УДК 004.056.53

МЕХАНИЗМЫ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА НА ОСНОВЕ СЛУЖБЫ КАТАЛОГОВ ACTIVE DIRECTORY

магистрант Н. П. ШАПОШНИКОВА, канд. техн. наук, доц. Т. А. ПУЛКО

(Белорусский государственный университет информатики и радиоэлектроники, Минск)

Рассмотрены основные вопросы, связанные с достоинствами использования службы каталогов Active Directory для локальных сред Microsoft. Расмотрены основные угрозы безопасности Active Directory и сформулированы рекомендации по обеспечению безопасности.

Ключевые слова: *информационные ресурсы, локальная сеть, служба каталогов, угрозы безопасности, Active Directory.*

Как правило, администраторы сетей пользуются правами и централизованным управлением пользователями, а также централизованным контролем над конфигурациями компьютеров и пользователей с помощью функции групповой политики службы каталогов Active Directory (AD). Пользователи могут пройти аутентификацию один раз, а затем беспрепятственно получить доступ к любым ресурсам в домене, для которого они авторизованы. Кроме того, файлы хранятся в центральном репозитории, где они могут использоваться совместно с другими пользователями для облегчения совместной работы, и должным образом резервируются IT-специалистами для обеспечения непрерывности работы всех компонентов сети.

Важно понимать, что AD предназначена только для локальных сред Microsoft и имеет три основных уровня: домены, деревья и леса. Домен – это группа связанных пользователей, компьютеров и других объектов AD, таких как все объекты AD головного офиса компании. Несколько доменов можно объединить в дерево, а несколько деревьев можно сгруппировать в лес. При этом домен – это граница управления. Объекты для данного домена хранятся в одной базе данных и могут управляться вместе. Лес – это граница безопасности. Объекты в разных лесах не могут взаимодействовать друг с другом, пока администраторы каждого леса не создадут между ними доверительные отношения.

Основной службой AD являются доменные службы Active Directory (AD DS), которые являются частью операционной системы Windows Server. Серверы, на которых работают AD DS, называются контроллерами домена (DC). Организации обычно имеют несколько контроллеров домена и у каждого из них есть копия

каталога. Изменения, внесенные в каталог на одном контроллере домена, такие как обновление пароля или удаление учетной записи пользователя, реплицируются на другие контроллеры домена, поэтому все они остаются актуальными. Сервер глобального каталога – это контроллер домена, который хранит полную копию всех объектов в каталоге своего домена и частичную копию всех объектов всех других доменов в лесу; это позволяет пользователям и приложениям находить объекты в любом домене своего леса. Настольные компьютеры, ноутбуки и другие устройства под управлением Windows могут быть частью среды Active Directory, но они не работают с AD DS, который опирается на несколько установленных протоколов и стандартов, включая LDAP (упрощенный протокол доступа к каталогам), Kerberos и DNS (система доменных имен).

База данных (каталог) Active Directory содержит информацию об объектах AD в домене. Общие типы объектов AD включают пользователей, компьютеры, приложения, принтеры и общие папки. Организации часто упрощают администрирование, объединяя объекты AD в организационные единицы (OU), и оптимизируют безопасность, объединяя пользователей в группы. Эти подразделения и группы сами по себе являются объектами, хранящимися в каталоге. Пользовательский объект обычно имеет такие атрибуты, как имя человека, пароль, отдел и адрес электронной почты, а также атрибуты, которые большинство людей никогда не увидят, такие как его уникальный глобальный уникальный идентификатор (GUID), идентификатор безопасности (SID), время последнего входа в систему и членство в группе. Базы данных структурированы, что означает, что существует структура (схема), определяющая какие типы данных они хранят и как эти данные организованы. Active Directory не является исключением: ее схема содержит формальные определения каждого класса объектов, который может быть создан в лесу AD, и каждого атрибута, который может существовать в объекте AD. Обычно AD поставляется со схемой по умолчанию, но администраторы могут изменить ее в соответствии с потребностями организации.

IT-среда – невероятно динамичное место, где пользователи постоянно приходят и уходят, сотрудники берут на себя новые роли, добавляются новые приложения, другие удаляются и т. д. Таким образом, безопасность Active Directory – это не разовое мероприятие, а непрерывный процесс. Однако, следует отметить что, если меры безопасности слишком сложны, они замедлят критически важные бизнес-процессы и отпугнут сотрудников. Например, если требовать от них создания сложных паролей, которые нужно менять каждые тридцать дней, то вскоре можно будет обнаружить у них на столе множество стикеров, что подорвет основную цель защиты.

Многие нормативные требования безопасности включают правила, которые напрямую влияют на политики и процедуры безопасности AD, но эти мандаты часто распространяются на многие другие области, такие как физический доступ

в офисные здания, обучение персонала и ответственность руководителей. С другой стороны, комплексная безопасность AD включает в себя нечто большее, чем соблюдение одного или нескольких правил. Это неотъемлемая часть многих нормативных требований, включая GDPR, CCPA, HIPAA, SOX и PCI-DSS.

Угрозы безопасности Active Directory возникают в основном из-за отсутствия понимания и контроля над тремя ключевыми факторами:

- кто попадает в локальную сеть,
- что им разрешено делать, когда они внутри,
- какая деятельность на самом деле имеет место.

У некоторых из этих рисков есть определенные названия, такие как внутренние угрозы, адресный фишинг, повышение привилегий и боковое перемещение. Однако лучший способ устранить риски безопасности AD – не бороться с каждым из них по отдельности. Такой подход увеличивает затраты и усложняет IT-систему, усугубляя проблему, а не решая ее.

