MSA 516

CyberProtect Assignment

Due: _____

Introduction

As cloud computing expands, understanding system security issues becomes increasingly critical. Using the Department of Defense CyberProtect simulation, you must protect your systems from attack. You will assume the role of a system administrator, learn about system security threats, and protect a computer network from threats. You will be protecting your systems from attacks such as viruses, flooding, data theft, jamming, etc. You will complete at least one round (4 quarters) during which you experience multiple attacks to security measures implemented. Each of these attacks may be either successful (your controls failed to prevent the attack) or unsuccessful (the controls stopped the attack from doing damage.)

Requirements

1. Launch the CyberProtect simulation from the following URL:

   http://iatraining.disa.mil/eta/cyber-protect/launchpage.htm

2. You must complete at least 1 round of simulation (4 quarters) with at least an **80%** rating. Save the CyberProtect report with your final rating.
3. Develop an Excel Spreadsheet with 2 sheets: Sheet 1 will contain a "Successful Attack Matrix" and Sheet 2 will contain an "Unsuccessful Attack Matrix." These matrices are based on each of the attacks in your simulation. (See example below)
4. Submit your CyberProtect report and spreadsheet to Canvas.

***Successful Attacks Matrix (Your controls FAILED to prevent the attack)**

Qtr	Source of Attack (Internal or External)	Attack Description	Damage Caused	Missing Control
1	Internal	Virus: Malicious program that reproduces by attaching itself to a computer program.	Network operation is unusual, degraded, or crashed	Anti-virus
…				

***Unsuccessful Attacks Matrix (Your controls BLOCKED the attack)**

Qtr	Source of Attack (Internal or External)	Attack Description	Damage Caused	Preventive Control
1	Internal	Virus: Malicious program that reproduces by attaching itself to a computer program.	Network operation is unusual, degraded, or crashed	Anti-virus
…				

Information Security Attacks

Attack	Description	Consequences	Countermeasures
Data Modification	Change or destroy information on a system	• Can't get information. • Get false information from our own data files.	• Intrusion detection • Access control • Backup (2) • User Training (2)
Data Theft	Steal sensitive information without owner knowing about it	• Competitor or bad guy gets information. • We don't know that someone has the information.	• Intrusion detection • Access control • User Training (2) • Backup (2)
Flooding	Bombards system with more messages or information than it can handle	• System cannot process all the data coming in or it processes this information and ignores other important processing tasks. • Results in denial of service to valid users.	• Firewall • Redundant Systems (2)
Imitation or Spoofing	Pretends to be a valid user by using a stolen userID and password or by "hijacking" a valid session	• Bad guy can get into a computer to steal data, destroy data, or take control of system, but looks like a valid user.	• Encryption • Access Control • User Training (2)
Jamming	Electronically disrupt transmission signals	• Information coming in over communications lines is incorrect or can't be understood.	• Disconnection • Redundant Systems (2)
Mole	A trusted person of an organization gives information to an outsider	• Competitor or bad guy gets information • We don't know that someone has the information.	• Access Control • User Training (2)
Packet Sniffer	Tools collect information from network such as UserID, passwords, contents of E-mail messages, credit card numbers.	• Attacker can get valid UserIDs and passwords that enable him to legally log onto a system. • Confidential information is read by unauthorized persons.	• Encryption • User Training (2)
Social Engineering	Information obtained by talking with people, obtaining their trust, and tricking them to give out information, like passwords.	• Passwords and other confidential information may be given to an unauthorized person.	• User Training
Virus	Malicious program that reproduces by attaching itself to a computer program.	• Destroys information on a system or makes it run very slowly.	• Anti-virus software • User Training (2) • Backup (2) • Redundant Systems (2)

(2) - Refers to a secondary countermeasure that may help you recover from the problem or may indirectly help to prevent it.

Tool Descriptions and Placement in the Network

Tool Descriptions

User Training: This often makes the difference between success and failure of an overall security strategy because users are positioned to be the first line of detection for many attacks. A well-trained user base will be able to recognize when something unusual is occurring, know what to do, and how to report the security problem to those who can investigate further. Training is automatically placed for you in their labeled locations separately from your network diagram.

Redundant System: Duplicates critical portions of you network hardware and software and are typically maintained in "standby" status or even in parallel operation during normal system operation. In the event of successful attack on your network (or other system failure), redundant system function independently permitting rapid restoration of your networks operation. Redundant systems are placed automatically for you in their labeled locations separately from your network diagram.

Access Control: Restricts access to your Information System resources to those users, programs, processes, and other systems that have specific authorization for their use. Access control is placed on the server.

Anti-Virus Program: Anti-virus safeguards include prevention, detection, containment, and recovery measures. The anti-virus program represents a combination of procedures and software that detects and removes most known viruses. Anti-virus protection is placed on the server and individual workstations.

Backups: These are hardware, software, and procedures used to mitigate the consequences of accidental, natural, or manmade damage that can effect your network and users. In using the backup defensive tool, copies of files and programs are maintained and updated to facilitate systems and information recovery. Backups are placed on the server and individual workstations.

Disconnection: This is a combination of hardware and software that denies external attackers (or the effects of their attack) entrance to a network through the link protected by with the disconnection capability protects. This permits continued functioning of your information systems exclusive of that link. Disconnection features are placed on routers.

Encryption: This converts, by means of a cryptographic system, original information (plain text) into transformed information (cyphertext), for transmission over one of your external links. Cyphertext usually has the appearance of random, unintelligible data. Without the method to decrypt the encrypted data, this information is of little use to an attacker. Encryption is placed on routers.

Firewall: This limits access for information transfer between networks in accordance with local security policy. Your firewall protects your network integrity by controlling information flow over your networks external linkages, thus restricting external access to your network. Firewalls are placed on the external links of the routers being protected.

Intrusion Detection Software: Collects data on user (and intruder) activity and performs analyses to detect security attacks, unauthorized activity, and network abuse. Intrusion Detection is designed to give you real-time warning and may automatically react to any computer misuse it detects. Intrusion Detection is placed on the server.

Tool	Server	Workstation	Router	Universal
Access Control	X			
Antivirus	X	X		
Backups	X	X		
Disconnection			X	
Encryption			X	
Firewall			X	
Intrusion Detection	X			
Redundant Systems				X
User Training				X