VARONIS

ОТЧЕТ О РИСКАХ ДАННЫХ, 2021 ГОД

ПРОМЫШЛЕННОСТЬ

Каждому сотруднику доступно более **6 миллионов** файлов, что подвергает данные риску со стороны программ-вымогателей и внутренних угроз.

СОДЕРЖАНИЕ

VARONIS

ОБ ОТЧЕТЕ

Отчет о рисках данных производственных предприятий за 2021 год — это третий отчет в нашей ежегодной серии, в котором анализируются отраслевые угрозы, тенденции и решения.

Этот отчет посвящен проблеме растущих угроз кибербезопасности, с которыми сталкиваются промышленные предприятия по всему миру. Мы сделали свои выводы, проанализировав 4 миллиарда файлов в 50 организациях.

Многие выводы в отчете представлены по размеру бизнеса:

1. **малый:** 0–500 сотрудников;
2. **средний:** 501–1500 сотрудников;
3. **крупный:** свыше 1500 сотрудников.

Этот отчет призван помочь производственным предприятиям объективно оценить текущую ситуацию в области кибербезопасности и предоставить рекомендации по сокращению поверхности атаки.

В основе отчета — анализ
4 миллиардов файлов
50 производственных компаний

Промышленные предприятия

Конструкторские бюро

VARONIS

ОСНОВНЫЕ ВЫВОДЫ

Угрозы производственному сектору сохраняются: от серьезных групп разработчиков программ-вымогателей, которые крадут данные жертвы, прежде чем зашифровать их, до злоумышленников на государственном уровне, ищущих технологические секреты, а также инсайдеров внутри компании, выполняющих поиск информации, которую можно заполучить и продать тому, кто больше заплатит. В последнее время из сводок новостей не сходят заголовки о том, как атаки программ-вымогателей останавливают работу конвейерных линий сборки и нарушают цепочки поставок.

Чрезмерный доступ к информации, особенно конфиденциального характера, приводит к значительному увеличению риска. Эта уязвимость является вашим «радиусом поражения» — считайте, что это тот ущерб, который злоумышленник может нанести, проникнув в вашу среду. Если хоть один сотрудник нажмет на ссылку в фишинговом письме, злоумышленник потенциально может получить доступ ко всем файлам, к которым имеет доступ этот сотрудник. Когда инсайдер компании решает пойти на преступление, он может не спеша украсть ценную информацию и использовать ее в личных целях.

Мы стремились понять, в какой степени производственные предприятия защищают свои конфиденциальные данные от этих растущих угроз.

Мы обнаружили, что **у каждого сотрудника есть доступ в среднем к 6 млн файлов уже в первый день работы в компании.** [1] Мы также обнаружили, что в среднем более **27 000 конфиденциальных файлов** открыты всем сотрудникам компании.

[1]В этом отчете под словом «все» подразумевается каждый сотрудник организации.

VARONIS

Производственные данные под угрозой: основные выводы

В среднем каждый сотрудник имеет доступ к **6 миллионам файлов,** в том числе содержащих конфиденциальную информацию.

В среднем **более 27 000 конфиденциальных файлов** (с финансовыми данными, информацией, представляющей собой коммерческую, промышленную тайну, и бизнес-планами) открыты для всех.

В 4 из 10 организаций **каждый сотрудник**имеет доступ к более чем **1 000 конфиденциальных файлов.**

Более чем в половине компаний имеется **свыше 500 учетных записей с бессрочными паролями.**

ГЛОБАЛЬНЫЕ ВЫВОДЫ

Риски для крупных компаний — в 2 раза выше

Данные представлены в зависимости от размера компании

Размер организации	Средн. кол-во файлов	Средн. кол-во файлов, открытых всем	Средн. % файлов, открытых всем
Крупный	63 571 806	12 303 704	19%
Средний	21 920 382	3 776 187	17%
Малый	12 347 728	2 212 460	18%
В среднем по отрасли	**33 975 882**	**6 331 523**	**18%**

Размер организации	Средн. кол-во папок	Средн. кол-во папок, открытых всем	Средн. % папок, открытых всем
Крупный	6 173 686	1 152 954	19%
Средний	1 974 167	308 329	16%
Малый	1 244 511	218 620	18%
В среднем по отрасли	**3 241 479**	**575 766**	**18%**

Размер организации	Средн. кол-во конфиденц. файлов	Средн. кол-во конфиденц. файлов, открытых всем	Средн. % конфиденц. файлов, открытых всем
Крупный	310 014	39 122	13%
Средний	232 305	19 958	9%
Малый	166 051	23 684	14%
В среднем по отрасли	**244 150**	**27 293**	**10%**

В среднем каждый сотрудник имеет доступ к более чем 6 млн файлов (примерно 1/5 от общего количества файлов) уже в первый день работы. Для крупных предприятий это число удваивается: в компаниях численностью персонала от 1 500 чел. сотрудники могут получить доступ более чем к 12 млн файлов.

