Agenda

- Review: Tenets of Information Systems Security
- The Seven Domains of a Typical IT Infrastructure

Tenets of Information Systems Security

- Confidentiality - only authorized users can view information
- Integrity - only authorized users can change information
- Availability - information is accessible by authorized users whenever they request the information

On January 17, 2017, in one of his final acts before leaving office, President Barack Obama commuted Chelsea Manning's sentence. Among the three tenets of information system security, Chelsea Manning was sentenced to serve 35 years in prison because of her violation of __?

On January 17, 2017, in one of his final acts before leaving office, President Barack Obama commuted Chelsea Manning's sentence. Among the three tenets of information system security, Chelsea Manning was sentenced to serve 35 years in prison because of her violation of __?

Assigned in 2009 to an Army unit in Iraq as an intelligence analyst, Manning had access to classified databases. In early 2010, she leaked classified information to WikiLeaks. -wikipedia

Example: Twitter

- Confidentiality: If Jidong blocked Selena Gomez on twitter, then she should not be able to view his tweets when she logged in on Twitter; if she is still able to view his tweets, then it means Twitter fails to guarantee confidentiality for its users.

Example: Twitter

- Integrity: If Jidong tweeted that "Selena Gomez's music is great!", and someone, without Jidong's authorization, somehow changed it to the following, then it means, Twitter fails to provide integrity for its users.

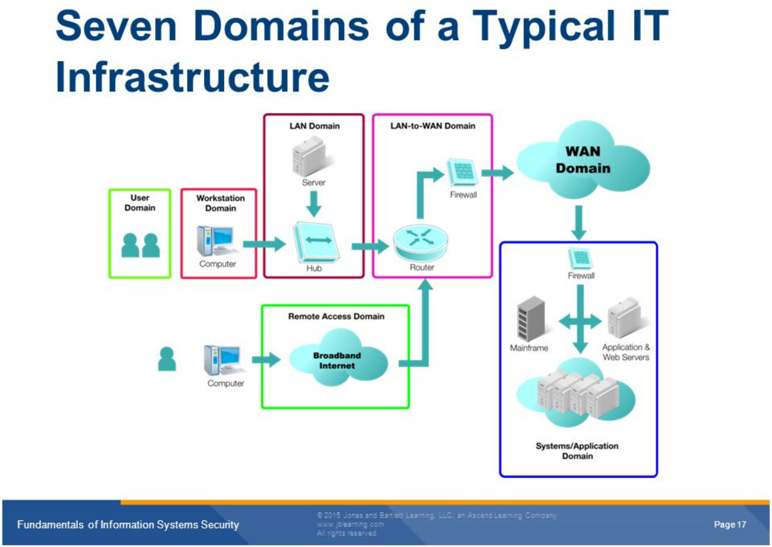
Example: Twitter

- Availability: If Selena Gomez knows her username/password - not hacked or changed by Jidong, and her network connection is okay, but she simply can't access her Twitter account, then it means Twitter fails to provide availability for its users.

Terminology

Defense in Depth: an information assurance (IA) concept in which multiple layers of security controls (defense) are placed throughout an information technology (IT) system. Its intent is to provide redundancy in the event a security control fails or a vulnerability is exploited that can cover aspects of personnel, procedural, technical and physical for the duration of the system's life cycle. -wikipedia
The idea behind the defense in depth approach is to defend a system against any particular attack using several independent methods. It is a layering tactic, conceived by the National Security Agency (NSA) as a comprehensive approach to information and electronic security. - wikipedia

The Seven Domains of a Typical IT Infrastructure



Seven Domains of a Typical IT Infrastructure

Fundamentals of Information Systems Security

Page 17

image source: Jones and Bartlett Learning, LLC

The Seven Domains of a Typical IT Infrastructure

- User - people who access an organization's information system
- Workstation - a desktop computer, laptop, or any other device that connects to your network
- LAN - a collection of computers connected to one another or to a common connection medium
- LAN-to-WAN - where the IT infrastructure links to a wide area network and the Internet
- WAN - connects remote locations
- Remote Access - connects remote users to the organization's IT infrastructure
- System/Application - holds all the mission-critical systems, applications, and data.

