CYBERARK®

ПРОГРАММА CYBERARK PRIVILEGED ACCESS SECURITY CYBER HYGIENE (ГИГИЕНА ЗАЩИТЫ ПРИВИЛЕГИРОВАННОГО ДОСТУПА В ЦИФРОВОМ ПРОСТРАНСТВЕ)

Содержание

Введение

В программе кибербезопасности одной из наиболее эффективных профилактических мер является защита привилегированных аккаунтов, учётных данных и конфиденциальной информации. Организации признают, что этот процесс может быть сложным, особенно в крупных структурах, а безопасность привилегированного доступа, к сожалению, невозможно обеспечить раз и навсегда. Злоумышленники постоянно ищут уязвимости в ИТ-системах компаний.

Например, если год назад организация обеспечивала защиту привилегированного доступа, то сегодня у неё все могло измениться. Она может использовать новую инфраструктуру, новые приложения SaaS или приложения, созданные на базе методологий DevOps, расширенный портфель облачных решений, а также планировать консолидацию ЦОД. Для наиболее эффективного противодействия атакам злоумышленников организации должны иметь актуальную программу по обеспечению безопасности привилегированного доступа, которая продолжит защищать их важнейшую инфраструктуру, приложения, данные заказчиков, интеллектуальную собственность и другие ключевые ресурсы.

Forrester Research сообщает, что «в результате утечки данных из Yahoo злоумышленникам получили доступ более чем к одному миллиарду записей о заказчиках», не считая компрометации около 500 миллионов записей[1].

Согласно отчету от 2017 года, «81% случаев утечки данных в результате взлома связан с украденными и/или ненадежными паролями»[2].

Для упреждающего снижения риска, связанного с получением привилегированного доступа злоумышленниками, организациям следует:

- Задействовать свое понимание наиболее распространенных типов атак с привилегированным доступом: как мыслит и ведёт себя злоумышленник в каждом случае, пытаясь использовать уязвимости организации?
- Уделять первостепенное внимание привилегированному доступу, учётным данным и конфиденциальной информации, а также определять потенциальные недостатки и уязвимости существующей программы обеспечения безопасности привилегированного доступа. Прежде всего те, которые могут поставить под угрозу критически важную инфраструктуру, наиболее ценные активы компании и т. д.
- Выработать наиболее эффективные меры по устранению этих недостатков и потенциальных уязвимостей. Что необходимо сделать в первую очередь? Каких результатов можно добиться быстро, а для чего потребуется долгосрочное планирование?
- Постоянно анализировать и совершенствовать защиту привилегированного доступа для соответствия меняющемуся ландшафту угроз.

[1] Стефани Балура (Stephanie Balouras) и др.: «Уроки, извлеченные из крупнейших утечек данных и нарушений конфиденциальности 2016 года», Forrester Research, Inc., 9 января 2017 г. | Обновлено: 15 февраля 2017 г., стр 2.

[2] http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/#report

Обзор программы CyberArk Privileged Access Security Cyber Hygiene

Компания CyberArk разработала программный подход, помогающий организациям обеспечитьзащиту за счет внедрения и поддержания строгого контроля и защиты привилегированного доступа. Программа CyberArk Privileged Access Security Hygiene использует богатый опыт специалистов службы CyberArk Security Services по реагированию на серьёзные утечки данных, в том числе во многих крупных организациях. Часто эти утечки происходят в результате некоторых наиболее распространенных атак на привилегированные аккаунты, и каждый пример предоставляет ценную информацию о том, как действуют злоумышленники и как они используют уязвимости организации.

Совместный, целенаправленный подход к решению этих проблем при помощи взаимодействия со специалистами Security Services помогает организациям устанавливать необходимый контроль над защитой привилегированного доступа и усиления комплексных мер безопасности. Эффективное внедрение подобной программы позволяет добиваться значительного снижения рисков в сжатые сроки и достигать целей в области безопасности и регулирования при меньшем объеме внутренних ресурсов.

