ОЦЕНКА РИСКОВ КИБЕРБЕЗОПАСНОСТИ ДАННЫХ

ПРИМЕР ОТЧЕТА

Откуда исходят наибольшие угрозы безопасности данных в вашей компании?

Varonis поможет узнать это.

Оценка рисков кибербезопасности данных — это подробный и объективный отчет на основе анализа данных вашей компании, демонстрирующий уязвимости, которыми могут воспользоваться хакеры.

Опираясь на данные этого отчета, вы без труда составите пошаговый план устранения уязвимостей и расставите приоритеты, определите дальнейшие действия для приведения организации в соответствие с требованиями и политиками безопасности.

VARONIS

ЧТО ВХОДИТ В ОЦЕНКУ РИСКОВ КИБЕРБЕЗОПАСНОСТИ ДАННЫХ

Вот перечень хранилищ данных, анализируемых в рамках данного отчета, включая данные, папки, файлы, права доступа, а также учетные записи пользователей и групп. Выделенные области риска включают незащищенные конфиденциальные данные, проблемы контроля доступа и многое другое.

КОНТРОЛИРУЕМЫЕ ИСТОЧНИКИ ДАННЫХ

- CIFS_FS_1
- CIFS_FS_2
- CIFS_FS_3
- CIFS_FS_4
- CIFS_FS_5
- NS_FS_1
- EXCH_1
- SP_1

ОБЪЕМЫ

- 331 237 ГБ данных
- 90 348 156 папок
- 1 617 176 767 файлов
- 701 387 576 разрешений

ACTIVE DIRECTORY

- 8580 учетных записей пользователей
- 14 427 групп
- 9268 учетных записей компьютеров
- 420 отключенных пользователей

Выборка данных анализируется на предмет рисков в следующих областях:

- незащищенные конфиденциальные данные «в зоне риска»
- подверженные риску данные Office 365 и Microsoft Teams
- риски, связанные с Active Directory
- мониторинг привилегированных учетных записей и конечных пользователей
- разрешения файловой системы NTFS и структура общедоступных ссылок в Office 365
- обнаружение угроз и возможности реагирования
- конфиденциальность данных и соблюдение требований регуляторов и политик безопасности

Срабатывания моделей угроз

85
оповещений

2 инцидента ежедневно,
требующих расследования

Риск вторжения и эксфильтрации

315
подозрительных событий

Подозрительные события,
выявленные на границе среды

Риски Active Directory

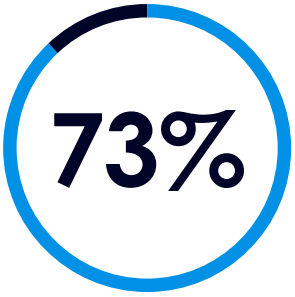
17
уязвимостей

Различные уязвимости, обнаруженные в **Active Directory**

Обнаруженных конфиденциальных данных

Файлы, содержащие
конфиденциальные данные (950 534 645 файлов)

Незащищенные конфиденциальные данные



Конфиденциальных записей, **доступных для каждого сотрудника** (1 212 568 008 записей)

Риски Office 365

8125
конфиденциальных записей

Конфиденциальные записи, доступные всем через **общедоступные ссылки Office 365**

ГЛОБАЛЬНЫЕ ГРУППЫ ДОСТУПА

Глобальные группы позволяют каждому сотруднику организации получить доступ к этим папкам. К глобальным группам доступа относятся такие группы, как Everyone («Все»), Domain Users («Пользователи домена») и Authenticated Users («Авторизованные пользователи»).

Общедоступные данные — распространенная уязвимость системы безопасности. По оценкам специалистов в области информационной безопасности, на поиск и удаление групп глобального доступа вручную, без средств автоматизации, уходит порядка 6–8 часов для каждой папки. Специалистам нужно определить пользователей, которым действительно необходим доступ, а затем создать и применить новые группы, и только потом добавить туда нужных пользователей.

