.
- Security professionals have been preaching the benefits of a “layered” approach to network defense.



Defense In Depth

- The layered approach to network security is based on the concept of “defense in depth”.
- A vaguely cool and military-sounding phrase which simply means that since any barrier you put up to guard against something may one day be breached.
- It is a good idea to have several barriers so that anyone attacking you has a lot more work to do.
- In terms of security modeling, these barriers translate into a set of layers which make up a complex and protective “skin” around the network.
- Each layer is dedicated to a specific aspect of the network, and each has its own set of protections and security controls.

Physical Layers

- These layers deal with the first interface between humans and machines.
- The three-dimensional barriers that control access to the sites where networks are housed, set hardware in its appointed place, and ensure the physical integrity of the connections between different network components.
- Provision of surveillance cameras or CCTV, security guards and patrols, turnstiles and metal detectors, etc.
- The physical integrity of network elements may be maintained through proper wiring, connections, and hardware configuration, isolation of critical components, and environment controls like cooling and ventilation.

Electronic Layers

- Closely associated with the physical layers (and considered by some as part of them), protocols like Ethernet, Frame Relay, and PPP are concerned with sending bits of data using various communication mechanisms via analog and digital pathways.
- Unauthorized users must be prevented from gaining access to these modes of transmission.
- Access control measures should be put in place to govern this, as well as surveillance and warning systems to monitor this access and give alerts in the event of any breaches.

Procedural Layers

- Procedural layers are made up of the policies and best practices governing a system’s IT management and security protocols.
- These would include

✓ drawing up of rules to determine access rights,

✓ the configuration of firewalls or IDSs,

✓ establishment of schedules for updates, maintenance, and patch management.

Network Security

- This layer comprises the actual software and hardware dedicated to protecting the network in part or whole.
- Protection here extends from enabling the on-board security features of routers and switches to the installation and configuration of firewalls, IPS and IDS.
- Defense in depth layering is further enhanced by dividing the network into segments or zones, each with its own requirements for establishing domains of trust and security access.
- This approach also makes it easier to monitor and manage data traffic on the network.

Computer Hardening

- Exploits targeting specific software vulnerabilities (in both operating systems and working applications) are a favored tool of cyber-criminals.
- Computer hardening aims at making systems proof against such attacks.
- Tools and methods include:

➢ Anti-virus and anti-malware applications.

➢ Whitelisting of approved applications and workloads.

➢ Endpoint security measures and Host Intrusion Detection Systems (HIDS).

➢ The removal of redundant or unused applications, services, and protocols.

➢ Effective management of ports.

Application Security

- Best security practices should be followed with control system applications, like a Role Based Access Control System that bars access to critical process functions and forces user authentication via password, token, or some other protocol.
- The pre-testing of patches.
- Verification of the authenticity of patches.

Device Hardening

- This layer of protection derives from the simple act of changing the default settings on system hardware.
- Measures would include resetting of passwords, and the reconfiguration of security settings on firewalls, switches, routers, and other embedded devices.

Multiple Levels of Defense

- Potential Internet security risks can occur at a variety of levels as given below:

✓ System level security

✓ Network level security

✓ Application level security

✓ Transmission level security

Contd…

- **System Level Security:** refers to the architecture, policy and processes that ensure data and system security on individual computer systems.
- **Network level security**

✓ It measures control access to your operating system and other network systems.

✓ A firewall is the most common means for providing network security.

✓ Network security scheme needs to outline what security measures our ISP provides, such as filtering rules for the ISP router connection and public Domain Name System (DNS) precautions.

Contd…

- **Application level security**

✓ It measures control how users can interact with specific applications.

✓ Configure security settings for each application.

- **Transmission level security**

✓ It protects data communications within and across networks.

✓ When we communicate across an untrusted network like the Internet, we cannot control how our traffic flows from source to destination.

✓ It protects your data as it flows between the other security level boundaries.

Types of Security Layers

- **Firewall/ Unified Threat Management (UTM):** An essential part of any network security, a firewall or UTM stands as the main barrier between your network and cyberspace.
- **End Point / End User Protection:** Securing endpoints or entry points of end-user devices such as desktops, laptops, and mobile devices from being exploited by malicious actors.
- **Email Filtering:** Businesses communicate heavily through email, and cyber thieves are keenly aware. Often time, 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.

