1

Основы Active Directory

> Несмотря на быстрые изменения в компьютерной индустрии, мы все еще в начале цифровой революции.
>
> *Сатья Наделла*

Прошло два года после выхода второго издания этой книги. Прежде всего я хотел бы поблагодарить читателей за ценные отзывы, которые вдохновили меня на написание третьего издания.

Начнем же мы с того, что освежим знания основ службы каталогов Windows Active Directory и поговорим о том, как пандемия и другие факторы сформировали современный подход к управлению идентификацией и доступом.

Современный подход к управлению доступом

Пандемия COVID-19 усилила неуверенность человечества в отношении физического и психического здоровья, экономики, семьи, общества и работы. Большинство из нас испытали на себе долгосрочные последствия, которых прежде и представить было нельзя. Некоторые из них могут замедлить или ускорить нашу жизнь на годы. Ускоренная пандемией смена парадигмы выражается в форсированной цифровизации общества. Правила режима изоляции и рост спроса на безопасную удаленную работу подтолкнули некоторые автономные сферы коммерции и промышленности к работе в режиме онлайн быстрее, чем ожидалось. Сейчас моя девятилетняя дочь берет уроки игры на фортепиано по видеосвязи в Zoom. Я никогда не думал, что игре на инструменте можно научиться онлайн, но оказался неправ.

В начале пандемии финансовый сектор не был готов к принятию культуры работы из дома. Но недавнее исследование, проведенное корпорацией Deloitte, подтверждает, что почти три четверти (70 %) работающих в сфере финансовых услуг

оценивают опыт работы из дома положительно (источник: https://bit.ly/3CSjC08). Ведущая платформа облачных коммуникаций и привлечения клиентов, компания Twilio, недавно опросила более 2500 руководителей корпораций в Соединенных Штатах, Великобритании, Германии, Австралии, Франции, Испании, Италии, Японии и Сингапуре, чтобы оценить их взгляды на цифровизацию в результате COVID-19. Согласно результатам исследования, 97 % руководителей корпораций считают, что пандемия ускорила цифровизацию их компаний (https://bit.ly/2ZSnTlK). Американская международная фирма по управленческому консалтингу, McKinsey & Company недавно опросила 900 руководителей высшего звена, имеющих различные специальности и представляющих компании практически из всех регионов, отраслей промышленности, разных масштабов. Респонденты подтвердили, что их компании внедрили стратегии цифровизации в 20–25 раз быстрее, чем ожидалось, а переход к удаленной работе произошел в 40 раз быстрее (рис. 1.1).

Рис. 1.1. Скорость реагирования на связанные с пандемией вызовы (https://mck.co/2Ykj9Fd)

В связи с ростом цифровизации работа из дома стала обычной практикой. Бизнесу необходимо внедрять приложения, службы и инструменты сотрудничества,

позволяющие удаленным работникам беспроблемно выполнять повседневные обязанности. Препятствием при решении этой трудной задачи являются не инвестиции или технологии.

Препятствием для множества предприятий, принимающих на вооружение массовый характер такого способа деятельности, стало время. Как только время начинает стоить денег или влиять на продажи, производственный процесс, поставки или производительность труда, становится некогда оценивать все за и против. Некогда выполнять всяческие подготовительные работы. Приходится рисковать, обходить правила. А когда мы спешим, то, как свойственно людям, склонны к совершению ошибок. Некоторые из них в 2020 году открыли ряд возможностей для киберпреступников.

- По данным компании iomart, количество случаев крупномасштабных утечек данных в первом квартале 2020-го выросло на 273 % (https://bit.ly/3mNckFB).
- Данные Управления комиссара по информации Великобритании (Information Commissioner's Office, ICO) подтверждают, что 90 % случаев утечки были вызваны ошибками пользователя (https://bit.ly/3whpgGV).
- Согласно отчету по безопасности на основе управления рисками за III квартал 2020 года (https://bit.ly/3mMxjbu), больше всего случаев утечки данных пришлось на здравоохранение (11,5 %) и ИТ (10,3 %). А эти две отрасли были наиболее активными в период пандемии.
- В отчете также сообщается, что 29 % случаев утечки данных за 2020 год связано с компрометацией паролей, 36 % — с компрометацией адресов электронной почты и 45 % — с компрометацией имен.

