Какие организации чаще других подвержены внутренним нарушениям корпоративной безопасности и служебной дисциплины?

2018–2020

rt-solar.ru
solar@rt-solar.ru

Ростелеком Солар

Содержание

Ключевые цифры и факты

1

Самая частая «жертва» нарушителей — производственная/научно-производственная организация со штатом свыше 1000 человек, в которой происходит в среднем 1900 нарушений за 3 месяца, 7 из которых признаются ИБ-службой высококритичными.

2

Лидер по числу критичных нарушений — организация сферы управленческого консалтинга и рекрутмента: 196 критичных нарушений за 3 месяца (каждое 80-е сообщение в корпоративном трафике).

3

Топ-5 отраслей с наибольшим количеством критичных нарушений за 3 месяца: научно-производственные организации (4181), производство (1968), финансовые организации (1847), транспорт и логистика (1335), органы государственной власти и предоставление государственных услуг (460).

4

Топ-5 подразделений, где чаще всего происходят внутренние нарушения ИБ и служебной дисциплины: бухгалтерия и финансы (14,8% инцидентов), ИТ и техподдержка (12,9%), кадры и маркетинг (10,3%), закупки (9,5%), отдел продаж (6,9%).

Методология

Данное исследование подготовлено на основе анализа обезличенных данных отчетов о пилотировании DLP-системы Solar Dozor в 97 организациях России и СНГ на протяжении трех лет: с 2018 по 2020 г. Из них 70 отчетов содержали информацию о различных внутренних нарушениях. При этом для целей исследования также было опрошено чуть менее 300 специалистов различных подразделений данных организаций.

DLP-система Solar Dozor ведет сплошной анализ трафика с рабочих станций сотрудников на предмет наличия в их ежедневной работе за компьютером признаков нарушений в области информационной безопасности и нарушений служебной дисциплины. Анализируются корпоративная электронная почта, веб-трафик (посещаемые интернет-сайты, сохранение информации на внешние облачные хранилища), хранение информации на рабочих компьютерах, ее копирование на съемные носители и сохранение на внутренних файловых хранилищах организации, печать документов.

В DLP-системе Solar Dozor, в соответствии с Национальным стандартом Российской Федерации ГОСТ Р ИСО/МЭК ТО 18044-2007, используется так называемая инцидентная модель управления рисками информационной безопасности.
При проведении пилотирования инцидентом является случай нарушения политики информационной безопасности организации, подтвержденный ответственным сотрудником ИБ-службы. Таким образом, все упомянутые в данном исследовании инциденты и статистика на их основе признаны самими заказчиками как нарушения.

Организации, пилотировавшие Solar Dozor, относятся к сегментам Small&Middle Business, Small&Middle Enterprise и Large Enterprise. Для большей наглядности вошедшие в исследуемую выборку организации сгруппированы по численности сотрудников на следующие категории: до 100 сотрудников, 100–200 сотрудников, 200–500 сотрудников, 500–1000 сотрудников, свыше 1000 сотрудников.

В выборку вошли такие рыночные сегменты, как производство, образование, финансы, розничная торговля, услуги, транспорт, культура, медицина, промышленность, ИТ/телеком, государственное управление и ряд других направлений — всего свыше 15 отраслей.

Пилотирование DLP-системы обычно проводится по желанию организации-заказчика перед принятием решения о покупке. Это позволяет бесплатно протестировать ее возможности на выбранном количестве реальных пользователей организации и оценить ее эффективность для решения реальных бизнес-задач потенциального заказчика.

Наибольшее количество перехваченных сообщений — свыше 13 млн — получено за время пилотного проекта длительностью 5,5 месяца (стандартная продолжительность не превышает 2 месяцев) в финансовой организации на выборке из 120 сотрудников, мониторинг действий на рабочих станциях которых велся непрерывно, а также 9000 корпоративных почтовых адресов.

Проанализированный трафик

Статистику собранного во время пилотов трафика, содержащего различные внутренние нарушения, авторам исследования предоставили 70 организаций. Общее количество собранных системой в этих пилотах сообщений составило свыше 40 млн единиц. В среднем примерно 600 тысяч сообщений в каждой из организаций.

Примечание: такой объем трафика может быть собран в организации численностью в 1000 человек за 40 рабочих дней.

