Адаптивное управление привилегиями: Обзор для руководства

White Paper

Содержание

Содержание 1
Привилегированные учетные данные 2
Какие риски они несут. 2
Как «утекает» привилегированный доступ 3
Бизнес-драйверы 4
Меньше замечаний аудиторских проверок - меньше затрат на приведение в соответствие требованиям ..5
Контроль внутренних угроз....6
Лучшие практики 6
Определение целей проекта 7
Автоматизация процессов управления учетными данными 7
В заключение 9
Следующие шаги 9
О компании Вэб Контрол....9

Привилегированные учетные данные

Индивидуальные учетные данные не являются единственным типом логинов в вашей сети. Персонал, который обслуживает Серверы, сетевые компоненты и программное обеспечение используют специальные учетные записи с повышенными правами доступа, необходимыми для установки нового аппаратного и программного обеспечения, конфигурирования сервисов и обслуживания ИТ-инфраструктуры.

Привилегированные учетные данные предоставляют неограниченный доступ для просмотра и изменения данных, изменения параметров конфигурации, и запуска программ. Обычно привилегированные учетные записи привязаны к аппаратным и программным комплексам (а не к одному пользователю), и предоставляют «супер-пользователю» доступ практически к каждому ресурсу в вашей сети, включая**:**

- Операционные системы, которые работают все компьютерные платформы
- Служба каталогов, которые управляют доступом к сети
- Бизнес-приложения, базы данных и промежуточного ПО
- Сети и устройства системы безопасности
- Резервное копирование, другие службы ПО, устройства
- Гипервизоры, управляющие виртуальными машинами (VM) в вашей сети ·
- SSH ключи и сертификаты

Привилегированные учетные записи не используются только лицами. **Бизнес-приложения и компьютерные услуги** также должны хранить и использовать привилегированные учетные данные для аутентификации с баз данных, промежуточного по и другие приложения, при запросе конфиденциальной информации и вычислительных ресурсов.

Какие риски они несут.

В отличие от личных учетных данных для входа конечных пользователей, **привилегированные учетные данные в большинстве организаций не управляются системно.** Это означает что, по всей вероятности:

- Ваша организация не имеет полного актуального перечня привилегированных учетных записей, которые есть в Вашей сети
- У Вас нет достоверных знаний, какие привилегированные учетные записи известны каким лицам
- У Вас нет доказательств, кто использовал эти привилегированные учетные записи для получения доступа к любому из ваших ИТ-ресурсов, когда и с какой целью
- Нет никакого способа проверить, что каждый из паролей ваших привилегированных учетных записей криптографический прочен, достаточно уникален и меняется достаточно часто, чтобы быть в безопасности
- У Вас нет полного списка паролей привилегированных учетных записей, хранящихся в приложениях, и нет способа узнать, какие сотрудники внутри компании и представители производителей оборудования и ПО знают эти учетные данные, которые могут быть использованы для доступа к конфиденциальной информации

Краткое описание привилегированных учетных записей, присутствующих в типичной корпоративной сети, и анонимные действия, которые могут быть принятый персоналом со знанием этих логинов, показаны на рисунке 1 на следующей странице.

ROLES	ASSETS	ACCOUNTS	ANONYMOUS ACTIONS
• System Administrators • Contactors • Integrators • Security Administrators • IT Managers	Windows, Linux, UNIX, and Mainframe Computers 	• Administrator • Root • Super User • Service	• Read, copy and alter data • Change security settings • Create and delete accounts • Enable and remove file shares • Run programs
• System Administrators • IT Managers	Directories 	• Admin • Administrator • Root	• Read, copy and alter data • Add and delete users • Change user privileges • Enable remote access
• App Administrators • App Developers • Webmasters • Contract Developers	Application Tiers 	• Service • Config Files • ASP.Net • Run As • DB Connection	• Modify back-end applications • Alter public-facing websites • Read and change DB records • Access transition data
• DB Administrators • App Developers • App Administrators • Contract Developers • Integrators	Databases 	• SA • Root • SYS • SYSDBA	• Read and change DB records • Access transaction data • Alter DB configuration and schema • Add and modify stored procedures
• Network Administrators • Security Administrators	Network and Security Appliances 	• Root • Enable • Admin	• Alter configuration settings • Change security and QoS policies • Grant and deny network access • Access data feeds • Enable and disable monitoring
• System Administrators • Backup Operators • Network Administrators • Contractors	Backup and Service Infrastructure 	• Administrator • Root • Super User • Service	• Browse and save archives • Access transition data • Delete saved files • Change configuration settings
• Cloud Administrator • Cloud User • Contractors	Cloud Platforms 	• Microsoft Azure • Amazon Web Services • Rackspace • Force.com • IBM SoftLayer	• Create and delete virtual environments • Configure operating systems • Provision users • Install applications