Подытоживая приведенные данные, можно заметить огромный рост количества случаев утечки данных в 2020 году, большинство из которых вызвано человеческим фактором. Основными мишенями, финансово мотивирующими киберпреступников, стали здравоохранение и ИТ. Эти сведения также подтверждают, что киберпреступники в основном охотятся за *учетными данными*.

Учетные данные стали новым периметром безопасности. Модель защиты уже не работает против современных угроз. Управление доступом и идентификацией — это краеугольный камень цифровизации.

В проведенном компанией Ping Identity исследовании сообщается, что 90 % ключевых лиц в сфере ИТ считают управление доступом и учетными данными основным фактором цифровизации (https://bit.ly/3BNw0gS). Решения для управления доступом и идентификацией зависят от того, как службы каталогов, такие как Windows Active Directory, хранят и извлекают учетные данные пользователя. Служба Active Directory была выпущена 17 февраля 2000-го и уже 21 год помогает организациям управлять учетными данными. Но сейчас перед нами встали новые вызовы.

Согласно отчету компании FireEye по прогнозам в сфере информационной безопасности на 2021 год (https://bit.ly/3nZBpfQ), около 95 % компаний в разных формах присутствуют в облачной среде.

Поэтому зададим следующие вопросы.

1. Как позволить пользователям задействовать учетные записи Active Directory для доступа к облачным ресурсам?
2. Как реализовать *единый вход* (single sign-on, SSO) для облачных приложений?
3. Как защитить учетные данные при их появлении в облаке и незащищенных сетях?
4. Как обеспечивать соответствие требованиям при переходе в облако?
5. Как выявлять/обрабатывать потенциальные утечки информации?

Чтобы ответить на них, нам требуется такое распределенное высоконадежное средство управления идентификацией и доступом, как Azure Active Directory. Это не значит, что оно заменит Windows Active Directory. Это различные продукты с множеством разных характеристик. Но оба они могут работать совместно для решения вопросов доступа и безопасности в двух средах — локально и в облаке. Множество разделов этой книги посвящено *гибридной идентификации*. Кроме того, вся информация скомпонована так, чтобы подчеркнуть важность защиты учетных данных.

Что такое идентичность

Слоны — удивительные создания. Слонихи остаются в стаде всю жизнь. При рождении слоненка молодые самки из стада помогают матери заботиться о малыше. Слоненок весит примерно 115 кг, а его рост около 1 м. Поначалу зрение у детеныша не очень четкое. Но он идентифицирует свою мать среди других молодых слоних по прикосновению, запаху и звукам. Такие общественные насекомые, как муравьи, распознают различные касты в собственной колонии по запаху тела. Таким же образом они выявляют муравьев из других колоний.

Что касается людей, то мы используем различные способы для уникальной идентификации человека. В повседневной жизни мы распознаём людей по имени, лицу, голосу, запаху, жестам, форме одежды и т. д. Уникальность личностей описывается идентичностью. Однако, чтобы доказать идентичность, нам нужно применять формальные методы идентификации, такие как паспорт, водительское удостоверение и регистрация по месту жительства. Эти методы признают многие государственные органы. Пока мы говорили лишь о физической идентичности. Но как нам привнести ее в цифровой мир? Для этого наша цифровая идентичность (digital identity) должна представлять идентичность физическую.

Например, когда я впервые записывался к терапевту, там проверили удостоверяющий мою личность документ и верифицировали мою личность. Затем мне

присвоили уникальный номер в Национальной системе здравоохранения. По этому номеру меня распознаёт компьютерная система. Когда я подключался к интернету, провайдер попросил меня установить уникальный пароль. Он будет применяться для подтверждения моей идентичности в дальнейшем при звонках в службу поддержки. В различных системах, приложениях и сервисах предусмотрены разные методы установления цифровой идентичности. Они используют базы данных и каталоги для хранения связанных с цифровой идентичностью сведений.

