CONFIDENTIAL

TROJAN BRICKS SECURITY

CYBER SYSTEM SECURITY PLAN

Approvals

_____

Lola Wolfe, CEO

Table of Contents

1. System Description

1. System Attributes

System Name	*Trojan Bricks Security*
Impact Categorization	*<See NIST 800-18, Section 3.2>*
System Owner	*<See NIST 800-18, Section 3.3>*
Security Manager	*<See NIST 800-18, Section 3.6>*
Primary System Administrator(s)	
Primary System Users	

2. System Description and Mission

<See NIST 800-18, Section 3.8 and 3.9, and write 2 -3 paragraphs about the system, its function and mission>

3. Security Requirements

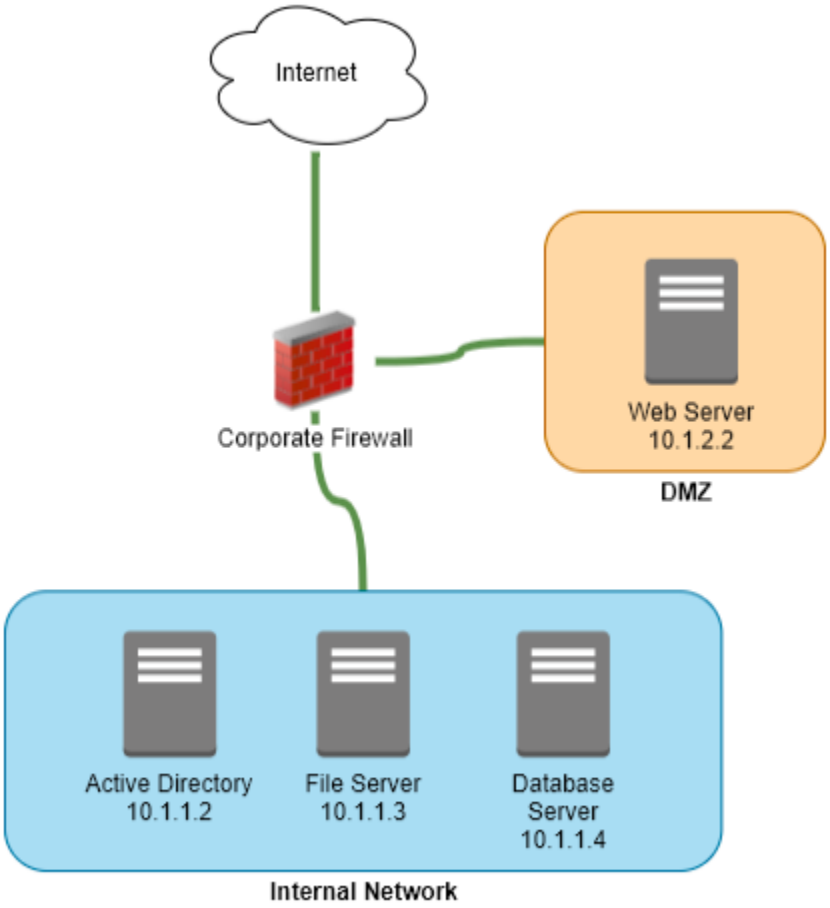
<NIST 800-18, Table 1>

Requirement	Impact	Description
Confidentiality	High	*Each segment of the information system is divided by the access privileges that have been given to different members of the organization depending on their hierarchy in their in the organization and the roles assigned to them. The roles vary according to their respective departments they belong to. Care has been given so that there is no access provided that undermines this division. Access control policies prevent unauthorized access of assets by users that don't have requisite roles for the system they are trying to access.*
Integrity	Med	Threats that may arise are in the form of competitors trying to corrupt the company's database that may hold their marketing and design information. The security protocols must be design to safegaurd the company systems from such attacks.
Availability	Low	Availability is of a lower concern for the organization as it does not provide a consumer interface. Even if the organization's access to its data is delayed, it still would not not affect the organization to a very high degree once the systems have been restored

4. System Environment

The system comprises a single Internet facing web server from which all marketing and purchases take place. The web server has a back end mysql database (i.e. Database Server). An Active Directory server is used to manage all employee and contractor accounts, and a file server exists for sharing documents throughout the company.

