CYBERARK

ТРИ ЭТАПА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИВИЛЕГИРОВАННЫХ АККАУНТОВ

Практические рекомендации на основе передового опыта

www.cyberark.com

Содержание

Что такое привилегированные аккаунты?

Привилегированные аккаунты ежедневно используются для изощренных и внутренних атак, направленных на хищение ценной конфиденциальной информации. Именно поэтому в базовых стандартах обеспечения кибербезопасности, включая Council on Cyber Security Top 20 Critical Security Controls, NIST и других, постоянно подчеркивается важность защиты, контроля и мониторинга привилегированных аккаунтов. Специалисты в области безопасности единодушны в том, что эти аккаунты являются ключами к цифровой инфраструктуре компании. Так что же они собой представляют и как примеры передового опыта могут помочь организациям не стать жертвой злоумышленников?

Привилегированные аккаунты, как и учётные записи обычных пользователей, включают действительный набор учётных данных для получения доступа к конкретной системе или системам в отдельно взятой сети. Однако их отличие заключается в том, что учётные данные привилегированных аккаунтов предоставляют расширенный неограниченный доступ к базовой платформе, который не могут получить непривилегированные пользователи. Эти аккаунты используются системными администраторами для управления сетевыми устройствами, устранения неполадок, запуска служб или коммуникации между приложениями. Недостаток в том, что те же самые учётные данные, помогающие реализации бизнес-процессов, могут легко применяться внешними или внутренними злоумышленниками для нанесения значительного ущерба сети и всей организации.

Виды привилегированных аккаунтов

В корпоративной среде насчитывается множество форм привилегированных аккаунтов, и их количество обычно в два или три раза превышает число сотрудников. Однако при отсутствии надлежащей защиты, чёткого управления и мониторинга все они создают угрозу безопасности. Для корпоративных сред характерны следующие виды привилегированных аккаунтов:

Аккаунты локальных администраторов — это неперсональные аккаунты с административным доступом только к локальному узлу или экземпляру. Они постоянно используются ИТ-специалистами для обслуживания рабочих станций, серверов, сетевых устройств, баз данных, мейнфреймов и т. д.

Обычно для большего удобства они имеют одинаковый пароль в рамках всей платформы или организации. Этот общий пароль для тысяч узлов служит причиной уязвимостей, которые часто используются при кибератаках.

Привилегированные аккаунты пользователей — это именные учётные записи с административными правами на одной или нескольких системах. Как правило, это одна из наиболее распространенных форм привилегированного доступа в корпоративной сети. Она позволяет пользователям получать административные права, например, на своих локальных настольных ПК или системах, которыми они управляют. Зачастую эти аккаунты имеют уникальные и сложные пароли, а их широкие возможности на управляемых системах делают необходимым постоянный мониторинг их использования.

Аккаунты администраторов домена предоставляют привилегированный административный доступ ко всем рабочим станциям и серверам внутри домена. Их число невелико, но они обеспечивают наиболее широкий и беспрепятственный доступ ко всей сети. Поскольку они позволяют полностью управлять всеми контроллерами домена и изменять принадлежность любого административного аккаунта, их компрометация — всегда представляет собой наихудший сценарий для любой организации.

Аварийные аккаунты предоставляют непривилегированным пользователям административный доступ к защищенным системам в чрезвычайных ситуациях. Поскольку по соображениям безопасности для доступа к этим аккаунтам, как правило, требуется одобрение со стороны руководства, то этот процесс выполняется вручную, неэффективно и при отсутствии контроля.

Сервисные аккаунты могут включать в себя привилегированные локальные или доменные аккаунты, которые используются приложениями или службами для взаимодействия с операционной системой. В некоторых случаях сервисные аккаунты имеют привилегии администратора домена в зависимости от требований приложения, которым они используются. Локальные сервисные аккаунты могут взаимодействовать с различными компонентами Windows, что затрудняет координацию ротации паролей. Изменение пароля Active Directory или доменного сервисного аккаунта может быть ещё более сложным, так как это требует координации между несколькими системами. Эти трудности приводят к тому, что пароли сервисных аккаунтов меняются очень редко, что создает серьёзную угрозу для всего предприятия.