Однако важно помнить, что цифровая идентичность не всегда представляет человека. Она может представлять другие сущности, такие как устройства, приложения, сервисы, группы и организации. Цифровые идентичности становятся все более динамичными. Например, ваш профиль в соцсети представляет собой цифровую идентичность. Он обновляется на основе загружаемых вами изображений, размещаемых сообщений и появления новых друзей. Это не идентичность живого человека. Цифровая идентичность может часто обновляться на основании атрибутов и полномочий доступа. В наше время различные системы позволяют пользователям применять одну форму цифровой идентичности для получения доступа. Например, учетная запись Microsoft может давать доступ к локальным приложениям и приложениям SaaS (ПО как услуга). Такие федеративные цифровые идентичности обеспечивают приобретение лучшего потребительского опыта. Служба Active Directory может управлять и цифровыми идентичностями, и федеративными цифровыми идентичностями.

Прежде чем перейти к основам Active Directory, хочу рассказать о некоторых тенденциях в управлении доступом и идентификацией пользователей и взглянуть, насколько Active Directory вписывается в эту картину.

Будущее управления идентификацией и доступом

В двух предыдущих разделах я несколько раз использовал выражение «управление идентификацией и доступом» (Identity and Access Management, IAM). Что же оно означает? Управление идентификацией и доступом — это решение, применяемое для регулирования жизненного цикла доступа пользователя в рамках организации. Его основная задача — убедиться в том, что правильный человек имеет правильный доступ к правильным ресурсам по правильным причинам. Решения управления доступом и идентификацией пользователей в основном включают в себя четыре компонента.

1. Хранилище учетных записей (служба каталогов).
2. Набор инструментов для предоставления пользователям привилегий и доступа к ресурсам, их изменения и удаления.

3. Служба регулирования доступа и привилегий с помощью политик и рабочих процессов.
4. Система аудита и отчетности.

Согласно приведенному ранее определению сама по себе Active Directory не является системой управления идентификацией и доступом, но играет важнейшую роль в этой системе. Элемент каталога системы управления идентификацией и доступом — это не только Microsoft Active Directory, это может быть любой каталог. Однако мы знаем, что Microsoft Active Directory — наиболее широко распространенная на рынке служба каталогов. Успех решения IAM опирается на четыре ранее упомянутых мною столпа. Как объяснялось в предисловии, IAM — это ключевой фактор цифровизации. Что же ждет IAM в дальнейшем?

Рост киберпреступности

Для большинства из нас 2021-й был годом взлетов и падений. Вместе с пандемией COVID-19 нас охватила неопределенность, изменившая наше будущее во многих отношениях. Возможно, вам пришлось пересмотреть приоритеты и сдвинуть некоторые планы на несколько лет. В дополнение к этому всем нам пришлось озаботиться своим ментальным здоровьем. Киберпреступники — тоже люди. Можно было бы подумать, что пандемия ударила и по их деятельности. Но это не так. Похоже, они нашли возможности даже во время пандемии. Вместо снижения уровня киберпреступности мы увидели огромный рост числа происшествий. По сообщениям ФБР, в 2020 году наблюдался 300%-ный рост киберпреступности (https://bit.ly/3o3uguL). Что касается индустрии здравоохранения, то можно было ожидать хоть какого-то уважения, ведь она была нашим спасательным кругом во время пандемии. Но для преступников это стало лишь еще одной возможностью. Отчет по результатам расследования компании Verizon об утечках данных за 2020 год (https://vz.to/3CQvPCL) подтверждает 58%-ный рост количества утечек данных в индустрии здравоохранения, большинство из которых были финансово мотивированными атаками. Кроме того, такие атаки с каждым днем становятся все более изощренными. Отличным примером служит недавняя атака хакерской группы Nobelium. Компания — разработчик ПО SolarWinds Inc. занималась решениями для контроля сетевых устройств, серверов, хранилищ, приложений и управления ими. 12 декабря 2020 года она объявила о тщательно подготовленной атаке на ее платформу Orion, которая затронула 18 000 клиентов SolarWinds, включая министерства торговли, обороны, энергетики, национальной безопасности, иностранных дел (Государственный департамент) и здравоохранения США. Эта атака стала одним из крупнейших происшествий в сфере информационной безопасности за многие годы. По данным Microsoft (https://bit.ly/3q6wSec), 44 % жертв этой атаки представляли область информационных технологий, а 18 % были правительственными учреждениями.