Вместо этого лучшая стратегия – очистить Active Directory и получить четкое представление о деятельности в рассматриваемой IT -среде. Инструменты, встроенные в Active Directory, предоставляют небольшую часть необходимой функциональности и требуют много времени для использования, поэтому разумно инвестировать в комплексные решения, которые автоматизируют и упрощают основные процессы, необходимые для надежной безопасности Active Directory.

Active Directory существует уже давно, поэтому легко доступны передовые методы, которые, как доказано, значительно повышают безопасность и соответствие требованиям AD. Внедрение следующих рекомендаций поможет свести к минимуму риски.

Одним из наиболее важных передовых методов обеспечения безопасности AD является регулярная проверка состояния ИТ-среды и упреждающий поиск потенциальных проблем с безопасностью и соответствием требованиям. Следует периодически сравнивать параметры конфигурации на конечных точках Windows, контроллерах домена и других системах с заведомо исправным состоянием, а затем незамедлительно устранять любые непреднамеренные отклонения или злонамеренные изменения. Обязательно регулярно просматривать групповую политику, которая используется для применения стандартных параметров к пользователям и компьютерам. Групповая политика контролирует многие действия; можно запретить пользователям доступ к панели управления, с помощью командной строки или установки программного обеспечения. Даже одно неправильное изменение объекта групповой политики (GPO) может нанести значительный ущерб. Например, пользователи могут внезапно получить возможность вставлять USB-накопители и тем самым запускать программы-вымогатели или другие вредоносные программы в защищаемые системы. Поэтому необходимо убедиться, что объекты групповой политики работают должным образом и могут быстро

обнаруживать и отменять любые неправомерные или несанкционированные изменения в них.

Возможно, наиболее фундаментальной передовой практикой в области ИТ-безопасности является принцип наименьших привилегий. Поэтому каждому пользователю грамотно предоставить именно тот доступ, который ему необходим для выполнения его работы – ни больше, ни меньше. AD позволяет поместить пользователей с похожими ролями (например, всех администраторов службы поддержки или всех сотрудников отдела кадров) в группу безопасности AD и управлять ими вместе. Пользователи могут быть – и обычно являются – членами нескольких групп AD, таких как проектные группы. Использование групп безопасности AD – это не просто удобство для администраторов, но и повышает безопасность, уменьшая количество ошибок при инициализации и деинициализации, а также сводя к минимуму сложность структуры разрешений, чтобы было легче с уверенностью сказать, кто к чему имеет доступ.

Независимо от того, насколько грамотны мероприятия по предотвращению, администраторы сетей часто сталкиваются с инцидентами кибербезопасности, поэтому необходимо быстро расследовать их и реагировать соответствующим образом: определить, откуда возникла утечка, как она развивалась и какие именно системы и данные были задействованы. Таким образом, можно привлечь людей к ответственности за их действия и принять меры для предотвращения подобных инцидентов в будущем.

Как указывалось ранее, принцип наименьших привилегий – это основная передовая практика ИТ-безопасности. Возможность создавать группы безопасности AD и совместно управлять разрешениями для похожих пользователей снижает нагрузку на администраторов и систему, а также повышает безопасность, уменьшая количество ошибок при инициализации и деинициализации, а также сводя к минимуму сложность структуры разрешений, чтобы было легче с уверенностью сказать, кто к чему имеет доступ.

Особую озабоченность вызывают группы безопасности AD, которые предоставляют привилегии административного уровня, такие как чрезвычайно мощные группы администраторов предприятия, администраторов домена и администраторов схемы, а также учетная запись локального администратора, которая создается во время установки Windows и имеет полный контроль над файлами, каталогами, службами и другими ресурсами на локальном компьютере. Организации должны строго контролировать, кто входит в эти группы привилегированного доступа, и быть готовыми к любым изменениям в их членстве, которые могут указывать на то, что злоумышленник пытается повысить свои привилегии, чтобы получить доступ к дополнительным системам или данным.

Учетные записи служб – это специальные учетные записи пользователей, которые приложения и службы используют для входа и выполнения действий

в IT-среде. К сожалению, учетные записи служб часто имеют больше разрешений, чем им действительно нужно, что увеличивает риски безопасности. Распространенные причины избыточного выделения ресурсов включают безропотное принятие требований, указанных поставщиком приложения, неспособность должным образом справиться с операционными проблемами и простое клонирование существующей службы вместо того, чтобы тратить время на создание новой с соответствующими разрешениями.

Лучше всего обеспечить, чтобы все учетные записи служб соответствовали принципу наименьших привилегий. Также необходимо принимать особые меры предосторожности всякий раз, когда служебной учетной записи требуются административные привилегии. Не следует делать учетную запись службы членом стандартной административной группы, такой как группа локальных администраторов или администраторов домена. Лучшими вариантами являются запуск службы под учетной записью LocalSystem или создание пользовательской группы для учетной записи службы и явный отказ в доступе к другим учетным записям для этой группы. И, когда это возможно, разумно настраивать учетные записи служб, чтобы они могли входить в систему только в течение определенного периода в течение дня.

ЛИТЕРАТУРА

1. Active Directory Security [Electronic resource] : Microsoft Platform Management. – New Haven : Quest Software Inc., 2022. – Mode of access: https://www.quest.com/solutions/active-directory/active-directory-security.aspx. – Date of access: 21.10.2022.
2. Рекомендации по защите Active Directory [Электронный ресурс]: Microsoft 2022. – Mode of access: https://learn.microsoft.com/ru-ru/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory. – Date of access: 23.10.2022.