Contd…

- **Email Archiving:** Duplicate emails, duplicate attachments, people saving every email they get. Email Archiving can solve these problems while also improving corporate email searching and reducing data storage needs and costs.
- **Email Encryption:** Once an email leaves a server it can be fair game for anyone trying to intercept. If there is sensitive information within the email, there is a potential for a breach of data. With email encryption, the email and its data are altered into a non-readable format.
- **Web Filtering:** The Internet is a great tool but is also a place where cyber criminals prey on unprotected web surfers. Ensuring users utilize their time effectively and are not going to websites which pose a security threat.

Contd…

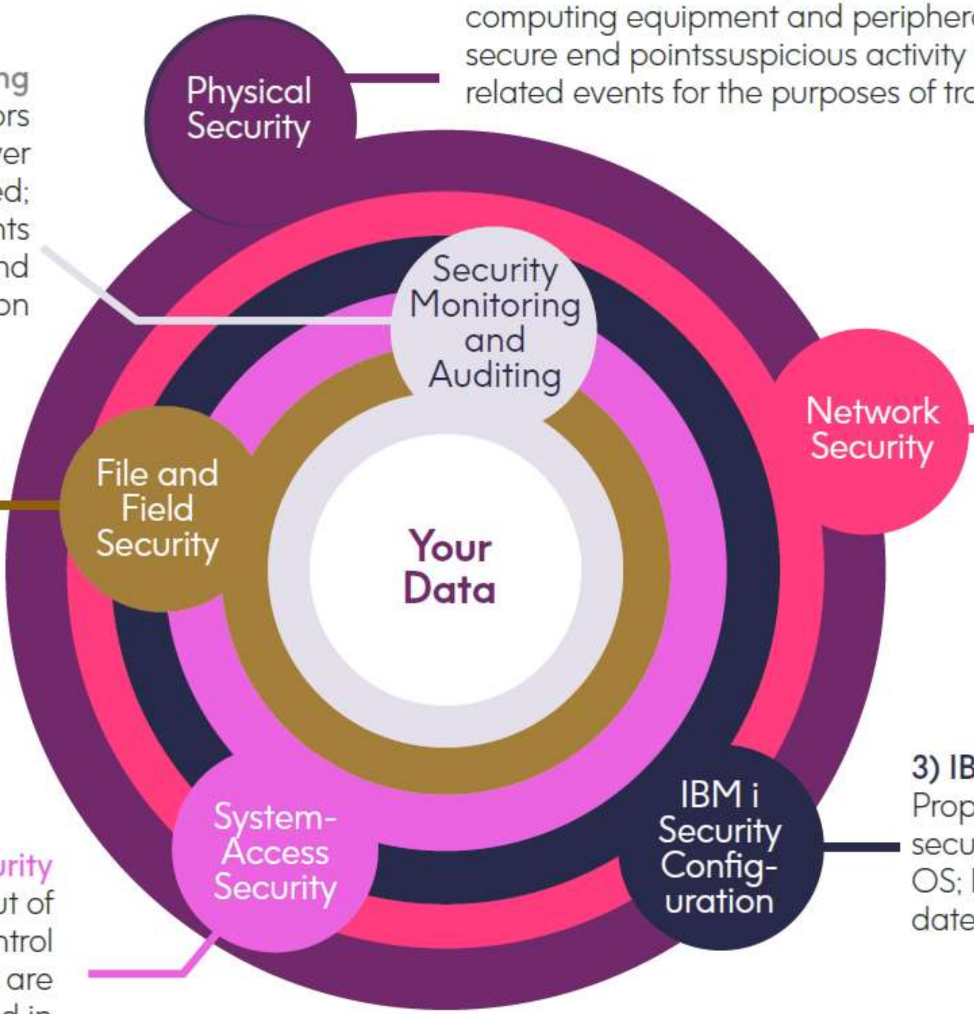
- **Data Encryption:** Similar to email encryption, data encryption protects data from breaches even in the event of a cyber-attack. Using an effective data encryption platform may not prevent the occurrence of a data breach, but it virtually renders the data unreadable to anyone trying to access it.
- **Mobile Device Management (MDM):** MDM keeps your business data protected and ensures your company retains control over confidential information. If a mobile device is lost or stolen, MDM can remotely lock and wipe all data. Remote locking and wiping capabilities enable companies to keep devices and data secure.
- **Mobile Security:** Mobile devices can leave you at increased risk for data breaches. Make sure your business can encrypt, secure, and remotely remove sensitive data and information that could fall into the wrong hands.