Атака стала настоящей вехой в развитии киберпреступности по следующим причинам.

- Вместо того чтобы атаковать непосредственно важные цели, хакеры выбрали в качестве мишени обычного поставщика.
- Они получили доступ к SolarWinds еще в сентябре 2019-го.
- Для проверки способности внедрить вредоносный код в сборку ПО хакеры осуществили пробный заход в версию платформы Orion от октября 2019 года.
- Двадцатого февраля 2020 года хакеры внедрили вредоносный код в файл `SolarWinds.Orion.Core.BusinessLayer.dll` от этой даты.
- Содержащие вредоносный код обновления от компании SolarWinds стали доступны клиентам с 26 марта 2020 года.
- В июне 2020-го хакеры удалили вредоносный код из среды SolarWinds.
- Согласно отчету FireEye (https://bit.ly/3ER8Isq) первоначальный, спящий период атаки мог составлять до двух недель. Это значит, что даже если вредоносный код уже попал в систему, немедленно заметить это было нельзя.
- На уже вскрытой системе хакеры могли инициировать такие процессы, как передача файлов/данных на сторонние серверы, запуск исполняемых файлов, сбор информации о системе, включая регистрационные данные пользователей, перезагрузка сервера и отключение системных служб.
- После получения регистрационных данных злоумышленники применили технику бокового перемещения (Lateral Movement) на локальном ПО для получения доступа к серверу федерации Active Directory (ADFS).
- После получения привилегий для создания токенов SAML хакеры использовали их для доступа к облачным сервисам, таким как Microsoft 365.
- Атака на SolarWinds стала первой, в ходе которой применялся метод Golden SAML.

Эта атака научила нас следующему.

- **Важен подход к безопасности на основе нулевого доверия (Zero Trust).** Подход к информационной безопасности на основе нулевого доверия предотвращает не только утечку данных, но и применение после нее техники бокового перемещения. Утечку данных следует подразумевать всегда. Далее в этой главе подход на основе нулевого доверия будет рассмотрен подробнее.
- **Атака на локально установленное ПО была применена для получения доступа к облачным ресурсам.** В ходе этой атаки киберпреступники получили привилегии для доступа к среде ADFS, позволяющей создавать токены SAML. Они позволили им получить беспарольный доступ к облачным службам. Как правило, коммерческие организации уделяют больше внимания защите облачных ресурсов, но эта атака показала, что следует задуматься о полном жизненном цикле получения доступа.

Все атаки имеют общие черты. Все они стремятся для начала получить какой-либо доступ к системе.

Это может быть имя пользователя и пароль, сертификат или даже токен SAML. Получив начальный доступ, хакеры применяют технику бокового перемещения, пока не проникнут к учетным записям с привилегиями, которые помогут выполнять такие задачи, как кража данных, вызов сбоев или ведение шпионажа. Поэтому перед IAM стоит непростая задача защиты цифровых идентичностей от растущей киберпреступности.