Рисунок 1 – что можно негласно сделать с помощью неуправляемых привилегированных учетных записей

Как «утекает» привилегированный доступ

IT персонал ради удобства часто дает одной и той же привилегированной учетной записи права на управление многочисленными аппаратными и программными ресурсами и потом редко меняет пароли. В результате знание пароля доступа может быстро и неуправляемо «расползаться» среди пользователей по мере того как:

- Развертывание новых аппаратных средств и приложений множит привилегированные учетные записи, известные многим людям
- Изменения в корпоративной структуре, такие как слияния, ИТ-аутсорсинг и реорганизации, требуют изменения ролей работников и раскрытие пароля для большего числа персонала
- Работники со знанием паролей привилегированной учетной записи покидают организацию и уносят с собой знание секретных паролей
- Пользователи, исходя из удобства, копируют и делятся SSH-ключами, и тем самым теряют контроль над учетными данными
- Неавторизованные пользователи и вредоносные программы легко раскрывают криптографически слабые, многократно используемые и нечасто изменяемые пароли привилегированных УЗ для нелегального вывода учетных данных.

Адаптивное управление привилегиями - защита от кибератак

К счастью, программное обеспечение управлением привилегиями поможет Вам активно смягчать кибер - угрозы, преодолевающие традиционные средства защиты. Основная мысль заключается в том, чтобы менять привилегированные учетные данные быстрее, чем хакеры могут использовать их. Решения управления привилегиями обеспечивают автоматическую остановку вторжений в режиме реального времени, чтобы:

- Прямо под атакой создавать **гибкую, автоматизированную и быструю** киберзащиту
- **Остановить горизонтальное распространение вторжения** по сети**.**
- **Управлять жизненным циклом привилегированных учетных данных** в сети предприятия и в облаке
- **Защитить логины приложений и вести запись активных сессий** в сети компании, в облаке, и в Интернете
- **Быстро противодействовать новым классам угроз -** включая атаки pass-the-ticket
- **Защитить соответствие** стандартам безопасности PCI DSS, HIPAA, ISO27001, NIST, FISMA, и т.д.

Бизнес-драйверы

Мотивация для реализации управления привилегированными учетными записями зачастую начинается с необходимости немедленно оправиться от кибер-атак, устранения негативных замечаний аудиторов, или приказа от службы GRC (управление, контроль рисков и соответствие требованиям регуляторов). Дополнительные бизнес-драйверы могут включать в себя желание снизить постоянные издержки и неопределенность, связанные с подготовкой к аудиту, стремление снизить риски от внутренних и внешних угроз и стремление повысить эффективность ИТ-персонала, как описано в следующих разделах.

Уменьшение количества кибератак

Недавние кибер-атаки демонстрируют, как отказ от защиты привилегированного доступа может привести к потере конфиденциальных данных и сбоев в критически важных для бизнеса сервисах. В дополнение к негативным сообщениям прессы и ущербу репутации, в каждом случае организация-жертва понесла значительные расходы для исправления нарушения, понесла штрафы и штрафы, или и то, и другое и, в соответствии с отчетом Mandiant M-Trends Report 2016, обнаружение взлома занимает в среднем 146 дней. Это означает, что у злоумышленников есть достаточно времени для поиска в вашей сети административных учетных данных, которые им необходимы для нанесения вреда. Вот примеры из недавних новостных заголовков:

- Yahoo говорит: данные украдены с 1 млрд счетов. CNN. 14 Декабря 2016
  Yahoo теперь считает, что в Августе 2013 «несанкционированной третьей стороной» украдены данные более чем одного миллиарда пользовательских аккаунтов.
- LinkedIn data breach blamed for multiple secondary compromises. CSO Online. Июнь 22, 2016. *“ «В каждом случае утечек из списка LinkedIn есть или одинаковые пароли или отсутствие двухфакторной аутентификации или программное обеспечение удаленного доступа от таких сервисов, как GoToMyPC, LogMeIn и TeamViewer »..”*
- Office Of The Comptroller Of The Currency Disclosed A Data Breach. PYMNTS. Октябрь 31, 2016.
  “Согласно отчету банковского регулятора потеря данных была связано с бывшим сотрудником, удалившим более 10 000 записей без разрешения.”

Рисунок 2 – жертвы кибер-атак в заголовках прессы

Меньше замечаний аудиторских проверок - меньше затрат на приведение в соответствие требованиям

Сегодняшние регулятивные мандаты могут привести к значительным издержкам, поскольку организации к каждой проверке вынуждены постоянно повторять свои действия по документированию соблюдения требованиям. Несоблюдение требований действующих стандартов может привести к прямым санкциям, негативному давлению на бизнес и значительным затратам, поскольку персонал потратит свое время на устранение негативных замечаний. К счастью, основные стандарты (в том числе SOX, PCI-DSS, HIPAA, FISMA и др.) разделяют в основном общие требования, когда дело доходит до обеспечения привилегированного доступа.

Чтобы оставаться в рамках соответствия основным нормативам, минимальные процессы управления привилегиями должны предоставить:

- Список всех привилегированных учетных записей - в том числе административных учетных записей и учетных данных, используемых приложениями и службами - на всех аппаратных платформах
- Полный список лиц, уполномоченных для доступа к ресурсам и учетным записям
- Журналы доступа, подтверждающие политику «наименьших привилегий» и показывающие, кто на самом деле просил доступ к какому ИТ-ресурсу, когда, и с какой целью
- Проверяемый процесс по смене привилегированных паролей сразу после доступа, так что пароль не может быть повторно использован без явно задокументированного запроса на доступ.
- Средства управления предупреждениями для любой необычной активности
- Возможность документировать, что доступ ко всем активам аппаратного и программного обеспечения покрываются политиками организации
- Управление привилегированным доступом к приложениям
- Мониторинг/запись привилегированного сессий

Как описано ниже, существуют программные решения для автоматизации вышеописанных шагов, позволяющие значительно сократить расходы на ИТ-персонал.

Контроль внутренних угроз

Согласно отчету Verizon 2016 Data Breach Investigation Report, 77% нарушений данных вызываются инсайдерами. Парадокс - в то время как многие организации применяют такие меры, как физические замки и идентификационные карточки для контроля физического доступа, большинству из них не хватает процессов, необходимых для управления привилегированным доступом. Бесконтрольный привилегированный доступ позволяет отдельным лицам просматривать и изменять записи данных или изменять настройки конфигурации в любое время по сети. В конечном счете бесконтрольный доступ может привести к потерям, соизмеримым или большим по сравнению кражей физических ценностей.

Чтобы смягчить риски инсайдерских угроз, организации работают над созданием климата полной и прозрачной отчетности путем введения проверок и встречных проверок в процессах управления ИТ. Критическим элементом является контроль доступа к базам данных с правами администратора, серверам, поддерживающим приложения и другим компонентам, в которых хранятся конфиденциальные данные. Процессы управления привилегированными учетными данными могут позволить организациям применять принципы «наименьших привилегий», показывая, что люди используют только уровень разрешений, необходимых для выполнения их работы. Одновременно сводится к минимуму вероятность повреждения данных и непредвиденные перебои в обслуживании. Это важное замечание, так как строгое исполнение, например, парольных политик в ручном режиме увеличивает риски потери доступности или целостности критических данных