5. Network Diagram(s)



6. Dependencies and Interconnections

<See NIST 800-18, Section 3.10>

-

2. Plan of Action and Milestones

Use this section to specify a plan of action to address unmet or partially met security control objectives or to track vulnerability mitigation.

POAM ID	*Security Control/Issue*	*Plan of Action*	*Responsible*	*Milestone Date*

3. Security Controls

<In a real security plan, this section will be long and comprehensive (i.e. 70-100+ pages). This describes how the required security controls are implemented. Include screenshots or references to other documents and configuration settings. For any areas where improvement is needed, include documentation in the Plan of Actions and Milestones (POAM) above.>

3.1. Access Management

<This maps to control families AC and IA>

3.1.1. EXAMPLE: Account Management

Requirement:	*The system owner creates, enables, modifies, disables, and removes cyber system accounts in accordance with the following policy:* • *Accounts must automatically be disabled after 90 days of inactivity* • *Contractor accounts must remain disabled when not in use*
Control Reference:	*NIST 800-53, AC-2(7)*
Last Review and Update:	2020-Feb-05
Implementation:	

A script runs every day on the Domain Controller to disable users. The following screen shots show the scheduled task and script use to disable users.

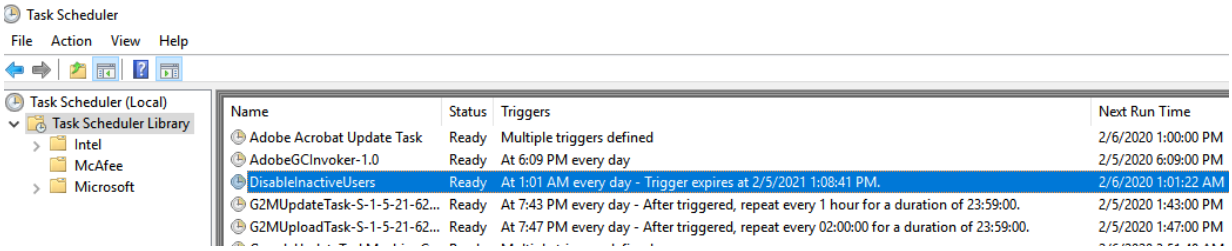


Figure 1: Scheduled Task

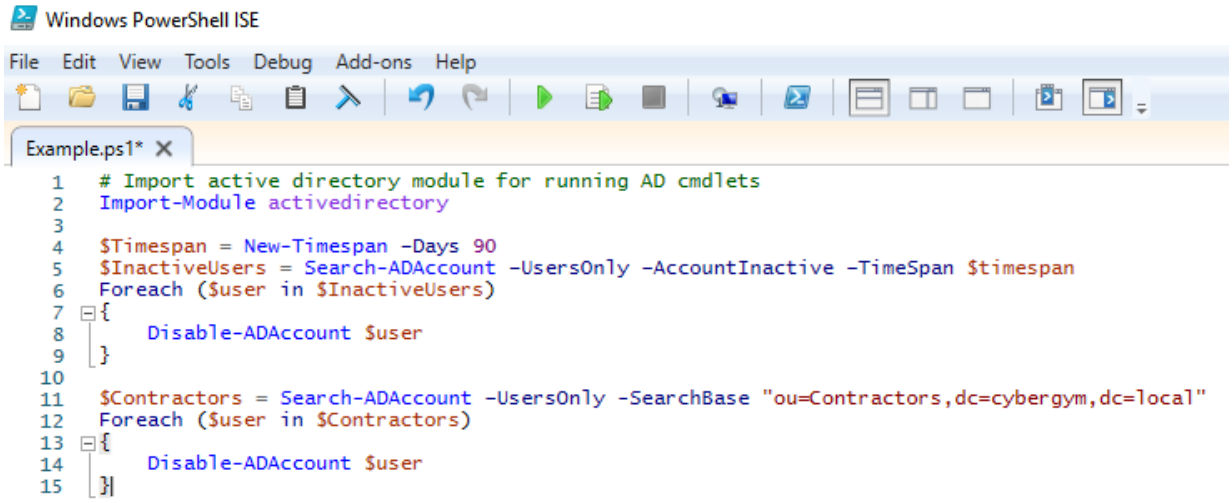


Figure 2: Contents of the Powershell Script Disabling Inactive Users and Contractors