Каждый из десяти файлов, открытых для всех сотрудников компании, содержит конфиденциальную информацию. Это могут быть объекты интеллектуальной собственности, данные о сотрудниках, информация о производстве и цепочке поставок, документация по разработке продукции, маркетинговые планы и многое другое. По сравнению с компаниями сферы финансовых услуг в производственных предприятиях открытых файлов меньше: сотруднику компании финансового сектора может доступно 11 млн файлов.

ГЛОБАЛЬНЫЕ ВЫВОДЫ

Аналитика данных (в пересчете на терабайт) в сфере производства

Размер организации	Файлы	Папки	Открытые папки	Конфиден-циальные файлы	Папки с уни-кальными правами	Открытые конфиден-циальные файлы	Устаревшие конфиден-циальные файлы	Несоответ-ствующие сиды (SID)	Папки с несогла-сованными разрешениями	Кол-во отчетов	Терабайт проанализи-ровано на компанию
Крупный	1 654 486	112 973	11 772	11 558	9 460	1 739	8 506	561	375	17	86
Средний	1 073 643	103 425	26 529	21 781	8 112	2 102	12 551	1 079	250	22	19
Малый	1 291 091	134 830	18 143	5 236	15 322	721	4 217	482	689	11	13
Средний	**1 318 968**	**113 581**	**19 667**	**14 665**	**10 157**	**1 675**	**9 342**	**772**	**389**	**50**	**40**

Оценка риска на терабайт данных дает более четкое представление о типичной поверхности атаки в зависимости от размера компании и показывает, какие организации наиболее уязвимы к внутренним и внешним атакам. В среднем один терабайт данных содержит около 1,3 млн файлов.

Мы обнаружили, что **в среднем у промышленных предприятий на каждый терабайт приходится около 20 000 незащищенных папок (открытых для всех)**. Это число аналогично показателю сектора финансовых услуг и значительно ниже, чем в секторе здравоохранения (19 251 и 29 965, соответственно). ИТ-специалистам требуется примерно 6–8 часов для поиска и удаления общего доступа к каждой папке вручную, что означает, что на исправление настроек и обслуживание таких папок вручную уйдут годы.

У производственных предприятий более 1 675 открытых конфиденциальных файлов на терабайт данных. Это число немного ниже, чем в сфере здравоохранения (1 837), и примерно такое же, как в финансовом секторе (1 646).

Наш анализ показал, что производственные компании в среднем имеют **меньшее общее количество уязвимых файлов**, чем представители других отраслей, таких как финансы и здравоохранение. Однако в среднем они имеют **больше открытых конфиденциальных файлов на один терабайт**. Особенно уязвимы малые и средние компании, так как у них больше всего открытых конфиденциальных файлов на терабайт.

ГЛОБАЛЬНЫЕ ВЫВОДЫ

Защита данных производственных предприятий

Данные по компаниям, в которых конфиденциальные файлы открыты для всех сотрудников через глобальный доступ

Конфиденциальные файлы, открытые всем	% компаний
< 1000	56%
1 000–10 000	22%
> 10 000	22%

Устаревшие конфиденциальные данные в зависимости от размера компании

Размер	Средн. кол-во устаревших конфиденц. файлов	Средн. % устаревших конфиденц. файлов
Крупный	190 215	80%
Средний	131 978	74%
Малый	133 957	84%
В среднем по отрасли	**152 214**	**78%**

Глобальные группы доступа (например, Все, Пользователи домена, Авторизированные пользователи) полезны для внутренней совместной работы, но они также значительно упрощают проникновение в вашу среду киберпреступников. Если злоумышленник скомпрометирует учетную запись одного конечного пользователя, он сможет воспользоваться правами доступа, которые позволят ему копировать, обмениваться, удалять и изменять незащищенную конфиденциальную информацию.

В 44% производственных предприятий в среднем более 1 000 файлов доступно каждому сотруднику, а более чем в каждой пятой компании каждому сотруднику открыто 10 000 файлов. Для компаний с чрезмерным доступом к конфиденциальным данным ограничение такого доступа путем применения модели наименьших привилегий является критически важным элементом программы снижения рисков.