Программа безопасности помогает организациям планировать и выполнять задачи по обеспечению наивысшего уровня защиты от наиболее распространенных атак на привилегированные аккаунты, учётные данные и конфиденциальную информацию. [Рис. 1]

Рис. 1. Основная цель программы CyberArk Privileged Access Security Cyber Hygiene — удовлетворение важнейших потребностей и устранение потенциальных уязвимостей в организациях при наиболее широком охвате ключевых возможностей привилегированного доступа. Например, связанных с критически важной инфраструктурой и приложениями, данными заказчиков и наиболее ценными активами компании — как локально, так и в облаке.

Обеспечение максимальной защиты привилегированного доступа

Для достижения максимального уровня защиты специалисты службы CyberArk Security Services тесно сотрудничают с организациями, помогая:

- Совместно анализировать риски, связанные с текущей программой обеспечения безопасности привилегированного доступа, включая выявление её слабых мест и анализ мышления и тактику злоумышленников.
- Определять надлежащий уровень необходимой защиты и устанавливать соответствующие приоритеты.
- Вырабатывать оптимальный подход и план внедрения для достижения надлежащего уровня защиты.

В каждой организации существует свой уникальный подход для обеспечения безопасности привилегированного доступа. В следующих разделах представлены действия службы CyberArk Security Services в отношении наиболее распространенных атак с привилегированным доступом. Некоторым организациям требуется уделить внимание каждому направлению, однако чаще всего, по крайней мере, на первоначальном этапе, это делается только для наиболее важных областей. Данный подход применяется независимо от того, где развернуты приложения и инфраструктура: локально, в облаке (IaaS, PaaS и SaaS) или в гибридных средах.

Защита от необратимых атак по захвату сети

Замысел злоумышленников

С помощью сложной для выявления атаки глубоко проникнуть и закрепиться в организации, что потребует полностью перестроить бизнес для нейтрализации злоумышленника. Примером может служить атака на протокол Kerberos, такая как Golden Ticket.

Golden Ticket — это не просто фальшивый билет Kerberos, а целый центр по распределению поддельных ключей, позволяющий атакующим на протяжении многих лет совершать любые действия в рамках возможностей аутентификации Kerberos.

→

В вашей текущей программе по обеспечению безопасности привилегированного доступа:

- Вы полагаетесь на однофакторную аутентификацию для администраторов домена?
- Имеются ли на ряде машин уровня tier1 и tier2 хеш-функции, обеспечивающие привилегированный доступ к системам уровня tier0?

Оптимальная защита от этого типа атаки предполагает:

- Изоляцию всех возможностей привилегированного доступа к уровню 0 и 1 с необходимостью многофакторной аутентификации;
- Изначальное отсутствие остаточных хеш-функций;
- Выявление и блокировку атак Kerberos на контроллер домена в процессе их осуществления;
- Невозможность создания инфраструктурных аккаунтов на уровне 0.

→

Подход к обеспечению оптимальной защиты:

- Разрешение доступа к решению CyberArk Core Privileged Access Security только с многофакторной аутентификацией;
- Защита контроллеров домена и других ресурсов уровня 0 и 1 с помощью решений CyberArk Core Privileged Access Security с модулем Domain Controller Protection (опция) и CyberArk Endpoint Privilege Manager.

Контроль и защита инфраструктурных аккаунтов

Замысел злоумышленников

Использование полнофункциональных стандартных инфраструктурных аккаунтов в локальных или облачных средах, которые редко используются в повседневной работе, но предоставляют киберпреступникам отличные возможности для получения доступа. Например, они могут взять под свой контроль весь технологический комплекс, скомпрометировав один инфраструктурный аккаунт с помощью заданного по умолчанию и не измененного пароля. Одни и те же учётные данные могут быть использованы для доступа к похожим ресурсам.

→

В вашей текущей программе по обеспечению безопасности привилегированного доступа:

- Сколько локальных администраторов имеется на:
  - Серверах Windows?
  - Серверах *NIX?
  - Серверах Cisco?
  - Серверах SQL?
- Как обстоят дела с учётными записями SYS и SYSTEM на серверах Oracle?
- Как защищены ваши инфраструктурные аккаунты облачных сред?

Оптимальная защита от этого типа атаки предполагает:

- Переход на полный контроль всех аккаунтов

→

Подход к обеспечению оптимальной защиты:

- Безопасное хранение всех известных инфраструктурных аккаунтов с использованием решения CyberArk Core Privileged Access Security;
  — Автоматическое изменение паролей — периодически и после каждого использования.