СВОДКА ПО РИСКАМ:

Низкий Средний Высокий

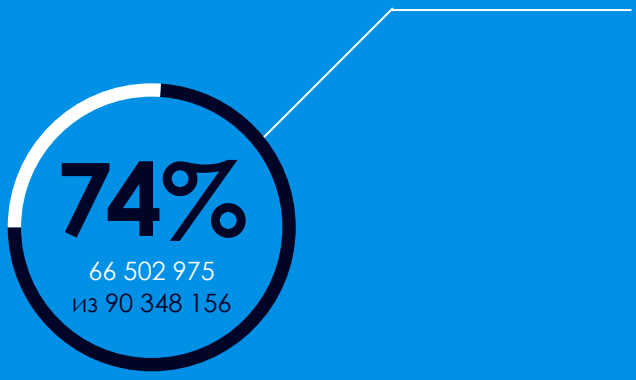
- Чрезмерный доступ — одна из основных причин утечек данных.
- Конфиденциальные данные с избыточным доступом представляют серьезную угрозу безопасности.
- Устаревшие права пользователей часто используются злоумышленниками для достижения своих целей.

РЕКОМЕНДУЕМЫЕ ДЕЙСТВИЯ:

- Удалить глобальные права доступа.
- Добавить активных пользователей в новую группу.
- Заменить глобальную группу доступа новой группой из списка контроля доступа.

66,5 МИЛЛИОНОВ

папок с глобальными правами доступа



РАСПРЕДЕЛЕНИЕ ГЛОБАЛЬНЫХ ГРУПП ДОСТУПА

- CIFS_FS_2 11%
- CIFS_FS_3 7%
- CIFS_FS_4 20%
- SP_FS_1 44%
- EXCH_FS_1 18%

ДОСТУП ГЛОБАЛЬНЫХ ГРУПП К КОНФИДЕНЦИАЛЬНЫМ ФАЙЛАМ

- CIFS_FS_2 2%
- CIFS_FS_3 1%
- CIFS_FS_4 2%
- SP_FS_1 82%
- EXCH_FS_1 13%

КОНФИДЕНЦИАЛЬНЫЕ ДАННЫЕ

Многие файлы содержат критически важную информацию о сотрудниках, клиентах или проектах, а также другие сведения, важные для бизнеса. Эти данные нередко регулируются международными, национальными или отраслевыми стандартами, такими как HIPAA, PCI, GDPR и т.д.

Конфиденциальные данные, открытые для глобальных групп, представляют для бизнеса значительный риск. Их следует выявлять и исправлять так, чтобы к ним имели доступ только те пользователи, кому это необходимо для выполнения рабочих обязанностей.

СВОДКА ПО РИСКАМ:

Низкий Средний Высокий

- Конфиденциальные данные часто содержат востребованную злоумышленниками и инсайдерами информацию: персональные данные, информацию о банковских картах, IP-адреса, электронную почту и многое другое.
- Чрезмерный доступ — одна из основных причин утечек данных.
- Конфиденциальные данные с избыточным доступом представляют серьезную угрозу безопасности.

РЕКОМЕНДУЕМЫЕ ДЕЙСТВИЯ:

- Сканировать, классифицировать и организовать мониторинг конфиденциальной информации (где она находится, кто имеет к ней доступ и кто пользуется этим доступом).
- Внедрить и поддерживать модель наименьших привилегий.
- Поддерживать политику информационной безопасности, ориентированную на данные, чтобы обеспечить соответствие нормативным требованиям в отношении конфиденциальной информации.

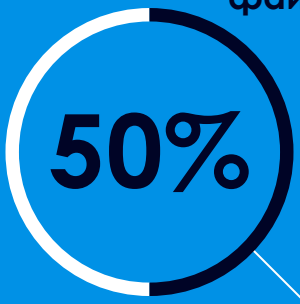
Основные результаты

Более 950 миллионов

файлов с конфиденциальными данными (950 534 645)

Более 339 миллионов

конфиденциальных файлов, с глобальным доступом (339 213 456)



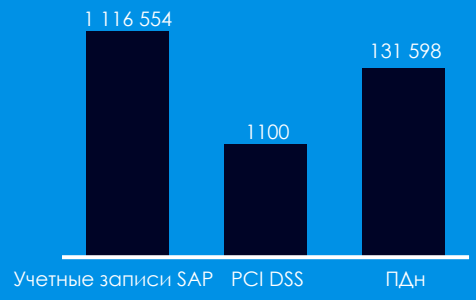
Свыше 50% конфиденциальной информации находится на одном файловом сервере: SP_FS_1

РАСПРЕДЕЛЕНИЕ КОНФИДЕНЦИАЛЬНЫХ ФАЙЛОВ

- CIFS_FS_2 13%
- CIFS_FS_3 12%
- CIFS_FS_4 8%
- SP_FS_1 54%
- EXCH_FS_1 13%

ОБЩЕЕ КОЛИЧЕСТВО ОБНАРУЖЕНИЙ ПО ТИПУ ДАННЫХ

- SAP Acc# 1 116 554
- PCI DSS 1100
- ПДн 131 598



РИСКИ OFFICE 365

SharePoint Online, OneDrive и Microsoft Teams позволяют обмениваться данными за пределами организации одним нажатием кнопки. Со временем Office 365 превращается в хаос общедоступных ссылок и неограниченного доступа к конфиденциальным данным, а пользователи сталкиваются с необходимостью оспаривать каждое разрешение.

