Стандарт конфигурирования механизмов безопасности операционных систем

ОГЛАВЛЕНИЕ

Общие положения

Настоящий документ представляет собой описание

Стандарт конфигурирования настроек безопасности ОС используется при первоначальной настройке ОС всех серверов,

Пересмотр положений настоящего документа проводится…, а также при:

- …;
- …;
- …;
- ….

1. Цели и задачи документа

1.1. Целью настоящего Стандарта является исключение ошибок конфигурирования и исключение возможности выполнения следующих действий злоумышленником[1]:

- получение доступа к данным на уровне ОС;
- повышение привилегий до роли администратора;
- ….;
- ….;
- ….;
- ….;
- ….;
- ….;
- …..

1.2. Основные задачи, решаемые настоящим документом:

- определение требований к настройкам механизмов безопасности;
- …;
- …;
- …;
- …..

2. Требования информационной безопасности

2.1. Требования к ОС

2.1.1. Правила (методики) конфигурирования механизмов безопасности должны быть разработаны для следующих операционных систем:

- ОС …..;
- ОС Windows 10;
- ОС Windows Server 2012;
- ОС...

[1] Основные атаки, совершаемые злоумышленниками в ОС, направлены на повышение своих привилегий и несанкционированного доступа к данным.

2.1.2. Перед осуществлением ввода ОС в промышленную эксплуатацию для каждой ОС необходимо выполнить:

- установить все новые обновления безопасности для ОС, определенные текущими схемами безопасности;
- ….
- …;
- …;
- ….;
- …;
- …;
- ….;
- …;
- ….

2.1.3. При внедрении нового типа ОС необходимо….

2.1.4. Правила (методики) конфигурирования механизмов безопасности ОС приведены ниже:

- для
- для.

2.1.5. После выполнения всех настроек необходимо… протестировать сконфигурированные механизмы безопасности и убедиться, что…

2.1.6. Подразделением ИБ осуществляется...

3. Требования к дополнительным средствам защиты

3.1. Требования по установке и настройке системы контроля целостности критичных файлов.

3.2. Требования по установке антивирусного ПО

3.3. Требования по настройке подключения системы автоматизированного контроля.

4. Контроль выполнения требований документа

4.1. Контроль выполнения требований настоящего документа проводится…

4.2. Объекты контроля:

- ...
- …
- …

5. Ответственность

5.1. Ответственность за выполнение требований настоящего документа при выполнении работ по настройке механизмов безопасности ОС несет…

5.2. Ответственность за контроль исполнения требований настоящего документа несет…

ПРИЛОЖЕНИЕ 1.

Список терминов и определений

Владелец информации (информационного ресурса) –

Информационный ресурс – …..

Обработка данных платежных карт – любое действие или совокупность действий, совершаемых с данными платежных карт, включая запись, систематизацию, накопление, хранение, изменение, использование, передачу, удаление, уничтожение.

Критичные файлы – файлы, которые редко изменяются, но изменение которых может служить признаком компрометации системы или указывать на попытку компрометации:

- ….
- ….
- ….
- ….

Middleware – серверное программное обеспечение промежуточного слоя.

PCI DSS – стандарт безопасности данных индустрии платежных карт

ПРИЛОЖЕНИЕ 2.

Перечень сокращений

ВНД	–	Внутренний нормативный документ
ИБ	–	Информационная безопасность
ИР	–	Информационный ресурс
ИТ	–	Информационные технологии
НСД	–	Несанкционированный доступ
ОС	–	Операционная система
ПО	–	Программное обеспечение
СУБД	–	Система управления Базами данных

ПРИЛОЖЕНИЕ 3.

Перечень ссылочных документов

1. PCI-DSS Payment Card Industry (PCI) Data Security Standard. Requirements and Security Assessment Procedures.
   https://www.pcisecuritystandards.org/security_standards
2. …
3. ….

ПРИЛОЖЕНИЕ 4.

Правила конфигурирования механизмов безопасности ОС MICROSOFT WINDOWS SERVER 2003, WINDOWS SERVER 2008, WINDOWS SERVER 2012

1. Установка всех новых обновлений безопасности для ОС

1.1. Необходимо установить….

1.2. Установка обновлений безопасности…

2. Проверка локальных учетных записей в ОС

3. Ввод сервера в домен

4. Документирование программного обеспечения

Цель: отключить и/или удалить всё неиспользуемое и ненужное программное обеспечение.

4.1. Все используемое программное обеспечение должно быть задокументировано в виде…

4.2. Допускается запуск следующих системных сервисов, указанных в Табл. 1.

Табл. 1. Запущенные сервисы

Краткое наименование	Полное наименование
AeLookupSvc	Application Experience
AppHostSvc	Application Host Helper Service
…	
…	
…	

Список сервисов может…

5. Конфигурирование механизмов безопасности в Active Directory

Настройка прав доступа пользователей, параметров безопасности и протоколирования событий осуществляется через консоль управления групповыми политиками (gpmc.msc).