При этом объем и плотность трафика (интенсивность переписки по разным каналам и других действий пользователей на рабочих станциях) от организации к организации значительно различаются. Помимо активности сотрудников, за которыми ведется мониторинг, эти показатели также зависят от целого ряда факторов: это и продолжительность пилотного проекта, и количество пользователей под наблюдением, и количество самих каналов перехвата (в одном случае под мониторинг попадает только переписка по электронной почте, а в другом — добавляется переписка через внешние почтовые ресурсы, переписка во всевозможных мессенджерах, а также копирование и печать файлов и их размещение в файловых хранилищах).

Аналитики отмечают, что отрасль организации влияет на объем собираемого трафика. Например, у организаций сферы услуг он выше, поскольку их ежедневные производственные процессы связаны с общением с клиентской базой. Все «абсолютные чемпионы» по объему собранного трафика относятся именно к сфере услуг. Свыше 1 млн собранных сообщений анализировалось системой в уже упомянутых финансовых организациях, организациях транспортно-логистической сферы, в компаниях-дистрибьюторах и в розничной торговле.

Введение

DLP-система Solar Dozor создавалась для целей выявления признаков утечек служебной информации / информации ограниченного доступа за пределы информационного периметра организации.

Однако при системном анализе обнаруживаемых с помощью DLP-системы инцидентов стало очевидно, что значительная часть нарушений, попадающих в поле зрения служб безопасности, связана с широким спектром случаев несоблюдения внутренних правил корпоративной безопасности и служебной дисциплины. Среди них и нарушения парольной политики организации, и нецелевое использование рабочего времени сотрудниками, и признаки конфликтных коммуникаций в переписке по корпоративной электронной почте, и многое другое.

Результаты данного исследования можно рассматривать как пособие по нарушениям внутренней ИБ и трудовой дисциплины и трендам, присущим компаниям разного размера и различных сфер деятельности.

Результаты исследования

По результатам исследования аналитики «Ростелеком-Солар» выделили профиль организации, наиболее подверженной различным видам нарушений внутренней ИБ и трудовой дисциплины, включая нарушение правил безопасного обращения со служебной информацией:

1000
человек

Крупная (свыше 1000 человек) производственная или научно-производственная организация.

1900
нарушений

3
месяца

В среднем за 3 месяца на 36 рабочих станциях и 300 почтовых ящиках сотрудников фиксируется 200 тысяч сообщений, из которых в среднем 1900 нарушают те или иные правила политик информационной безопасности.

7
серьезных рисков

При этом 7 из них признаются существенными инцидентами информационной безопасности и, по мнению ИБ-службы, несут в себе серьезные потенциальные риски для организации.

Организации-лидеры по числу внутренних нарушений ИБ и служебной дисциплины

1 В одной крупной финансовой организации среди накопленных 13 млн сообщений зафиксировано более 45 тысяч (!) нарушений политик безопасности, при этом событий критичного уровня — 54.

2 Еще большее количество нарушений — свыше 50 тысяч (!) — зафиксировано в геологоразведочной организации, где общий объем накопленного трафика за 2,5 месяца пилотирования составил чуть менее 200 тысяч сообщений. Таким образом, в среднем на каждое 4-е сообщение приходится 1 нарушение. При этом событий наивысшего — критичного — уровня в системе было зарегистрировано 62.

3 Также среди организаций с наиболее высокой долей событий информационной безопасности в общем объеме собранного трафика отметилась строительная компания. Здесь среди 22+ тысяч выявленных нарушений политик информационной безопасности (практически 10% всего собранного трафика в 200 тысяч сообщений) количество критичных событий достигло 51.

4 Замыкает четверку «антилидеров» организация сферы управленческого консалтинга и рекрутмента. Здесь среди 500 тысяч накопленных сообщений выявлено 14,5 тысячи событий, где каждое 30 сообщение содержит информацию о срабатываниях политики, настроенной в Solar Dozor совместно заказчиком и аналитиками. При этом именно в данной организации зафиксирована наиболее высокая доля критичных потенциальных нарушений — 196 (каждое 80-е!)

Аналитики «Ростелеком-Солар» подчеркивают, что большое количество выявляемых в общем трафике событий безопасности может быть связано как с действительно низким уровнем дисциплины среди сотрудников организации, так и со строгими настройками политик. В связи с этим эксперты рекомендуют пользователям DLP-системы (ИБ-службам) уделить внимание тщательному формированию политик. Это поможет оградить ответственных за администрирование DLP сотрудников от излишней ручной работы по анализу предварительно отфильтрованного трафика.

Общее количество событий информационной безопасности [1] в указанной выборке из 70 организаций составило свыше 320 тысяч — то есть примерно 4600 дисциплинарных и ИБ-нарушений в среднем в каждой организации. При этом здесь есть и яркие «антигерои».