Внешние ссылки предоставляют доступ определенным пользователям, находящимся за пределами вашей сети.

Общедоступные ссылки открыты для всех, то есть доступны кому угодно.

СВОДКА ПО РИСКАМ:

Низкий Средний Высокий

- Раскрытие конфиденциальных данных через гостевой доступ и общедоступные ссылки несет серьезную угрозу безопасности.
- Совместная работа в Microsoft Teams хаотична и должна сочетаться с комплексным мониторингом прав доступа и аналитикой поведения пользователей для выявления подозрительной активности в Office 365.
- Для предотвращения атак методом перебора паролей (брутфорс) и подстановки учетных данных у всех сотрудников должна быть включена многофакторная аутентификация.

РЕКОМЕНДУЕМЫЕ ДЕЙСТВИЯ:

- Классификация и защита конфиденциальных и регулируемых данных в SharePoint, OneDrive и Microsoft Teams.
- Автоматическое перемещение в карантин критичных для бизнеса данных, хранимых на личных сайтах OneDrive.
- Настройка и применение политик распространения внешних ссылок и автономного доступа, чтобы защитить данные от эксфильтрации и несанкционированного доступа.
- Отслеживать аномалии поведения пользователей в Office 365 и Azure Active Directory.

Основные результаты

1 239 241

конфиденциальных записей обнаружено в Office 365 (29 235 файлов)

8125

конфиденциальных записей, доступных всем через общедоступные ссылки (1824 файла)

2512

конфиденциальных записей, доступ к которым открыт внешним пользователям в 895 файлах

310
общих ссылок использовалось
за последние 30 дней

551
папка с общим доступом

8
оповещений, связанных с Office 365, за последние 30 дней

УСТАРЕВШИЕ ДАННЫЕ

Устаревшими считаются данные, которые хранятся сверх установленного срока, или же которыми не пользовались определенное время. Такие данные дорого хранить, ими сложно управлять, их наличие в целом ведет к ненужному повышению рисков безопасности.

СВОДКА ПО РИСКАМ:

Низкий | Средний | Высокий

- Устаревшие данные приводят к ненужным расходам на хранение.
- Устаревшие данные представляют ненужную угрозу безопасности, оставляя возможности их для разглашения или кражи.

РЕКОМЕНДУЕМЫЕ ДЕЙСТВИЯ:

- Найти устаревшие данные и определить, какие из них можно переместить, архивировать или удалить.
- Создать и обеспечить выполнение политики управления устаревшими данными.

253 168 ГБ

устаревших данных

Более 85 миллионов

(85 377 723)

папок с устаревшими данными

Более 75% проверенных данных устарело.

ОБЪЕМ УСТАРЕВШИХ ДАННЫХ

- CIFS_FS_2 25%
- CIFS_FS_3 22%
- CIFS_FS_4 8%
- SP_FS_1 29%
- EXCH_FS_1 16%

УСТАРЕВШИЕ ДАННЫЕ С КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ

- CIFS_FS_2 14%
- CIFS_FS_3 11%
- CIFS_FS_4 9%
- SP_FS_1 53%
- EXCH_FS_1 13%

УЧЕТНЫЕ ЗАПИСИ ПОЛЬЗОВАТЕЛЕЙ

- **15** учетных записей администратора с SPN
- **2** учетные записи с идентификатором безопасности (SID) из текущего домена
- **4** учетные записи с правами делегирования Kerberos

ПОЛЬЗОВАТЕЛИ И УЧЕТНЫЕ ЗАПИСИ КОМПЬЮТЕРОВ

- **40** учетных записей пользователей не требуют пароля
- **8** учетных записей компьютеров, которые также являются учетными записями администраторов
- **12** учетных записей компьютеров имеют слабое шифрование для Kerberos

40

учетных записей пользователей не требуют пароля

УЧЕТНЫЕ ЗАПИСИ И ПОЛЬЗОВАТЕЛИ

Учетные записи администраторов с SPN

Злоумышленники могут запрашивать тикеты (шифрованный сеансовый ключ) или учетные записи с уникальным идентификатором конкретной службы (SPN). Тикеты, зашифрованные с помощью RC4, чрезвычайно уязвимы для взлома паролей.