Аккаунты приложений служат для доступа приложений к базам данных, выполнения пакетных заданий и сценариев или получения доступа к другим приложениям. Эти привилегированные аккаунты обычно имеют широкий доступ к базовой информации компании в приложениях и базах данных. Пароли для этих аккаунтов часто встроены и хранятся в незашифрованных текстовых файлах. В связи с необходимостью повышения отказоустойчивости приложений подобная уязвимость распространяется на множество серверов. Она представляет значительный риск для организации, поскольку приложения часто содержат точные данные, на которые нацелены APT-атаки.

Обеспечение безопасности привилегированных аккаунтов

Отсутствие контроля и защиты привилегированных аккаунтов в корпоративных сетях становится уязвимостью, которая чаще всего используется для изощренных и внутренних атак. В связи с этим нельзя недооценивать преимущества обеспечения безопасности привилегированных аккаунтов. Независимо от ресурсов, для каждой организации может быть найдено практическое решение в рамках имеющегося бюджета. Практические рекомендации на базе передового опыта предлагают для поэтапного повышения уровня безопасности варианты от применения выполняемых вручную процессов до автоматизированных корпоративных решений, обеспечивающих аналитику и максимальную защиту. В этой статье описываются различные варианты обеспечения безопасности привилегированных аккаунтов для организаций.

Защита в ручном режиме

В конечном счете это лучше, чем полное бездействие, тем не менее защита, контроль и мониторинг привилегированных аккаунтов в ручном режиме могут быть утомительными, трудоемкими и дорогостоящими процессами. Крупные организации практически лишены возможности ежедневно делать это для тысяч привилегированных аккаунтов. Кроме того, подобный подход малоэффективен для организаций любого размера ввиду ограниченности масштабирования, контроля и отчетности. Жестко регулируемые среды, отвечающие требованиям нормативов HIPPA, SOX, PCI и иных стандартов, подразумевают необходимость аудита, который не сможет обеспечить даже самое эффективное ручное решение. Кроме того, ручные процессы анализа и оповещёния подвержены человеческим ошибкам, которые могут вызвать многомиллионные убытки, связанные с реагированием на инциденты, восстановлением и снижением продуктивности. Защита привилегированных аккаунтов с помощью ручного контроля — наименее зрелое и эффективное из всех доступных решений.

Решения по обеспечению безопасности привилегированного доступа

Ручное управление привилегированными идентификационными данными приводит к крайне низкой окупаемости инвестиций для средних и крупных предприятий. Следовательно, более эффективный и действенный подход для этих организаций — это приобретение собственного решения по обеспечению безопасности привилегированного доступа или заключение договора на предоставление подобной услуги. При интеграции с существующими системами обеспечения безопасности, такими как SIEM (управление информационной безопасностью и событиями безопасности), корпоративные решения, служащие для защиты, контроля и мониторинга привилегированных пользователей, сеансов и приложений, предоставляют крупным компаниям максимальные преимущества.

Независимо от выбранной стратегии, следует применять поэтапный подход и повышать безопасность решения с течением времени. Организации, которые не в состоянии обезопасить привилегированный доступ, не смогут защитить эти критически важные аккаунты. Однако существуют решения, обеспечивающие поэтапное и организованное развертывание. Внедрение оптимального решения в сочетании с непрерывным мониторингом и оптимизацией по мере изменения бизнес-среды позволяет организациям опережать новейшие и внутренние угрозы.

Практические рекомендации на основе передового опыта

Ниже приводятся лучшие практики, позволяющие организациям контролировать и защищать привилегированные аккаунты. Многие из них требуют только изменений процесса, а другие предусматривают внедрение инструментов или решений. Чтобы помочь вам определить наиболее эффективные действия, мы сгруппировали их по уровню зрелости.

