ACTIVE DIRECTORY И БЕЗОПАСНОСТЬ

Шапошникова Н.П., магистрант гр. 267241

Белорусский государственный университет информатики и радиоэлектроники

г. Минск, Республика Беларусь

Пулко Т.А. – канд. техн. наук

Аннотация. Уровень защищенности службы каталогов нередко определяет уровень безопасности всей компании. Целесообразно максимально усложнить деятельность злоумышленника, уменьшив возможные области атаки, проводить регулярный мониторинг системы в целях выявления злонамеренных действий и всегда быть готовым к отражению атак, имея детальные планы действий для разных ситуаций.

Уровень защищенности службы каталогов нередко определяет уровень безопасности всей компании. Целесообразно максимально усложнить деятельность злоумышленника, уменьшив возможные области атаки, проводить регулярный мониторинг системы в целях выявления злонамеренных действий и всегда быть готовым к отражению атак, имея детальные планы действий для разных ситуаций.

Проблемы построения безопасных ИТ-инфраструктур являются актуальными для любых организаций. Как только возникает потребность в ИТ-решениях, тут же встает вопрос их безопасности. Не существует абсолютно неуязвимых с точки зрения ИБ организаций, тем не менее необходимо создать как можно больше трудностей злоумышленнику, пытающемуся скомпрометировать или уничтожить ИТ-инфраструктуру компании. Обеспечение безопасности службы каталога – важнейшая задача ИТ и ИБ-отделов предприятия.

Ниже представлен перечень мер, которые помогут значительно снизить вероятность повреждения или внесения несанкционированных изменений в базу данных Active Directory [1]:

1 Своевременное обновление ОС и ПО позволяет уменьшить вероятность компрометации системы и осуществления несанкционированной злонамеренной деятельности внутри ИТ-инфраструктуры организации.

2 Эффективная антивирусная защита и защита от зловредного ПО позволяет существенно повысить защищенность ИТ-инфраструктуры организации в целом.

3 Регулярное резервное копирование AD обеспечивает возможность оперативно восстановить БД СК и удаленные объекты AD, а также службу каталога в ситуации катастрофического сбоя.

4 Эффективная стратегия именования объектов позволяет администраторам службы AD эффективно идентифицировать объекты и управлять данными, хранящимися в AD.

5 Безопасность контроллеров доменов (DC) обеспечивают серверы, хранящие реплику БД службы каталога AD, которые выполняют функции управления данными AD.

6 Защита учетных записей привилегированных пользователей. Ошибочное включение пользователей в высокопривилегированные группы может привести к краху системы как из-за отсутствия достаточных знаний и навыков, так и в результате злонамеренных действий [2].

7 Использование дополнительных возможностей ОС по обеспечению безопасности.

8 Использование принципа наименьших привилегий позволит существенно повысить уровень безопасности, уменьшая для злоумышленника область атаки.

9 Блокировка возможности развертывания и выполнения неавторизованных приложений и сервисов, очевидно, повышает безопасность системы.

10 Наличие доступа к Интернету значительно снижает безопасность всей инфраструктуры. Обеспечение безопасного доступа в Интернет и доступа из Интернета к ресурсам организации является одной из важнейших задач по повышению общего уровня безопасности системы.

Обеспечить безопасность AD – сложная задача, но, приняв ряд элементарных мер предосторожности, можно достаточно надежно защитить инфраструктуру AD.

Список использованных источников:

1. Москалев С., Шапиро Л. Active Directory и безопасность. Часть 1. Построение защищенных служб каталога. //«Системный администратор», №7-8, 2013 г. – С. 44-45.

2. https://www.osp.ru/winitpro/2005/03/177563