[1] Под событиями информационной безопасности понимаются любые нарушения заранее настроенных в системе политик безопасного и оправданного с точки зрения должностных обязанностей обращения сотрудников с информацией.

Отрасли-лидеры по числу критичных внутренних нарушений ИБ

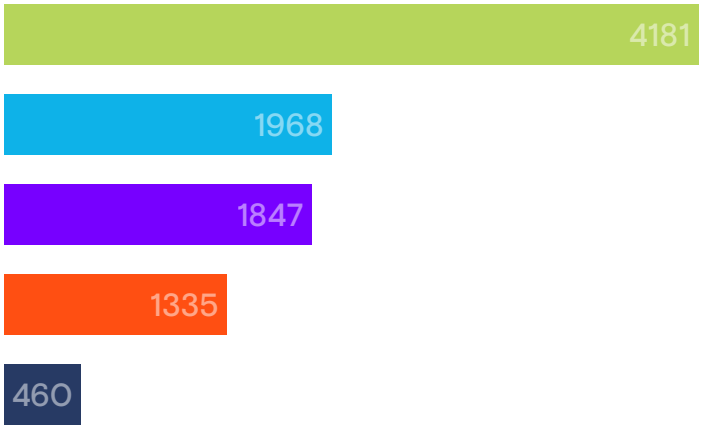
Наиболее часто в этих организациях встречаются следующие нарушения рабочей дисциплины и, в частности, политик информационной безопасности:

Нерегламентированная работа с документами с грифом ДСП и иными документами ограниченного распространения (бесконтрольное копирование на съемные носители, пересылка на внешние адреса электронной почты на бесплатных почтовых сервисах, хранение в открытом доступе во внутренней сети)

Нецелевое использование рабочего времени, включая поиск работы

Нарушение парольной политики

Топ-5 отраслей с наибольшим количеством критичных нарушений:



4181
Научно-производственные организации

1968
Производство

1847
Финансовые организации

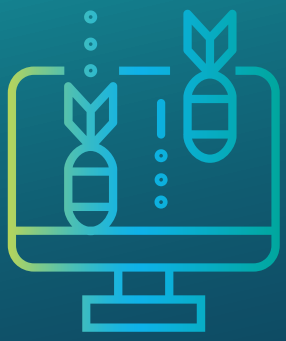
1335
Транспорт и логистика

460
Органы государственной власти и предоставление государственных услуг

Отделы-лидеры по числу нарушений

- 14,8% Бухгалетерия и финансым
- 12,9% ИТ, техподдержка и т.п.
- 10,3% Кадры, маркетинг
- 9,5% Закупки
- 6,9% Отдел продаж
- 5,2% Секретариат, АХО
- 5,2% Отдел снабжения
- 5,2% Конструкторскае бюро
- 5,2% Отдел строительства
- 3,4% Правовой отдел
- 3,4% Отдел статистики
- 2,6% Отдел логистики
- 1,7% Руководство
- 1,7% Корпоративное управление
- 12% Другое

Лидеры по числу выявляемых нарушений — подразделения, обслуживающие основные производственные процессы: бухгалтерия (14,8%), ИТ и техподдержка (12,9%), кадры и маркетинг (10,3%), закупки (9,5%). Суммарно на них приходится почти половина всех нарушений. В этих подразделениях чаще всего встречается «нецелевое использование рабочего времени».



Более дисциплинированные подразделения не стоит упускать из виду. Именно в них нарушения могут быть наиболее болезненными: через отдел продаж может утекать чувствительная информация о клиентах, а через конструкторское бюро — уникальные технологические наработки.

Вопреки мнению, что для производственного блока информационные утечки не характерны, именно организации производственной сферы проявляют наиболее высокий интерес к DLP.

Особенности исследованных срезов данных

Отраслевой ландшафт организаций

Доля производственных и строительных организаций, включая ТЭК, добычу и переработку природных ресурсов, составляет 33% от всех организаций, апробировавших в 2018–2020 гг. DLP-систему Solar Dozor. Высокий интерес связан с использованием DLP в том числе в целях контроля трудовой дисциплины сотрудников. Это подтверждают данные исследования: к наиболее распространенным нарушениям относятся нецелевое использование рабочего времени, поиск работы или несанкционированное совмещение основной и дополнительной работы, а также другие аналогичные нарушения. С другой стороны, часть производственных процессов в этих организациях связана ссозданием уникальных продуктов. Эту гипотезу подтверждает значительная доля научно-производственных организаций (15%) в исследуемой выборке (в основном военно-промышленного комплекса). В случае с ВПК речь явно идет об использовании DLP-системы по прямому назначению — для защиты от утечек информации, составляющей не только коммерческую, а зачастую и государственную тайну.