3.2. Personnel Security

<This maps to control family PS>

3.3. Security Awareness and Training

<This maps to control family AT>

3.4. Physical Security

<This maps to control family PE>

3.5. System Communication Protection

<This maps to control family SC>

3.6. Remote Access

<This maps to control family MA>

3.7. Change Management

<This maps to control family CM>

3.8. Malicious Software Protection

Malware, also known as malicious code, refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system. Malware is the most common external threat to most hosts, causing widespread damage and disruption and necessitating extensive recovery efforts within most organizations. Organizations also face similar threats from a few forms of non-malware threats that are often associated with malware. One of these forms that has become commonplace is phishing, which is using deceptive computer-based means to trick individuals into disclosing sensitive information.

A. Employs malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.

The Windows Virus Protection needs to be configured(and kept that way) to periodically scan all entry and exit points into the Trojan system . All real-time events that allow data transfer from outside the organization need to be monitored.These include all email attachments which should be checked for known malwares. This further extends to performing real-time scans of each file as it is downloaded, opened or executed(on-access scanning).

B. Updates malicious code protection mechanisms whenever new releases are available in accordance with organizational configuration management policy and procedures.

The system administrator should monitor the antivirus software regularly and should continuously and periodically make sure that software updates are delivered throughout the organization. Users should not be able to disable or delete antivirus software from their hosts, nor should they be able to alter critical settings. Antivirus administrators should perform continuous monitoring to confirm that hosts are using current antivirus software and that the software is configured properly. Implementing all of these recommendations should strongly

support an organization in having a strong and consistent antivirus deployment across the organization.

C. Configures malicious code protection mechanisms to:

1. Perform periodic scans of the information system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more); endpoint; network entry/exit points] as the files are downloaded, opened, or executed in accordance with organizational security policy.

All common applications such as email clients, web browsers, and instant messaging software must be monitored as these are most likely to infect hosts. The Antivirus software must be configures to scan all hard drives regularly to identify any file system infections and scan all removable media inserted into the host before allowing its use. Manual scan settings should also be configured and accessible to users.

2. [Selection (one or more): block malicious code; quarantine malicious code; send alert to administrator; [Assignment: organization-defined action]] in response to malicious code detection.

Malware incidents must be contained when they are able to pass through the antivirus software. This will be accomplished through shutting down the services used by the malware such as the mailing lists that are the source of the malware.Shutting down the affected services is the best way to contain the infection without losing all services. This will be done by configuring the firewalls to block the IP addresses and ports associated with the specific services.This allows the overall system to be preserved by limiting the infection to a limited scope.

D. Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.

The false positives are analyzed and the the reasons for their identification as malicious codes logged for future reference. These settings may be altered to prevent further disruption of service by the same services after the appropriate analysis by the antivirus administrator.

3.9. Logging Configuration

<This maps to control family AU>

3.10. Media Protection

<This maps to control family MP>

4. Cyber Security Incident Response Plan

<This maps to control family IR. It is included outside of the security controls section because it is useful for individuals to quickly find in an event of a cyber security incident.

For the project provide a few paragraphs of things you would need to consider when responding to an incident. This does not need to be comprehensive.>

5. Recovery Plan

<This maps to control family CP. It is included outside of the security controls section because it is useful for individuals to quickly find in an event of a disaster.

For the project provide a few paragraphs of things you would need to consider when recovering from a disaster. Include documentation about taking system backups and steps for saving logs before writing over or destroying old configurations.>

6. Contacts – Vendor, Supplier, Internal

<See NIST 800-18, Section 3.5>