Risks, threats, vulnerabilities and mitigation plans for the User Domain

- Lack of user awareness
- Security policy violations - place employee on probation, review acceptable user policy and employee manual, discuss during performance reviews.
- Attacks on the organization or acts of sabotage by disgruntled employees - track and monitor abnormal employee behavior, and use of IT infrastructure during off-hours.
- User insertion of (infected) CDs and USB drives with personal photos, music, and videos. - disable internal CD drives and USB ports, enable automatic antivirus scans for inserted media drives, files and email attachments.

Risks, threats, vulnerabilities and mitigation plans for the Workstation Domain

- Unauthorized access to workstation - enable password protection on workstations for access. enable auto screen lockout for inactive times. disable system admin rights for users.
- Desktop or laptop computer operating system software vulnerabilities
- Infection of a user's workstation or laptop computer by viruses, malicious code, or malware.
- Employees and users want to use their own smartphone or tablets, driving the need to support Bring Your Own Device BYOD - develop a BYOD policy and procedure to allow employees to use their personal smartphones or mobile devices.

Risks, threats, vulnerabilities and mitigation plans for the LAN Domain

- Unauthorized access to LAN - making sure wiring closets, data centers, and computer rooms are secure. Do not allow anyone access without proper ID.
- LAN server operating system software vulnerabilities
- Unauthorized access by rogue users on WLANs - require a password for wireless access.
- Compromised confidentiality of data transmissions via WLAN - encryption.

Risks, threats, vulnerabilities and mitigation plans for the LAN-to-WAN Domain

- Unauthorized network probing and port scanning - disable ping, probing, and port scanning on all exterior IP devices within the LAN-to-WAN domain.
- Denial of service (DoS)/distributed denial of service (DDoS) attacks on external public-facing IP's and Internal link - upstream Internet service providers (ISP) must participate in DoS/DDoS attack prevention.
- IP router, firewall, and network appliance operating system software vulnerabilities
- IP router, firewall, and network appliance configuration file errors or weaknesses

Risks, threats, vulnerabilities and mitigation plans for the WAN Domain

- Most Internet traffic sent in cleartext
- Email of Trojan, worms, and malicious software by hackers, attackers, and perpetrators - scan all email attachments, isolate unknown file attachments until further security review is conducted.
- Maintaining high WAN service availability

Risks, threats, vulnerabilities and mitigation plans for the Remote Access Domain

- Brute force USER ID and password attacks
- Unauthorized remote access to IT systems, applications, and data. - two factor authentication.
- A mobile worker's laptop is stolen - encrypt data on the hard drive.

Risks, threats, vulnerabilities and mitigation plans for the System/Application Domain

- Unauthorized access to data centers, computer rooms, and wiring closets
- Downtime of servers to perform maintenance
- Data breach where private data of individuals are compromised
- Loss or corruption of data

Hands-on

Network protocols use port numbers to identify the application or function; these port numbers function like channels on a TV, dictating which station you're watching. When a packet is sent via TCP or UDP, its port number appears in the packet header. Because many services are associated with a common port number, knowning the port number essentially reveals what type of packet it is. This is like advertising to the world what you are trasmitting. Using command "telnet cs.boisestate.edu portnumber" to verify which of the following ports is open on cs.boisestate.edu.

Port 80: HTTP (Hypertext Transfer Protocol) Port 20: FTP (File Transfer Protocol) Port 69: TFTP (Trivial File Transfer Protocol) Port 23: Telnet (Terminal Network) Port 22: SSH (Secure Shell) Port 25: SMTP (Simple Mail Transfer Protocol)

References

A large portion of the material is adapted from:

- Fundamentals of Information Systems Security - David Kim, Michael G.Solomon
- Selena Gomez answers to mean tweet https://www.youtube.com/watch?v=0jtt78pnA0E