Контрольный список аудита сетевой безопасности

1. Общие вопросы

- ✓ Письменная политика сетевой безопасности, в которой перечислены права и обязанности всего штата сотрудников и консультантов.
- ✓ Обучение по безопасности для всех пользователей в отношении использования сетевой среды и обмена данными за пределами компании, а также предоставления доступа к своим системам для посторонних лиц.
- ✓ Убедитесь в том, что пользователи прошли обучение по вопросам обмена информацией по электронной почте и через Интернет.
- ✓ Все внешние поставщики и подрядчики должны подписать соглашение об обеспечении безопасности во время работы в вашей ИТ-среде.
- ✓ Имеются планы действий в чрезвычайных ситуациях на случай нарушения целостности данных или взлома системы безопасности.

2. Безопасность паролей

- ✓ Письменная политика обращения с паролями
- ✓ Обучение работе с паролями для всех авторизованных пользователей, чтобы обеспечить понимание ими потенциальных рисков, связанных с обращением с паролями небезопасным образом.
- ✓ Проверить рабочие станции на наличие записанных паролей в непосредственной близости от рабочих станций или серверов.
- ✓ Хранить документацию по требованиям к паролю в безопасном месте

3. Безопасность LAN-сети

- ✓ Усиление серверов во внутренней сети, удаление ненужных сервисов и приложений.
- ✓ Удаление ненужных файлов с серверов
- ✓ Права доступа к серверу для пользователей установлены надлежащим образом
- ✓ Анонимные пользователи не допускаются
- ✓ Разделение функций администрирования сервера между администраторами
- ✓ Политика удаленного администрирования
- ✓ Отключение режима удаленного администрирования там, где он не нужен.
- ✓ Политика безопасности удаленного доступа и ее реализация
- ✓ Переименование учетной записи администратора
- ✓ Включить аудит попыток входа администратора

- ✓ Создать сверхнадежные пароли для учетных записей администраторов
- ✓ Пароли учетных записей серверных администраторов должны отличаться от паролей учетных записей, используемых теми же пользователями для входа в рабочую станцию.
- ✓ Отключить формирование гостевой учетной записи
- ✓ Ограничить доступ к группе "Все"
- ✓ Создать надлежащие учетные записи пользователей и групп
- ✓ Установить соответствующие разрешения доступа для групп
- ✓ Настроить журналы аудита для отслеживания несанкционированного доступа к файлам/системам/папкам/учетным записям
- ✓ Настроить управление исправлениями или плановыми загрузками и применением операционной системы и изменениями в системе безопасности.
- ✓ Убедиться в правильной конфигурации системы безопасности беспроводной сети, включая использование соответствующих протоколов безопасности.

4. Вход в систему с рабочей станции

- ✓ Блокировка экрана на всех компьютерах
- ✓ Требовать пароли на всех компьютерах, включая пароли для выключения блокировки экрана.
- ✓ Рассмотреть возможность использования двухфакторной аутентификации
- ✓ Усиление рабочих станций, удаление ненужных приложений и программ.
- ✓ Установлено антивирусное программное обеспечение и отключена возможность обходного маневра
- ✓ Убедиться, что обновления антивирусной программы происходят регулярно
- ✓ Убедиться, что обновления программного обеспечения происходят регулярно
- ✓ Убедиться в том, что патчи для операционной системы и системы безопасности устанавливаются регулярно.
- ✓ Включено блокирование всплывающих окон

5. Мобильные устройства

- ✓ В отношении мобильных устройств, используемых в сети, должна действовать политика ИТ-безопасности или политика BYOD (*концепция использования сотрудниками собственных устройств*).
- ✓ Необходимо принять решение о внедрении политики в отношении мобильных устройств и обеспечить ее соблюдение.

- ✓ Беспроводные точки доступа должны быть защищены

6. Безопасность сетевого оборудования

- ✓ Настроить журналы аудита для контроля доступа
- ✓ Конфигурация документа/Настройки рабочей конфигурации на случай сбоя
- ✓ Задокументировать учетные записи пользователей/пароли для доступа к этим устройствам и поместить их в безопасное место.
- ✓ Убедиться, что обновления прошивки происходят регулярно.

7. Безопасность роутеров / межсетевых экранов

- ✓ Использовать межсетевой экран и убедиться, что все публичные службы находятся в отдельном сегменте сети или в зоне децентрализованной машины (например, электронная почта, FTP, web) для предотвращения вторжений.
- ✓ Убедиться в том, что доступ для всех внешних IP-адресов в локальную сеть запрещен, и открыт только в зону децентрализованных машин (DMZ).
- ✓ Настроить политику межсетевого экрана на запрещение входящего доступа к неиспользуемым портам
- ✓ Проанализировать все политики межсетевого экрана на предмет потенциальных угроз безопасности
- ✓ Внедрить трансляцию сетевых адресов (NAT) там, где это возможно
- ✓ Использовать контроль состояния соединений на межсетевом экране для предотвращения подмены IP-адресов и DOS-атак.
- ✓ Убедиться, что программное обеспечение роутера и межсетевого экрана регулярно обновляется.
- ✓ Убедиться, что прошивка роутера и межсетевого экрана регулярно обновляется.
- ✓ Рассмотреть возможность проведения тестирования на проникновение для выявления дополнительных слабых мест.