Повышение эффективности ИТ-персонала

Помимо совершенствования организации с точки зрения GRC*, эффективное управление процессами управления привилегированными учетными записями может повысить эффективность работы персонала путем внедрения средств для:

- Исполнения постоянных процессов по актуализации списка привилегированных учетных записей, присутствующих на программных и аппаратных ресурсах
- Сокращения времени и ошибок при изменении паролей привилегированных учетных записей за счет автоматизации
- Сокращения времени и повышение прозрачности процесса допуска к ресурсам при рабочем и аварийном привилегированном доступе к ПАК
- Автоматизация задачи журналирования доступов к ресурсам в соответствии с требованиями регуляторов
- Инструмент для анализа инцидентов, позволяющий быстро понять, кто, когда, сколько раз, и с какой целью запрашивал доступ к критическим ПАК
- Исключение затрат времени персонала на устранение замечаний внешнего и внутреннего аудита.

Лучшие практики

Эффективное управление привилегированными учетными данными представляет собой непрерывный цикл, как представлено на рисунке 3 ниже.

Рисунок 3 – Цикл управления привилегированными учетными записями

Этот процесс может быть разбит на четыре этапа, сокращенно I.D.E.A.:

- **Идентифицировать** (**Identify**) документирование всех критических ИТ-активов, их привилегированнх учетных записей и взаимозависимостей, присутствующих на всех платформах аппаратного или программного обеспечения.
- **Делегировать** (**Delegate**)доступ к учетным данным так, что только допущенный персонал, с использованием наименьших необходимых привилегий, с документальным подтверждением, может зайти на ресурс в установленное время и на оговоренный срок.
- **Усилить** (**Enforce**)правила по сложности пароля, частоте смены и распространять смененные пароли во все зависимые активы для предотвращения сбоев в обслуживании
- **Аудит**, (**Audit, alert and report**) тревожные оповещения, и отчетность по запрашиваему, цели, продолжительности каждого доступа с возможностью поиска и выделения аномалий

Определение целей проекта

Каждая реализация, с самого начала, должна начинаться с обсуждения всеми заинтересованными сторонами, включая руководителя ИБ, ИТ-директоров, ИТ-администраторов и других лиц, участвующих в управлении чувствительными ресурсами. Основные заинтересованные стороны это те, кому будет нанесен наибольший урон, если проект затянется, излишне загрузит работников или не приведет к ожидаемым результатам.

Следует определить основные цели проекта и затем решить кто из команды сможет наилучшим образом определить требования и рамки имплементации решения. Результаты процесса должны включать:

- Подробный, письменный анализ бизнес-целей организации
- Подробный документ по потребностям контроля привилегированного доступа в отношении систем, приложений и способов контроля
- И, как только решение выбрано, четкий список работ с учетом времени и затрат, необходимых для внедрения управлением привилегированными учетными записями, присутствующими в Ваших целевых системах и приложениях

Автоматизация процессов управления учетными данными

Программное обеспечение для управления привилегиями автоматизирует задачу каталогизации привилегированных учетных записей организации и их взаимозависимостей и помогает обеспечить полноту и актуальность результатов. Лучшие из решений могут использовать многочисленные источники для создания исчерпывающих списков привилегированных учетных данных, присутствующих в среде.

Как показано на Рисунке 4, **Enterprise Random Password Manager (ERPM)** от Lieberman Software в автоматическом режиме обнаруживает и регистрирует привилегированные учетные записи в широком

диапазоне серверных и настольных операционных систем, сетей и устройств резервного копирования, баз данных, веб-служб, бизнес-приложений и других ИТ-ресурсов.