Учетные записи с записью истории SID из текущего домена

Злоумышленники используют их для закрепления в системе или сети жертвы, повышая привилегии обычного пользователя до привилегированного.

Учетные записи с правами делегирования Kerberos (неограниченное делегирование)

Злоумышленники могут взломать учетную запись, обладающую правами делегирования Kerberos, и использовать ее для выдачи себя за другие учетные записи пользователей.

СВОДКА ПО РИСКАМ:

Низкий | Средний | Высокий

- Учетные записи с уникальным идентификатором конкретной службы (SPN) должны иметь длинные сложные пароли и часто их менять. Шифрование RC4 можно отключить, если оно не требуется.
- Учетные записи не должны иметь атрибута SID History из одного и того же домена.
- Делегирование Kerberos должно использоваться только уполномоченными учетными записями служб, которым требуется возможность работы от имени других учетных записей, с использованием их привилегий.

РЕКОМЕНДУЕМЫЕ ДЕЙСТВИЯ:

- Проверяйте индикаторы пользователя, компьютера и домена.
- Выявляйте учетные записи пользователей без пароля.
- Отслеживайте события Active Directory на наличие признаков эксплуатации уязвимостей.

ПАПКИ

- **277 027** папок с конфликтами SID
- **58 419** папок с несоответствиями разрешений
- **1 040 040** папок с уникальными разрешениями

ПРАВА ДОСТУПА

- **423 872** папки с прямыми записями управления доступом (ACE) пользователей
- **25 551** защищенная папка
- **90 348 156** папок, для которых не назначены владельцы данных

277 027

несоответствующих сидов (SID)

ПАПКИ И ПРАВА ДОСТУПА

Несоответствующие сиды (SID)

Конфликты с идентификаторами безопасности (SID) возникают, когда учетная запись из списка управления доступом удаляется из Active Directory. Конфликты SID усложняют обеспечение безопасности и могут использоваться злоумышленниками.

Несоответствия разрешений

Несоответствия разрешений возникают, когда папки или файлы наследуют дополнительные записи управления доступом (ACE) от своих родительских папок, но при этом не наследуют основные ACE. Пользователи могут непреднамеренно получить доступ или лишиться его.

СВОДКА ПО РИСКАМ:

Низкий | Средний | Высокий

- Ошибки в наследовании прав доступа подвергают данные риску, открывая к ним доступ лицам, которые его иметь не должны, или блокируя доступ тем, кто с этими данными действительно работает.
- Конфликты SID и несоответствие разрешений подвергают корпоративные данные ненужному риску.
- Папки с несоответствиями разрешений потенциально подвергают данные повышенному риску со стороны инсайдеров, хакеров и других злоумышленников.

РЕКОМЕНДУЕМЫЕ ДЕЙСТВИЯ:

- Пересмотреть структуру разрешений, чтобы определить, требуются ли каким-то папкам уникальные права доступа. Если нет, разрешить папке повторное наследование родительских разрешений, заменив уникальные записи управления доступом.
- Определить папки с конфликтами идентификаторов безопасности (SID) и удалить их из списков управления доступом.
- Определить папки с прямыми разрешениями пользователей, поместить пользователей в соответствующие группы и удалить записи управления доступом пользователей из списков управления доступом.

ЧАСТО СРАБАТЫВАЮЩИЕ МОДЕЛИ УГРОЗ

- Нестандартное поведение службы — доступ к нетипичным файлам, содержащим персональные данные, данные GDPR
- Необычная загрузка файлов
- Атака методом распыления паролей

ВАЖНЫЕ СОЕДИНЕНИЯ

- 18 VPN-соединений от неактивных пользователей
- 8 соединений с теневыми ИТ-ресурсами (Shadow IT)
- 10 попыток перехода на вредоносные сайты

АКТИВНОСТЬ ПОЛЬЗОВАТЕЛЕЙ

- **423 110** файлов открыто
- **182 335** файлов изменено
- **65 120**файлов удалено
- **22 965** изменений в правах доступа

более 750 000

событий с конфиденциальными данными

АКТИВНОСТЬ ПОЛЬЗОВАТЕЛЕЙ И УСТРОЙСТВ

Активность и поведение пользователей

К активности пользователей и устройств относят действия в облачной и локальной файловой системах, электронной почте и SharePoint, телеметрию периметра и Active Directory, а также результаты анализа угроз.