Ожидаемо высок уровень спроса на DLP-системы в организациях финансового блока (подробнее об утечках в финсекторе читайте в исследовании «Особенности защиты конфиденциальной информации в финансовом секторе»), а также предоставляющих транспортно-логистические услуги. Их доли в общем количестве испытывавших Solar Dozor составили соответственно 10% и 8%. Востребованность DLP связана с тем, что основным — и очень ликвидным! — активом в производственных процессах организаций этих типов являются клиентские базы, попытки краж которых постоянно растут.

Информация о гражданах в государственных информационных системах становится мишенью для злоумышленников на порядок реже. В то же время авторы исследования отмечают среди пилотирующих DLP-системы организаций весьма существенную долю структур сферы государственного управления (10%), в том числе занимающихся оказанием государственных услуг.

Невысокой остается доля телекоммуникационных компаний, а также ИТ-разработчиков и интеграторов среди групп потенциальной заинтересованности в DLP-решениях. В общей сложности они составляют около 7%. Аналитики связывают показатель с высоким уровнем технологической продвинутости указанной категории пользователей ИБ-решений. Большинство из них определилось с инструментами контроля еще несколько лет назад.

Размер организаций

Аналитики утверждают, что для средних и крупных компаний эффективность выбранного решения более очевидна за счет большой наблюдаемой выборки сотрудников (чем больше людей, тем выше вероятность обнаружить нарушение).

Также эффективность DLP в явном виде прослеживается, когда дело касается защиты исключительно ценной информации и/или данных, которые представляют высокий интерес для потенциальных злоумышленников (клиентские базы данных, уникальные разработки и т. д.).

Среди исследуемых компаний преобладают средние и крупные заказчики. Половину из них составляют организации численностью свыше 1000 человек. Это говорит о том, что внедрение и использование ведущих разработок в области DLP все еще требует от организации существенных ресурсов.

Контролируемые каналы

В рамках пилотирования потенциальный заказчик выбирает набор модулей DLP-системы, протестировать действие которых он хотел бы в среде организации. Абсолютное большинство пилотных площадок DLP-системы Solar Dozor испытывает все функциональные возможности, что говорит о высоком интересе к технологиям DLP. В то же время в реальной статистике пилотов прослеживаются наименее популярные источники трафика, которые, на первый взгляд, могут говорить о низкой заинтересованности заказчиков в контроле данных каналов. Так, наименее популярными являются функции контроля мессенджеров и публикаций документов в локальной сети. От первой категории отказались практически 75% пилотных площадок, от второй — порядка 40%.

Низкий интерес к контролю мессенджеров связан с тем, что контроль веб- и десктопных версий коммуникаторов сотрудников — даже используемых с рабочего компьютера в основное рабочее время — вызывает много этических и правомерных вопросов у большинства работодателей.

Юридическая служба компании «Ростелеком-Солар»: «Работодатель достаточно легко может обеспечить себе возможность мониторинга использования сотрудником рабочего времени и оборудования работодателя. Для этого достаточно заблаговременно предупредить сотрудников в рамках дополнительного соглашения к действующему трудовому договору или дополнительного пункта в соответствующем договоре, заключаемом с новыми сотрудниками, о возможности ведения соответствующего мониторинга, в том числе путем установки специального программного обеспечения на рабочие станции сотрудников, а также ввести в организации регламенты в том числе по сбору и обработке такой информации».

Корпоративная электронная почта почти единогласно признается ИБ-службами одним из основных каналов возможных утечек данных или источником информации о других нарушениях рабочей дисциплины сотрудниками.

Если при этом трудовой договор будет содержать описание порядка использования результатов такого мониторинга, например, при решении вопросов поощрений или дисциплинарных взысканий, формируется комплексная система применения DLP-решения во внутренних процедурах работы с персоналом.

Интересно при этом, что в финансовых организациях в рамках исследования «Ростелекома» именно мессенджеры признаны ИБ-специалистами одним из основных каналов утечек данных.

Невысокую популярность контроля сетевого трафика в локальной корпоративной сети (кто и что сохраняет на внутренних ресурсах) можно объяснить двумя факторами:

1. Во-первых, для большинства служб ИБ утечки — это факт выхода данных за рамки корпоративного информационного периметра. До тех пор, пока информация остается внутри, предполагается, что она собрана для использования по назначению.

