wiseadvice
Consulting Group

Типовая программа ИТ-АУДИТА

(Департамент инфраструктурных решений WiseAdvice Consulting Group)

1. Определение узких мест информационной системы с точки зрения безопасности:

- **анализ политик безопасности;**

1) Результирующие локальные политики безопасности на серверах

1.Политика аудита

2.Назначение прав пользователя

3.Параметры безопасности

4.Брандмауэр Windows

5.Настройки лог файлов

6.Сервисы в автозагрузке

7.Список установленного ПО

2)Применяемые к рабочим станциям доменные политики

1. Назначение прав пользователя

2.Параметры безопасности

3.Брандмауэр Windows

4.Ограничения приложений

5.Сетевая установка ПО

6.Скрипты выполняемые при запуске/остановке рабочей станции

3) Применяемые политики обновления ПО

1.наличие сервера WSUS

2.Состояние синхронизации WSUS

3.Состояние распространения обновнений

- **сканирование сети и доступных сервисов извне на предмет уязвимостей;**

1) список сервисов доступных из внешних сетей

1.Права с которыми запущены службы доступные из вне.

2) Порядок предоставления доступа из вне.

1.Кто предоставляет доступ/и как хранится история

разрешений

2.Ограничения при доступе из вне.

3) Контроль доступа из внешней сети

1.Наличие лог файлов/хранение истории

2.Возможность быстрой блокировки доступа всем/отдельным сотрудникам

- **аудит антивирусной защиты, политика паролей и пользовательских разрешений;**

1) Название антивирусного по и его тип(централизованное или персональное)

2) Политики применяемые к серверам

1.Ограничения проверяемых файлов

2.Кто может приостановить работу антивируса на сервере

3)Политики применяемые к рабочим станциям

1.Ограничения проверяемых файлов

2.Кто может приостановить работу антивируса.

4)Доступ к статистике антивируса

5)Оповещаемые лица при возникновении вирусной угрозы

2. Диагностика работы серверного оборудования на программном и аппаратном уровне:

тестирование серверного оборудования; тестирование отказоустойчивости источников бесперебойного питания;

1)Внешний осмотр серверов (без выключения)

2)Соответствие мощности ИБП мощности серверов и ожидаемое время автономной работы

3)настройки ПО ИБП на серверах

4)Внутренний осмотр серверов (с выключением)

5)реальное тестирование нагрузочной способности ИБП (с выключением)

- анализ записей в журналах событий;

1)Поиск событий связанных с аппаратными сбоями

2)Поиск событий связанных с перезапуском служб

анализ настроек серверных служб;

1)Права с которыми запущены службы

2)Поиск ошибок связанных с запущенными службами

3. Определение узких мест производительности серверов:

1)анализ загруженности серверов в часы наибольшей активности;

2)анализ распределения нагрузок на сервера;

3)проверка наличия места на жестких дисках;

4)выявление наиболее ресурсоёмких приложений;

4. Диагностика работы компьютерной сети, активного оборудования:

1)диагностика потери пакетов внутри и снаружи

2)тестирование скорости интернет-канала;

3)анализ настроек и политик безопасности активного оборудования;

4)Тестирование загруженности внутренних каналов между активным оборудованием

5. Анализ корректности пользовательских настроек (по выбору несколько рабочих станций):

1)Соответствие эталонным настройкам

2)Состояние антивирусного ПО

3)наличие нелицензионного ПО

4)Наличие вредоносного ПО (Сниферы, кйлогер, подбор паролей и.тп.)

6. Аудит политики резервного копирования:

1.наличие резервных копий для сервисов

2.политика резевного копирования для сервисов

3.выборочное тестирование бакапов

4.диагностика устройств хранения резервных копий

7. Анализ сетевой структуры, поиск уязвимых мест, анализ компоновки серверных и сетевых решений:

1)Способ доступа к северному и активному сетевому оборудованию.

2)Выявление перегруженных серверов.

3)Анализ системы кондиционирования серверов

4)Анализ альтернативного подключения электричества к серверам

5)Соответствие текущих характеристик электрической мощности серверов подводящей сети.

8. Определение узких мест Информационной системы с точки зрения надежности:

1)Определение единых точек отказа для нескольких сервисов

2)Определение единых узких мест производительности для нескольких сервисов.

9. Анализ ситуаций полного или частичного отказа серверного или сетевого оборудования.

На основании пунктов 6,7,8 прогноз простоя и потери данных при выходе из строя отдельных серверов.

10. Анализ заявок пользователей и предыдущих инцидентов:

1)Наличие системы учета заявок, или способ их учета.

2)анализ наиболее типовых заявок от пользователей

3)анализ предыдущих крупных происшествий и их последствий