Varonis отслеживает и анализирует поведение пользователей и объектов в облачных и локальных хранилищах данных, Active Directory, компонентах периметра сети, чтобы получить представление о потенциальной подозрительной активности.

Varonis обнаруживает внутренние угрозы, программы-вымогатели, отклонения в поведении пользователей и оповещает о них.

СВОДКА ПО РИСКАМ:

Низкий Средний Высокий

- Несанкционированные попытки получить доступ к данным или изменить их часто свидетельствуют о внутренних угрозах, кибератаках или деятельности вредоносных программ.
- Необычное поведение пользователя или устройства может указывать на потенциальный захват учетной записи или утечку данных.
- Соединения от неактивных пользователей или подключения к вредоносным IP-адресам часто свидетельствуют об активной кибератаке: злоумышленники пытаются получить доступ к учетной записи или системе, либо украсть данные.

РЕКОМЕНДУЕМЫЕ ДЕЙСТВИЯ:

- Отслеживать поведение пользователей и файловую активность.
- Отслеживать подозрительные VPN и DNS-соединения и блокировать попытки проникновения со стороны известных вредоносных соединений.
- Настроить обнаружение и оповещение при нарушениях безопасности, подозрительном поведении и необычной активности.
- Внедрить план реагирования на инциденты и процессы расследования для выявления потенциальных нарушений кибербезопасности.

ОСНОВНЫЕ НАПРАВЛЕНИЯ ОЦЕНКИ РИСКОВ

- Глобальный доступ, устаревшие данные и несогласованные права доступа
- Уязвимые конфиденциальные данные, относящиеся, например, к персональным данным, коммерческой тайне, PCI и GDPR
- Несоответствующие требованиям процессы предоставления прав доступа и авторизации

ПРЕИМУЩЕСТВА

- **Стопроцентная** адаптация под ваши потребности
- **Выделенный инженер Varonis** проведет оценку вашей инфраструктуры
- Минимальная нагрузка на инфраструктуру

нулевое влияние на бизнес-процессы

менее 90 минут вашего времени

ОСНОВНЫЕ РЕЗУЛЬТАТЫ

Глобальные группы доступа

Конфиденциальные данные

Устаревшие данные

Учетные записи и пользователи

Папки и разрешения

Активность пользователей

СВОДКА ПО РИСКАМ:

Низкий | Средний | Высокий

- Сводка по рискам для каждого обнаруженного случая
- Оценка возможностей по снижению рисков
- Конкретные шаги по сокращению рисков

ОХВАТ:

- Windows
- SharePoint
- Exchange
- Office 365
- Azure Active Directory
- Unix/Linux
- Active Directory
- Dell EMC
- NetApp
- HPE
- Nasuni

РЕКОМЕНДАЦИИ:

- Дальнейшие практические шаги для каждой области риска
- Проверенная методология защиты данных

О КОМПАНИИ VARONIS

Varonis — разработчик решений по кибербезопасности, основанных на поведенческом анализе пользователей и защите корпоративных данных от внутренних угроз и кибератак. Непрерывный мониторинг и оповещения о состоянии систем и использовании данных позволяют нашим заказчикам быть уверенными в том, что их данные надежно защищены. Varonis сочетает в себе средства классификации и управления доступом, а также инструменты анализа поведения пользователей и сущностей, благодаря чему в модели угроз закладывается более широкий контекст данных, а оповещения отличаются высокой точностью.

ИНТЕРАКТИВНАЯ ДЕМОНСТРАЦИЯ

Настройте Varonis в своей инфраструктуре. Быстро и без лишних хлопот.

info.varonis.com/demo/ru

ОЦЕНКА РИСКОВ КИБЕР-БЕЗОПАСНОСТИ ДАННЫХ

Поможет устранить проблемы безопасности данных и снизить риск их утечки.

https://info.varonis.com/risk-assessment/ru

СВЯЗАТЬСЯ С НАМИ

Остались вопросы? Свяжитесь с нами!
+7 495 997 6366

sales-russia@varonis.com

NASA ING Nasdaq CHAMPAGNE BOLLINGER MAISON FONDÉE EN 1829 DELL EMC

TOYOTA LUXEMBOURG INSTITUTE OF HEALTH RESEARCH DEDICATED TO LIFE L'ORÉAL

VARONIS