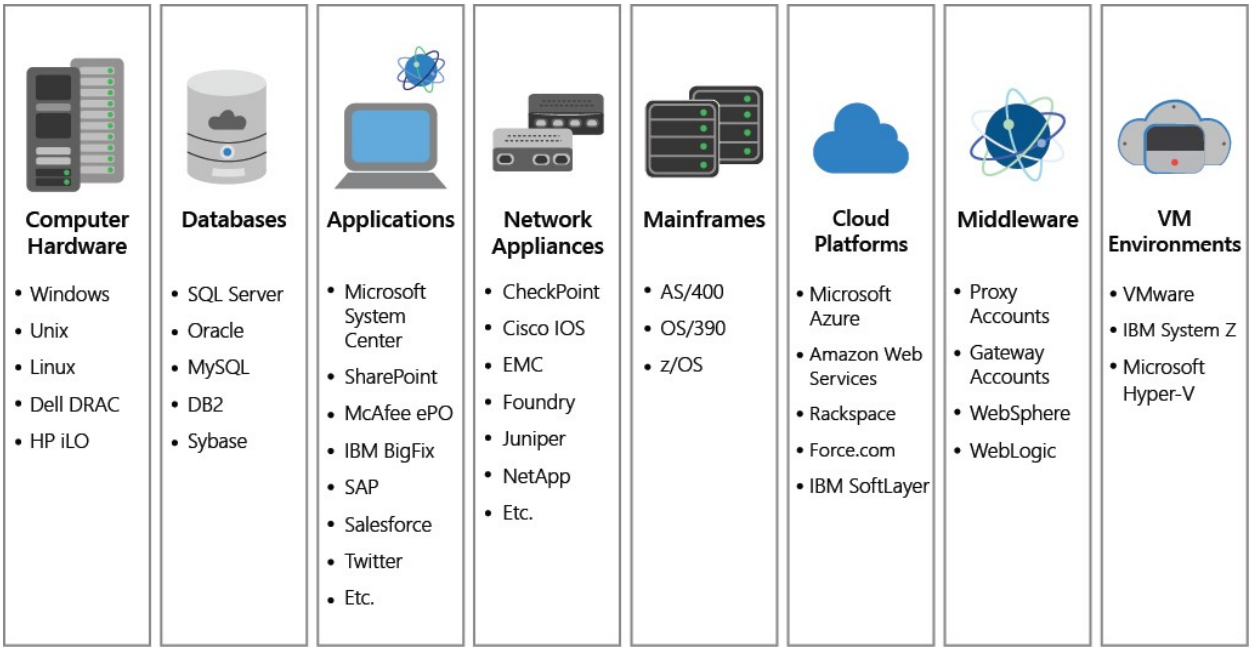

Рисунок 4 – уязвимости привилегированных учетных данных могут существовать на всех уровнях, и хакеры умело их используют. ERPM обеспечивает управление всеми перечисленными типами привилегированных учетных записей

ERPM в полном масштабе автоматизирует процесс управления привилегированными учетными данными. ERPM обнаруживает и сообщает о каждом расположении где используются привилегированные учетные записи - включая локальные и доменные учетные записи, настроенные службы, запланированные задачи, приложения, включая COM + и DCOM, веб-сайты IIS, базы данных, такие как Oracle, SQL Server и т. Д., А затем быстро распространяет изменения пароля во все места, на которые ссылается каждая учетная запись, чтобы предотвратить блокировки и сбои в обслуживании из-за учетных записей, которые в противном случае могут возникнуть, когда ручные процессы используют устаревшие учетные данные. ERPM идентифицирует, защищает и управляет привилегированными учетными данными, обнаруженными в системах, включая:

- Учетные записи **СуперПользователя**, правомочные изменять параметры конфигурации, запускать программы и выполнять другие административные обязанности
- **Учетные записи служб**, требующие привилегированный доступ
- Доступ **приложений к приложениям** - пароли, учетные записи, используемые веб-службами, бизнес-приложениями, программным обеспечением и практически любым другим типом приложений для подключения к базам данных, ПО промежуточного слоя и другими уровнями приложений
- **SSH ключи,** используемые для проверки подлинности отдельных лиц и приложений на системах Linux и UNIX по всей Вашей сети

ERPM защищает свои пароли в зашифрованной базе данных, к которой можно получить доступ с любого устройства, поддерживающего веб доступ. Пользователи получают пароли привилегированных учетных записей с помощью автоматизированного процесса, который улучшает существующую структуру управления идентификацией и доступом, и ускоряет делегирование доступа. Пароли автоматически повторно рандомизируются после использования. Доступен функционал введения временных рамок на восстановление паролей, принудительного окончания сессий администрирования, периодических верификаций паролей, таймаутов веб-сессий и фонетического проговаривания паролей