Блокировка злоумышленников в конечных точках

Замысел злоумышленников

Кража учётных данных посредством горизонтального перемещения по инфраструктуре, например использование методов Pass-the-Hash для получения расширенных прав.

→

В вашей текущей программе по обеспечению безопасности привилегированного доступа:

- Сколько рабочих станций Windows содержат права локального администратора для пользователей конечных точек?

Оптимальная защита от этого типа атаки предполагает:

- Полное удаление всех пользователей конечных точек из группы локальных администраторов на рабочих станциях Windows.

→

Подход к обеспечению оптимальной защиты:

- Использование CyberArk Endpoint Privilege Manager для удаления прав локального администратора на рабочих станциях Windows с целью предотвращения кражи учётных данных.

Защита привилегированных аккаунтов приложений сторонних производителей

Замысел злоумышленников

Компрометация приложений сторонних производителей, используемых для выполнения таких операций, как глубокое сканирование, с целью хищения встроенных привилегированных учётных данных. Дальнейшее проведение атак с полным обходом средств защиты компании.

→

В вашей текущей программе по обеспечению безопасности привилегированного доступа:

- Для какого количества установленных приложений и решений по обеспечению безопасности требуются наиболее привилегированные аккаунты с широким доступом к среде?
- Сколько из этих привилегированных аккаунтов хранится под защитой?
  - Механизмы сканирования уязвимостей?
  - Агенты управления инвентаризацией и серверы приложений?
  - Пароли баз данных WebLogic/WebSphere/Tomcat/JBoss?

Оптимальная защита от этого типа атаки предполагает:

- Безопасное хранение всех привилегированных аккаунтов, используемых приложениями сторонних производителей.

→

Подход к обеспечению оптимальной защиты:

- применение решения CyberArk Core Privileged Access Security с настройкой автоматического изменения паролей после каждой операции;
- использование CyberArk Application Identity Manager с целью исключения возможности применения встроенных учётных данных в готовых коммерческих приложениях.

Безопасность SSH-ключей на критически важных серверах *NIX

Замысел злоумышленников

Использование неуправляемых SSH-ключей для входа в систему с правами суперпользователя и получения контроля над комплексом технологий *NIX. Системы Unix/Linux служат для размещения некоторых наиболее конфиденциальных активов предприятия. Отдельные аккаунты и учётные данные, в том числе ключи SSH, используемые для получения привилегий суперпользователя, часто упускаются из виду специалистами по ИТ-безопасности.

→

В вашей текущей программе по обеспечению безопасности привилегированного доступа:

- Сколько неуправляемых SSH-ключей имеется на рабочих серверах Unix и Linux?

Оптимальная защита от этого типа атаки предполагает:

- Безопасное хранение и регулярную ротацию всех пар SSH-ключей на рабочих серверах Unix и Linux.

→

Подход к обеспечению оптимальной защиты:

- Безопасное хранение и ротация SSH-ключей на рабочих серверах Unix и Linux и их защита политиками с использованием решения CyberArk Core Privileged Access Security.

Защита секретов DevOps в облачных и локальных средах

Замысел злоумышленников

Компрометация наиболее привилегированных ключей API, встроенных в код и инструменты непрерывной интеграции/разработки, с целью использования среды и получения более широкого доступа.

→

В вашей текущей программе по обеспечению безопасности привилегированного доступа:

- Конфиденциальная информация и учётные данные, используемые Ansible, Jenkins, Docker и другими инструментами DevOps, встроены в открытом или жестко закодированном формате?
- Вы используете много инструментов DevOps, которые не имеют централизованной возможности для хранения и согласованного управления секретами? Вы можете контролировать, какие приложения и инструменты используют конкретные секреты?
- Для какого количества аккаунтов с правами суперпользователя общедоступных/частных облачных сред не реализованы надежное хранение и ротация? (Например, доступ с правами суперпользователя AWS и стандартные API-ключи).