2. Во-вторых, высокий интерес к модулю инспектирования файловых хранилищ File Crawler, который в ходе пилотов протестировали почти 90% участников, говорит об ориентации заказчиков не на процесс, а на результат. Вместо постоянного контроля перемещений документов по файловым хранилищам заказчики предпочитают контролировать результат — анализировать с помощью File Crawler то, что уже хранится в сетевых папках.

Мониторинг файловых хранилищ, в число которых попадают и рабочие станции самих сотрудников, позволяет выявлять достаточно специфические нарушения ИБ-политики, в частности небрежное обращение с паролями, а также несанкционированное размещение в открытом доступе строго конфиденциальной информации – например, организационно-штатной структуры компании или бонусных выплат сотрудникам.

В 2018–2020 гг. 90% пилотных площадок опробовали функциональность контроля электронной почты. В 51% случаев службы информационной безопасности интересовал анализ веб-трафика рабочих станций сотрудников. При том что одним из наиболее распространенных нарушений, выявляемых с помощью DLP-систем, является нецелевое использование рабочего времени, аналитики «Ростелеком-Солар» уверены, что реальный процент заинтересованных в анализе веб-трафика может быть гораздо выше.

Выводы

Компания «Ростелеком-Солар» представила результаты исследования «Какие организации чаще других подвержены внутренним нарушениям корпоративной безопасности и служебной дисциплины?».

В среднем в каждой из исследованных организаций, в которой были зафиксированы события информационной безопасности, на протяжении квартала происходит примерно 4600 дисциплинарных и ИБ-нарушений. Из них 7 признаются существенными инцидентами информационной безопасности и, по мнению ИБ-службы, несут в себе серьезные потенциальные риски для организации. Наибольший интерес к системам контроля служебной дисциплины и корпоративной безопасности проявляют производственные/научно-производственные организации со штатом свыше 1000 человек. При этом уже в ходе эксплуатации таких решений наибольший процент действительно серьезных нарушений отмечается в организациях сферы управленческого консалтинга и рекрутмента.

Авторы исследования отмечают, что столь высокий показатель может отражать как реальное положение дел с нарушениями в компании, так и недостаточно гибкие настройки политики защиты информации. Специалисты «Ростелеком-Солар» подчеркивают, что «идеальная» настройка политик безопасности возможна только в результате глубокого погружения в бизнес-процессы подразделений выделенной проектной группы компании и вовлечения опытного DLP-вендора, который заинтересован в качественной работе продукта для решения задач заказчика.

Однако в целом ряде случаев организации сами провоцируют возникновение ИБ-рисков, а также рисков нарушений сотрудниками рабочей дисциплины: например, уделяя недостаточное внимание проработке возможностей контроля тех или иных потенциально опасных каналов передачи данных, таких как мессенджеры.

На лидирующие по количеству нарушений подразделения – бухгалтерия (14,8%), ИТ и техподдержка (12,9%), кадры и маркетинг (10,3%), закупки (9,5%) – приходится около половины выявленных нарушений ИБ и служебной дисциплины.

Кроме того, результаты исследования показали, что значительная часть нарушений носит дисциплинарный характер. Наиболее часто в организациях встречаются следующие нарушения рабочей дисциплины: нерегламентированная работа с документами с грифом ДСП и иными документами ограниченного распространения (бесконтрольное копирование на съемные носители, пересылка на внешние адреса электронной почты на бесплатных почтовых сервисах, хранение в открытом доступе во внутренней сети), нецелевое использование рабочего времени, включая поиск работы, нарушения парольной политики.

При этом большинство из описанных проблемных тенденций «поведения» организации поддаются эффективному контролю, считают аналитики. Выполняемые на рабочих компьютерах процессы могут в автоматическом режиме агрегироваться и исследоваться на предмет соответствия рабочим функциям и задачам анализируемой должности или отдела. Вместе с этим автоматизированному анализу подлежит и внутренняя среда организации: интенсивность, продуктивность и тональность коммуникаций персонала. При условии приобретения мощной DLP-системы и тщательной настройки политик ИБ количество пользователей и объем контролируемого трафика не представляют проблемы: эффективному контролю поддаются миллионы сообщений, получаемых и отправляемых с тысяч почтовых ящиков.

Ростелеком
Солар

rt-solar.ru
rt.ru

Email:

solar@rt-solar.ru
support@rt-solar.ru

Телефоны:

+7 (499) 755-07-70 - продажи и общие вопросы
+7 (499) 755-02-20 - техническая поддержка

Адреса

125009, Москва, Никитский пер., 7, стр. 1
127015, Москва, Вятская ул., 35/4, БЦ «Вятка», 1-й подъезд