В борьбе с киберпреступностью организациям приходится решать и другие сложные проблемы. Согласно отчету о влиянии COVID-19 на службы безопасности в корпоративной сфере ИТ, изданному ISC2 (https://bit.ly/3mLiJkq), перед организациями стояли следующие вызовы:

- в период пандемии около 20 % предприятий были вынуждены сократить бюджеты на обеспечение информационной безопасности;
- 36,4 % организаций сферы информационной безопасности приостановили набор персонала;
- 31,5 % организаций сферы информационной безопасности сократили рабочее время инженеров;
- 25,1 % организаций использовали для снижения эксплуатационных расходов принудительные неоплачиваемые отпуска;
- 21,7 % организаций сферы информационной безопасности снизили зарплаты инженеров;
- 17,4 % организаций сферы информационной безопасности сократили штаты путем временного увольнения.

Мы уже испытываем огромный недостаток квалифицированных кадров в сфере информационной безопасности. Пандемия COVID-19 негативно повлияла на финансовое состояние некоторых коммерческих организаций. По этой причине и в ближайшие годы организации ждут трудности с финансированием проектов информационной безопасности и совершенствования ее навыков.

Безопасность на основе нулевого доверия (Zero Trust)

В период пандемии COVID-19 большинство коммерческих организаций не могло позволить служащим работать из дома. Нельзя защитить корпоративные и учетные данные, заходя в незащищенные домашние сети с использованием того же подхода, что и для закрытых сетей. То, что у большинства компаний не было времени, чтобы оценить риски, связанные с удаленной работой, и подготовиться заранее, дало огромные возможности киберпреступникам. Риски, связанные с удаленной работой, до сих пор настигают большинство компаний. Согласно отчету IBM (https://ibm.co/3wwOSjf) удаленная работа увеличила сред-

ние издержки от утечек данных на 137 000 долларов. По данным исследования, проведенного Malwarebytes (https://bit.ly/3HUQWXc), 20 % респондентов сообщили о том, что сталкивались с нарушениями систем безопасности в результате удаленной работы; 44 % подтвердили, что не проводили для служащих обучения по вопросам информационной безопасности с акцентом на потенциальные угрозы в связи с работой из дома.

Интересно, что это исследование также подтвердило, что только 47 % служащих были осведомлены о рекомендациях по обеспечению информационной безопасности в ходе работы из дома.

Эта статистика демонстрирует то, что внезапный переход к работе из дома создает риски для компаний. Она также подтверждает, что традиционной подход «охраны периметра» не соответствует современным требованиям информационной безопасности. Наилучший способ решить этот вопрос — принять стратегию безопасности на основе нулевого доверия. Модель безопасности на основе нулевого доверия основана на трех главных принципах.

- **Явная верификация.** Означает необходимость одинаковой верификации всех до единого запросов доступа. Она не должна основываться на сетевом расположении, лице или роли. В ходе атаки, предпринятой хакерами из группы Nobelium, было хорошо заметно, что при наличии явной верификации ее можно было предотвратить на многих стадиях. Традиционные модели безопасности основаны на подходе «доверяй, но проверяй», в то время как модель с нулевым доверием — это противоположный вариант, определяемый как «никогда не доверяй, всегда проверяй».
- **Принцип наименьших привилегий.** Почти все инженеры отделов ИТ обычно имеют права администратора домена или администратора предприятия. Но некоторые применяют их лишь для выполнения базовых задач администрирования, таких как сброс пароля. Доступ с минимумом привилегий означает, что пользователи имеют только те привилегии, которые необходимы для выполнения поставленных перед ними задач. Это предотвращает использование хакерами техники бокового перемещения и не дает им завладеть привилегированными учетными записями.
- **Презумпция нарушения.** Киберпреступники — тоже люди. Невозможно закрыть все двери, преступники всегда найдут способ проникнуть внутрь. Время от времени они меняют тактику и методы. Нам следует допускать существование нарушения и ответить на важные вопросы: если нарушение произошло, как его распознать, как быстро мы можем сделать это? Чтобы ответить на них, необходимы инструменты и службы:
  - для сбора различных журналов системы;
  - эффективного анализа данных;
  - анализа поведения пользователя;
  - обнаружения отклонений от нормы.