Базовые меры

Подсчет и сокращение количества привилегированных аккаунтов в вашей организации.
Определение количества и расположения аккаунтов в среде — это важнейший первый шаг к принятию обоснованных решений в отношении их защиты от рисков. После инвентаризации привилегированных аккаунтов необходимо проанализировать их, а затем удалить ненужные для сокращения общего числа учётных записей, требующих управления.

Запрет привилегированного доступа для стандартных пользовательских аккаунтов.
Наличие отдельных аккаунтов для общего и административного использования позволяет организациям выявлять случаи злоупотреблений в отношении привилегированных аккаунтов. Кроме того, установление минимальных привилегий — это важный шаг для повышения безопасности сетевой среды организации.

Внедрение процесса приема и увольнения сотрудников, имеющих доступ к привилегированным аккаунтам.
Сотрудники должны понимать ответственность, которую накладывает привилегированный доступ, и проходить обучение существующим корпоративным политикам для предоставления прав администратора. Возможность привилегированного доступа должна регулярно пересматриваться для подтверждения его актуальности и необходимости. Процесс увольнения должен предусматривать блокировку всех привилегированных аккаунтов сотрудников и изменение паролей любых общих аккаунтов, к которым они имели доступ.

Искоренение практики использования аккаунтов с бессрочными паролями.
Пароли следует регулярно изменять для снижения их уязвимости перед средствами взлома и при обмене между сотрудниками.

Надежное хранение паролей.
Организации обязательно должны размещать свои привилегированные пароли в наиболее безопасной и зашифрованной системе хранения. Следует исключить использование конвертов, папок, таблиц, простых файлов и т. п. для хранения информации о привилегированных аккаунтах.

Необходимо предпринять все зависящие от организации меры по соотнесению всех действий с использованием общих административных аккаунтов с конкретным лицом.
Совместное использование учётных данных должно быть полностью исключено. Если это невозможно, следует обеспечить внедрение и контроль индивидуальной ответственности.

Промежуточные меры

Автоматическое изменение паролей привилегированных аккаунтов с периодичностью 30 или 60 дней.
Привилегированные пароли должны регулярно изменяться и быть сложными, трудно угадываемыми и уникальными среди аккаунтов. Однако политики паролей не должны быть излишне сложными, чтобы исключить нарушающее их поведение, такое как записывание паролей.

Использование одноразовых паролей, действительных только для одного сеанса регистрации или транзакции.
Частая смена паролей, например после каждого использования, заставит злоумышленников тратить гораздо больше времени и средств для их получения, что значительно снижет риск атаки.

Внедрение записи сеансов для ключевых ресурсов, серверов и доступа третьих лиц.
Мониторинг и регистрация действий с привилегированными аккаунтами для ключевых активов, серверов и доступа третьих лиц.

Исключение интерактивной (пользовательской) авторизации для сервисных аккаунтов.
Интерактивное использование сервисных аккаунтов представляет собой серьезную уязвимость, которую довольно легко устранить путем их инвентаризации.

Внедрение процесса изменения жестко закодированных или встроенных паролей для сценариев и сервисных аккаунтов.
Без надлежащих процессов изменение жестко закодированных паролей может легко нарушить какие-либо компоненты инфраструктуры. Автоматизированная система изменения встроенных паролей в сценариях и сервисных аккаунтах повышает уровень безопасности без дополнительного риска.

Целенаправленный аудит использования административных привилегированных функций и мониторинг для выявления аномального поведения.
Регистрация всей активности и генерация уведомлений о необычном поведении предоставляют дополнительную информацию о доступе к привилегированным аккаунтам и их использовании. Интеграция с системами обеспечения безопасности значительно повышает скорость анализа и исследования потенциальных инцидентов и/или нарушений.