The Essential Layers of IBM i Security

- These layers cover physical devices, networks, configuration of the IBM i OS, access to systems, protection of data at the file and field level, and monitoring and auditing of systems.
- The reason it's particularly helpful to view these security categories as "layers" is that, to some extent, each category overlaps with the others to provide multiple lines of defense.
- In other words, should one security layer be somehow compromised, there's a good chance that another layer will thwart a would-be intruder.

The Essential Layers of IBM i Security: Why a Comprehensive Protection of Systems and Data Requires Multiple Lines of Defense, White Paper, Precisely

Layers of IBM i Security



1) Physical Security
Control access to computer rooms and data centers; ensure computing equipment and peripherals cannot be tampered with; secure end pointssuspicious activity is detected; log all security-related events for the purposes of tracking and documentation

2) Network Security
Implement intrusion prevention and detection technologies; group and protect related resources within network segments; encrypt network traffic

3) IBM i Security Configuration
Properly configure necessary security settings within the IBM i OS; keep the OS and PTFs up to date; closely manage user profiles

4) System-Access Security
Keep unauthorized users out of your IBM i; maintain tight control over what authorized users are able to do once logged in

5) File and Field Security
Ensure sensitive data cannot be seen by unauthorized individuals, whether internal or external

6) Security Monitoring and Auditing
Automatically alert administrators and security officers whenever suspicious activity is detected; log all security-related events for the purposes of tracking and documentation

Physical Security

More than just controlling access to computer rooms and data centers, a thorough physical security plan is required to protect the computing environment from theft, misuse, and intentional or accidental tampering.

1. **Servers and storage devices:** Lock into place all servers and storage devices, lock front-panel covers to prevent intentional or accidental changes, and secure power and other cabling to prevent easy disconnection.
2. **Network devices:** Lock into place physical firewalls, routers, switches, and other network devices; ensure power and other cabling can't be easily disconnected; watch for unauthorized configuration changes to network equipment, including covert installation of "sniffing" equipment; and use proper encryption for wireless networks (WPA, WPA2, etc.).
3. **Peripheral devices:** Keep within secure areas all printers and fax machines that output sensitive information.

Contd…

4. **End-point devices —** Educate employees on how to safely use desktops, laptops, and mobile devices, including taking care that these devices aren't lost or stolen. If a device, however, is lost, stolen, or simply repurposed, IT staff needs the ability to locally or remotely execute a secure-wipe process. Of course, end-point devices need to be kept up to date with anti-virus, anti-malware, and anti-ransomware protection.

Network Security

The networks to which an IBM i is connected must be carefully secured, and if any of these networks are connected to the Internet, extra vigilance is required as Internet-connected networks often see thousands of access attempts each day by bots, sniffers, and hackers.

1. **Firewalls —** By examining the flow of data entering a network, firewalls prevent unauthorized traffic by allowing only network traffic that meets predefined firewall rules.
2. **IDS and IPS -** These technologies go beyond traditional firewall capabilities by analyzing traffic within the network itself for suspicious patterns of activity and then triggering alerts when such activity is detected. IPS goes a step further than IDS by acting to prevent the suspicious activity from affecting the network.

Contd…

3. **Network segmentation —** A network-security best practice is to **avoid** putting all IT assets together within a single network. By grouping together within each network only the systems and components that are related to one or more specific applications would be compromised.

4. **Encryption of network data —** Any data that is sent across a network must be encrypted to prevent passwords and other sensitive information from being read "in the clear."

IBM i Security Configuration

Foundational to sound IBM i security is the proper configuration of the IBM i OS and related resources, as well as keeping OS versions and PTFs up to date.

1. **System values settings**
2. **IBM i server-configuration settings —** review all IBM i servers and deactivate any that aren't needed.
3. **Controlling access to System Service Tools (SST) —** special care should be taken when giving users SST access.
4. **User authority settings**
5. **Staying current on OS releases and PTFs**

System-Access Security

It helps keep unauthorized people out of IBM i environments while maintaining tight control over what authorized users are able to do once logged in.