В рамках процесса изменения пароля, ERPM поддерживает пулы взаимозависимых учетных записей - **pooled account rotation**. Бывает, что системе есть ряд служб и/или приложений, обращающихся от имени одной учетной записи к какому-либо ресурсу. Если на ресурсе сменить пароль, то все службы и приложения должны быть снабжены новым паролем для этой учетной записи. И если хотя бы одна из этих служб или приложений будет на момент смены пароля недоступна, она не будет «оповещена» о смене пароля, при попытке доступа к корневому ресурсу сошлется на старый пароль, получит отказ в доступе и может вызвать отказ работы системы.

Функция **pooled account rotation** помогает защититься от подобных системных сбоев и блокировок, возникающих в случаях, если на момент смены пароля управляемые системы оказываются вне доступа из-за проблем с сетью, обслуживания и т.д. При невозможности сменить пароль, система откатывает изменения во всем пуле, возвращая старые пароли, и оставляя их неизменными, пока возможность смены паролей для всех систем пула не будет восстановлена.

Администраторы ERPM имеют возможность настраивать пулы учетных записей, содержащие любое количество учетных записей.

ERPM также обнаруживает, коррелирует, ротирует и надежно хранит ключи SSH, чтобы помочь Вам определить источник и распространение этих файлов и поддерживать безопасность Вашей инфраструктуры. ERPM обнаруживает ключи SSH на Linux и UNIX системах, изменяет их и сохраняет новый закрытый ключ в безопасном хранилище. Авторизованные пользователи могут немедленно получить SSH доступ, либо получить закрытый ключ, который они могут копировать или делиться.

В заключение

По мере того, как регуляторы будут становиться все более осведомленными в угрозах, создаваемых неуправляемыми привилегированными учетными записями, Ваша организация будет сталкиваются со возрастающим давлением с их стороны. Это давление будет направлено на усиление контроля над привилегированными учетными записями. Хакеры также усилили внимание на эти учетные записи, увеличив частоту атак, использующих разделенные или учетные записи с повышением привилегий, с целью получить контроль над сетями организаций - жертв.

По счастью, программное обеспечение для управления привилегированными учетными записями может помочь Вам получать на постоянной основе данные по привилегированным учетным записям по всей Вашей сети и предоставить проверенный журнал контроля доступа. Успешная реализация может также сэкономить время ИТ-персонала, по требованию мгновенно предоставляя списки учетных записей и уменьшая потребность в ручных процессах для обнаружения, изменения и документирования учетных записей.

Следующие шаги

Организации, которые хотят получить более полное представление о потенциальных рисках небезопасных привилегированных учетных записей в своем ИТ окружении, могут связаться с дистрибутором Lieberman Software на территории EMEA – компании Вэб Контрол для организации **пробного использования ERPM**. В ходе пилотного проекта ERPM документирует потенциальные риски, инфраструктуру и составит списки привилегированных учетных записей по аппаратной/программной платформам, аккаунтам и типу служб. Затем он защитит привилегированные учетные записи в Вашей сети и предоставит контрольный журнал для каждого запроса на доступ. Программное обеспечение для проведения испытаний ERPM доступно **бесплатно** для прошедших квалификацию организаций. За дополнительной информацией обращайтесь по электронной почте nvalaev@web-control.ru

О компании Вэб Контрол

Основная специализация - решение задач, связанных с обеспечением внутренней безопасности, оптимизацией и повышением эффективности использования ИТ и телекоммуникационных инфраструктур. Наши технологические решения составляют взаимодополняющую экосистему для формирования эффективной и безопасной ИТ среды, превращая Web технологии в эффективный инструмент бизнеса.

Главная задача, которую мы ставим перед собой - помочь максимально реализовать потенциал существующей инфраструктуры и сохранить уже сделанные и новые инвестиции в сеть и сетевые приложения для повышения конкурентоспособности бизнеса наших клиентов. www.web-control.ru