Количество устаревших конфиденциальных данных, которые хранят производственные предприятия, превышает средние показатели, что расширяет поверхность атак и излишне увеличивает затраты на хранение. В среднем **78% конфиденциальных файлов предприятий являются устаревшими и могут быть удалены или заархивированы.**

ПРИЗРАК ВНУТРИ СИСТЕМЫ

Уязвимости Active Directory

Компании с бессрочными паролями

Бессрочные пароли	% компаний
< 500	44%
500–1 500	32%
> 1500	24%

Компании с фантомными пользователями

Размер групп пользователей с устаревшими данными	% компаний
< 1000	56%
1 000–10 000	36%
> 10 000	8%

Неактивные учетные записи пользователей и служб, которые остаются подключенными еще долгое время после ухода сотрудников (они же «фантомные пользователи»), дают злоумышленникам достаточно времени для того, чтобы проникнуть в вашу среду с помощью перебора паролей и, оказавшись внутри, исследовать ваши хранилища данных. Оттуда они могут незаметно похитить данные и избежать обнаружения, прежде чем зашифровать их.

Неактивные, но подключенные привилегированные учетные записи администраторов с бессрочными паролями — один из лучших подарков, который вы можете сделать киберпреступникам. Зачастую такие уязвимости не замечают, их трудно обнаружить и устранить без надлежащей видимости в вашей среде.

56% компаний имеют более 500 учетных записей с бессрочными паролями, а в 44% компаний имеется свыше 1 000 активных учетных записей «фантомных пользователей».

СОСТОЯНИЕ ОТРАСЛИ

Производство было **пятой по популярности среди хакеров сферой в 2020 году,** а **средняя величина ущерба от утечки данных составляет 4,99 млн долларов. В среднем на локализацию взлома системы производственного предприятия требуется 220 дней —** один из самых продолжительных жизненных циклов угроз по всем сферам деятельности.

В сочетании с результатами нашего анализа можно сделать два основных вывода:

1. Промышленная отрасль сильно отстает от финансового сектора по уровню зрелости процессов обеспечения информационной безопасности. Почти половина всех компаний всё еще недостаточно подготовлена к современным кибератакам.
2. Готовность производственных предприятий к обеспечению кибербезопасности имеет большую вариативность по сравнению с регулируемыми отраслями, такими как здравоохранение и финансы. В то время как некоторые компании имеют развитые политики безопасности данных и процедуры реагирования на инциденты, другие предпринимают лишь незначительные шаги по снижению рисков.

Производственные компании могут добиться успеха, используя развернутые решения в полной мере, устраняя «слепые пятна» в безопасности данных путем повышения прозрачности и сокращая доступ к данным по принципу наименьших привилегий с помощью автоматизации. Уменьшение радиуса поражения поможет минимизировать ущерб, который злоумышленники могут нанести, когда (а не если) они попадут в вашу сеть.

[2] IBM Cost of a Data Breach Report 2020 (отчет об ущербе в связи с утечкой данных компании IBM за 2020 г.)

В среднем в 2020 году каждая утечка данных в производственном секторе обходилась в **4,99 млн долл.**[2]

ПРИМЕР ИЗ ПРАКТИКИ

Как Varonis Edge помогает американскому производителю повысить безопасность локальных и облачных данных

Когда неавторизованный пользователь открыл папку с кадровыми данными, содержащую информацию о зарплате сотрудников, Varonis помог найти данного пользователя и выяснять, какие файлы он открыл и изменил.

Прочтите полную статью, чтобы узнать, как всё получилось.

ЧИТАТЬ ИСТОРИЮ УСПЕХА

VARONIS

О КОМПАНИИ VARONIS

Varonis — передовая компания в области кибербезопасности и аналитики данных, специализирующаяся на программном обеспечении для защиты данных, обнаружения угроз и реагирования на них, а также соблюдения нормативных требований. Varonis защищает данные компаний, анализируя информацию о телеметрии периметра сети, а также поведение пользователей и действия с данными. Решения компании предотвращают потери, блокируя доступ к конфиденциальной информации, и эффективно поддерживают защищенное состояние с помощью автоматизации.

Varonis — это лучшее в своем роде решение мирового уровня. Благодаря Varonis мы можем делать всё — от управления разрешениями общего доступа до поиска конфиденциальных данных и обеспечения безопасности локальной и облачной среды. В конечном итоге использование единой панели экономит время.

ДИРЕКТОР ПО ИНФРАСТРУКТУРЕ
Производственное предприятие

Хотите проверить, как обстоят дела в **вашей организации**?

Мы проведем бесплатную оценку рисков кибербезопасности и подготовим подробный отчет об уровне защищенности и скрытых рисках, которым подвергаются конфиденциальные данные вашей компании.

ЗАКАЗАТЬ АУДИТ РИСКОВ