Оптимальная защита от этого типа атаки предполагает:

- Безопасное хранение и регулярную автоматическую ротацию привилегированных аккаунтов общедоступных облачных сред, ключей и API-ключей;
- Безопасное хранение, оперативное получение, автоматическую ротацию и управление учётными данными и конфиденциальной информацией, которые используются инструментами непрерывной интеграции/разработки, такими как Ansible, Jenkins и Docker.

→

Подход к обеспечению оптимальной защиты:

- Использование решения CyberArk Core Privileged Access Security для безопасного хранения и регулярной автоматической ротации аккаунтов с правами суперпользователя, ключей и API-ключей;
- Применение CyberArk Conjur для защиты, хранения и оперативного доступа к секретам, используемым идентификаторами машин, в средах DevOps и других динамичных инфраструктурах (таких как встроенные учётные данные в инструментах непрерывной интеграции/разработки);
- Использование CyberArk Application Identity Manager для хранения и оперативного получения учётных данных и секретов в более статичных средах приложений (обычно развернутых локально).

Безопасная работа администраторов решений SaaS и привилегированных бизнес-пользователей

Замысел злоумышленников

Хищение учётных данных, используемых администраторами SaaS и привилегированными бизнес-пользователями, для получения высокоуровневого скрытого доступа к информационно важным системам.

→

В вашей текущей программе по обеспечению безопасности привилегированного доступа:

- Сколько учётных записей с высокой привилегией для приложения Workday и веб-сайтов кредитных организаций совместно используется специалистами финансового отдела?
- Сколько учётных записей с высокой привилегией для системы BambooHR совместно используется сотрудниками отдела кадров?
- Каким образом вы обеспечиваете безопасность работы администраторов решений SaaS, которые имеют доступ к конфиденциальным приложениям, связанным с социальными сетями, продажами, финансовой деятельностью и т. д.?

Примечание: поскольку эти учётные записи часто подразумевают совместное использование, для них не применяется многофакторная аутентификация.

Оптимальная защита от этого типа атаки предполагает:

- Изоляцию доступа к коллективным учётным записям и обязательное введение многофакторной аутентификации.

→

Подход к обеспечению оптимальной защиты:

- Разрешение доступа к решению CyberArk Core Privileged Access Security только с многофакторной аутентификацией;
- Защита всех коллективных учётных записей и доступа администратора SaaS к конфиденциальным приложениям с использованием решения CyberArk Core Privileged Access Security, включая защищённые от взлома журналы аудита, а также усиление контроля и регистрации, плюс, изоляция сеансов.

Следующие шаги

Поддержание оптимального уровня безопасности привилегированного доступа требует сохранять бдительность. CyberArk предлагает несколько решений и возможностей, которые помогут организациям и дальше развивать свою программу по обеспечению безопасности привилегированного доступа и повышать общий уровень защиты. К ним относятся:

- Оценка прогресса: CyberArk Discovery and Audit (DNA) — это эффективный инструмент для регулярного сканирования инфраструктуры организации с целью выявления потенциального скрытого и незащищенного привилегированного доступа, в том числе в облаке и средах DevOps;
- Проверка и повышение эффективности защиты от реальных атак: для оценки эффективности средств контроля Служба внешнего тестирования CyberArk Red Team моделирует атаки до и после развертывания;
- Расширение знаний, опыта и осведомленности в организации. Например:
  - Служба обучения и сертификации CyberArk Certification Services помогает организациям обучать собственных специалистов с использованием сертифицированных возможностей и опыта CyberArk;
  - Служба информационной безопасности CyberArk Security Services помогает организациям ускорять реализацию программы и передачу знаний.

Благодаря программе CyberArk Privileged Access Security Hygiene организации могут применять структурированный подход к улучшению общей гигиены привилегированного доступа. Взаимодействуя со службой CyberArk Security Services, организации могут более оперативно реализовывать эту важнейшую составляющую общей корпоративной стратегии и комплекса мер безопасности. Программа помогает организациям существенно снижать риски за меньшее время и достигать цели в области безопасности и регулирования без повышения нагрузки на внутренние ресурсы.

Чтобы получить дополнительную информацию о защите привилегированного доступа с помощью CyberArk Security Services, посетите веб-сайт www.cyberark.com/services-support/professional-services/.