5.1. Необходимо настроить права пользователей.

Табл. 2. Права пользователей в Active Directory

Параметр	Права	Критичность применения требования
Access this computer from the network	Administrators, Backup Operators, Users, Authenticated Users	
Load and Unload Device Drivers	Administrators	
Manage Auditing and Security Log		
Modify Firmware Environment	Administrators	Обязательно
Allow log on through Terminal Services	Administrators, Remote users	Обязательно
Lock pages in memory	No one	Допускается добавлять технологические учетные записи
Change the system time	Administrators	Настройки устанавливаются согласно рекомендациям производителя в

Параметр	Права	Критичность применения требования
		зависимости от технологического назначения сервера.
Create a pagefile	Administrators	
Debug programs[2]	No one	
Deny access to this computer from the network	Anonoymous logon; Guests;	В настоящий момент неприменимо в инфраструктуре: есть клиенты LM и NTLM, которым для смены пароля первоначально требуется анонимный доступ.
Deny logon locally	Guests;	Обязательно
Force shutdown from a remote system	Administrators, Server Operators	N/A
Increase security scheduling priority		
Profile single process	Administrators	Обязательно
Restore files and directories		
Perform volume maintenance tasks	Administrators	Обязательно
Profile System Performance		
Take Ownership of Files and Objects	Administrators	

5.2. Необходимо настроить параметры безопасности.

[2] Данный параметр неприменим для серверов с ролью MS SQL Server

Табл. 3. Параметры безопасности Active Directory

Параметр	Значение	Критичность применения требования
Microsoft network server: Disconnect clients when logon hours expire	Enable	Обязательно
Network Access: Allow anonymous SID/NAME translation	Disable	
Network Security: Force Logoff when Logon Hours expire		
Allowed to format and eject removable media		
Prevent users from installing printer drivers		
Digitally encrypt secure channel data (when possible)		
Digitally sign secure channel data (when possible)		
Disable machine account password changes		
Maximum machine account password age		
Require strong (Windows 2000, Windows XP, or Windows Server 2003) session key		
Digitally sign communications (always)		
Digitally sign communications (if server agrees)		
Send unencrypted password to third-party SMB servers		
Amount of idle time required before suspending session	15	
Do not allow anonymous enumeration of SAM accounts		
Do not allow anonymous enumeration of SAM accounts and shares		
Do not allow storage of credentials or .NET Passports for network authentication		
Let Everyone permissions apply to anonymous users		
Restrict anonymous access to Named Pipes and Shares		
Shares that can be accessed anonymously	None	
Do not store LAN Manager hash value on next password change		
LAN Manager authentication level	Send NTLMv2 response only\refuse LM & NTLM	
LDAP client signing requirements		
Minimum session security for NTLM SSP based (including secure RPC) clients		
Minimum session security for NTLM SSP based (including secure RPC) servers		
Allow automatic administrative logon		

Параметр	Значение	Критичность применения требования
Allow system to be shut down without having to log on		
Clear virtual memory page file		
Default owner for objects created by members of the Administrators group		
Strengthen default permissions of internal system objects (for example, Symbolic Links)		

5.3. Настроить политики безопасности домена на контроллере домена, создав объекты групповой политики, привязав их к домену.

Табл. 4. Настройка политики безопасности домена

Параметр	Значение
Maximum Password Age	
Minimum Password Length	
Minimum Password Age	
Enforce password history	
Password Complexity Requirements	
Reversible Encryption for Passwords	

5.4. Необходимо настроить параметры блокировки учетной записи.

Табл. 5. Параметры блокировки учетных записей в Active Directory

Параметр	Значение
Account lockout duration	
Account lockout threshold	
Reset account lockout counter after	

5.5. Необходимо активировать функцию ввода пароля при блокировке экрана.

Настройка экрана:

5.6. Необходимо настроить параметры протоколирования событий.

Настройка параметров протоколирования:

Необходимо настроить аудит событий, представленных в Табл. 6 через групповую политику.

Табл. 6. Параметры протоколирования событий

Политики	Значение
Account Logon Events	
Account Management Events	
Directory Service Access Events	
Logon Events	
Object Access Events	
Policy Change Events	
Privilege Use Events	
Process Tracking	
System Events	

Для тех серверов, журналы которых не хранятся на централизованном сервере сбора событий, необходимо настроить в Settings of Event Log (Настройка журнала событий) и производить периодическое резервное копирование журналов (Табл. 7).

Табл. 7. Параметры настройки журналов событий

Политики	Значение
Restrict Guest Access to the Application Log	
Restrict Guest Access to the Security Log	
Restrict Guest Access to the System Log	
Retention Method for Application Log	
Retention Method for Security Log	
Retention Method for System Log	

Необходимо настроить размер журналов ….

6. Настройка службы времени

На серверах в составе домена служба времени Windows настраивается...