Высокоэффективные меры

Использование автоматизированных инструментов для блокировки неактивных привилегированных аккаунтов.
Обеспечение безопасности привилегированного доступа на предприятии сопряжено с трудностями и человеческими ошибками. Применение ручных решений и институциональных знаний лучше, чем полное бездействие, однако автоматизация способна обеспечить гораздо более высокую эффективность.

Использование многофакторной аутентификации для всего административного доступа, включая права администратора домена.
Этот дополнительный уровень безопасности значительно затрудняет использование привилегированных идентификационных данных в качестве мишени для новейших угроз, хотя и не обеспечивает полную защиту. Многие платформы (например, устаревшие сетевые устройства или бизнес-приложения) могут не поддерживать многофакторную аутентификацию. Развертывание решения по обеспечению безопасности привилегированного доступа с поддержкой мультифакторной аутентификации устраняет необходимость ее изначальной реализации на целевых устройствах.

Внедрение автоматизированной проверки и синхронизации паролей для обеспечения их актуальности на всех системах.
Автоматизация имеет большое значение при управлении привилегированными идентификационными данными. Постоянное создание и удаление аккаунтов вызывает необходимость использовать автоматизированные системы для управления паролями и их проверки.

Регулярное изменение и проверка жестко закодированных паролей, встроенных в приложения.
Аудит всех аккаунтов и внедрение автоматизированного управления учётными данными приложений позволяют регулярно проводить ротацию паролей без дополнительного риска. При отсутствии управления аккаунтами приложений компании не смогут полностью исключить риск, связанный со всеми привилегированными аккаунтами в своей инфраструктуре.

Развертывание решения с возможностью прямого подключения к целевой системе без демонстрации пароля пользователю.
Предотвращение раскрытия привилегированных паролей конечным пользователям создает дополнительный уровень безопасности, сокращает расходы на обслуживание коллективных аккаунтов и одновременно повышает удобство работы конечных пользователей.

Внедрение шлюза для исключения прямого доступа привилегированных пользователей к конфиденциальным ресурсам в ИТ-инфраструктуре.
Шлюз между конечным пользователем и конфиденциальными ресурсами снижает уязвимость сети перед вредоносным ПО и не позволяет использовать привилегированные учётные данные на конечных точках и настольных ПК администраторов.

Применение процедур подтверждения доступа к учётным данным, включая двойной контроль и интеграцию с системами регистрации запросов.
Процессы двойного контроля обеспечивают необходимый баланс для предотвращения использования привилегированных учётных записей внутренними злоумышленниками и позволяют четко контролировать доступ пользователей.

Внедрение записи сеансов с привилегированным доступом.
Обязательная регистрация всех действий на привилегированных аккаунтах посредством записи сеансов с возможностью их воспроизведения для ретроспективного и управленческого анализа.

Упреждающее выявление вредоносных действий.
Решение для мониторинга, обнаружения и оповещёния об аномальном поведении привилегированных пользователей — это критически важный уровень оптимальной стратегии по обеспечению безопасности привилегированного доступа.

Заключение

Уязвимости учётных данных и/или привилегированных аккаунтов используются злоумышленниками в 100% случаев. При такой статистике сложно представить себе организацию, которая до сих пор закрывает на это глаза. Цена бездействия постоянно отображается в бесконечном потоке отчетов, подробно описывающих очередной случай компрометации данных в крупных и небольших компаниях по всему миру. Каждая организация в любой отрасли и любом секторе экономики подвержена риску несанкционированного использования своих привилегированных аккаунтов.

При внедрении решения для упреждающей защиты и мониторинга привилегированных аккаунтов организациям следует оценивать потребности бизнеса с учетом доступных вариантов и выбирать оптимальный подход на основе существующих рекомендаций на основе передового опыта. Для повышения уровня защиты процесс обеспечения безопасности привилегированных аккаунтов должен идти непрерывно с постоянной оценкой и корректировкой существующей ситуации.