1. **Password management —** Weak passwords and dormant user profiles pose a significant security vulnerability. Effective password management system is needed.
2. **Multi-factor authentication -** In instances where users need to access IBM i environments containing especially sensitive data, third-party technologies can be implemented that require two or more identifying factors from users before access is granted.
3. **Network-access control —** Unauthorized access via sockets and network protocols (e.g., ODBC, FTP, DRDA, etc.) can be prevented through the use of rules-based exit programs that cover network and socket exit points.
4. **Command control —** In addition to normal IBM i OS object security controls, third-party solutions provide rules-based exit programs (trigged by command-specific exit points) that give administrators a more granular approach to locking down commands.

File and Field Security

Numerous regulations require companies in various industries to protect personally identifiable information (PII), personal health information (PHI), personal credit card information, and other sensitive data from being exposed. The following strategies and technologies are key to protecting files and data on the IBM i.

1. **Object-level authority management:** Sensitive file should be protected from public access. Designated users can then be given specific authority to access these files through private authority.
2. **Row and Column Access Control (RCAC):** prevent selected users from viewing specified rows in a file and/or data in particular columns.
3. **File-access protection:** Building upon object-level authority management, various exit points can be used with rules-based exit programs to further control access to files in very specific ways.

Contd…

4. **Encryption:** Convert the data into an unintelligible format using Encryption techniques. Encryption requires the careful management of encryption keys to ensure they don't fall into the wrong hands.

- ✓ **Data at Rest:** Third-party encryption solutions can encrypt sensitive data on the IBM i—such as credit card numbers—at the field level within databases. Technologies are also available that encrypt backup media and disk drives.
- ✓ **Data in motion:** TLS 1.2 or greater must be used to encrypt application data sent across networks. In addition, when entire files containing sensitive information need to be sent between systems or entities via FTP, they should always be encrypted, both during transit and when transfer files reside within send/receive staging areas.
- ✓ **Date in use:** Restrict access by user role, limiting system access to only those who need it.

Contd…

5. Tokenization of field data: An alternative method of shielding sensitive data within applications and on printouts is to replace this data with non-sensitive substitute values called tokens. Third-party tokenization solutions utilize a database called a token vault (residing on a different server) to store both the sensitive data and information about the relationship between it and its replacement token.

- ✓ Tokenization is often used to replace credit card numbers, social security numbers, and other personally identifiable information.

6. **Anonymization:** Although similar to tokenization solutions, third-party anonymization solutions differ by eliminating the use of a token vault, thus permanently replacing sensitive data with a substitute value and making the original data unrecoverable. Anonymization is best utilized when production data is needed for development or test environments.

Security Monitoring and Auditing

While all of the previous layers of security address prevention, this security layer focuses on implementing functions that log security-related events for the purposes of tracking, documentation, and to automatically alert administrators and security officers whenever suspicious activity is detected.

1. **System-audit journaling:** When properly activated and managed, the system-auditing functions provide the ability to monitor and track system, object, and security configuration changes.
2. **File journaling:** Another important aspect of auditing is the ability of file journaling to track and monitor any changes made to sensitive data stored in either Db2 (*FILE) or stream file (*STMF) objects.

- ✓ With file journaling activated, whenever users or applications make a change to data within the designated files, a journal entry is written to record the change.
- ✓ The combination of system-audit journaling and file journaling can provide a complete audit trail of file-access and data-change activity

Contd…

3. Monitoring database-read activity: In situations where it is important for administrators and security officers to know if a user accessed and viewed particularly sensitive data— regardless if the data was changed—third-party technologies exist that can record these activities, complete with a snapshot showing the precise data the user viewed.

4. Analyze and report on journaled information and generate alerts: Once journaling is activated, it is important to have the ability to search for specific events, create reports, and set up alerts. Because information captured by journaling is recorded in a cryptic format, third-party solutions exist that make these important tasks significantly easier.

5. Save journaled data for compliance: All logged information from both the system-audit journal and file journaling is kept within objects called journal receivers, which must be regularly saved and archived in a secure location.

6. Forward journaled data to a SIEM solution: For companies that utilize a security information and event management (SIEM) solution, third-party tools are available that filter and format journaled data for integration with a SIEM.