Ростелеком
Солар

Исследование «Особенности защиты конфиденциальной информации в финансовом секторе»

Июнь 2021

СОДЕРЖАНИЕ

КЛЮЧЕВЫЕ ЦИФРЫ

4/5

финансовых организаций, использующих DLP, фиксируют неоднократные утечки конфиденциальной информации

для 20%

компаний серьезная утечка информации обернулась крупным штрафом со стороны регуляторов

порядка 80%

участников опроса подтверждают увеличение объема утечек с переходом сотрудников на удаленный режим работы

36%

участников опроса оценили потенциальную экономию средств в результате предотвращенных утечек в более чем 10 млн руб. за последний год

33%

утечек в финансовом секторе происходят через интернет-каналы (облачные хранилища, интернет-почту и т. п.), а 28% – через мессенджеры. Всего участники исследования выделили 6 основных каналов, через которые утекают данные

100 млн руб.

самый крупный ущерб в результате произошедших утечек, который отметили респонденты. Он зафиксирован в организациях, не использующих DLP

100%

респондентов считают необходимым установку DLP-агентов на рабочие станции руководящего состава организаций

МЕТОДОЛОГИЯ

Данное исследование проведено методом электронных опросов финансовой части аудитории сайта компании «Ростелеком-Солар», портала по информационной безопасности Securitylab.ru, представителей направления по информационной безопасности финансовых организаций – в рамках крупнейшего форума по противодействию внутренним угрозам «DLP+» и отраслевого финансового портала bosfera.ru (издание «Банковское обозрение»).

В опросе приняли участие представители финансовых предприятий, относящихся к сегментам Small&Middle Business, Small&Middle Enterprise и Large Enterprise.

Всего в исследовании приняли участие свыше 100 специалистов в сфере информационной безопасности из финансовых организаций. Опросы проводились в период с марта по июнь 2021 года.

В ходе опросов респондентам предлагалось выбрать один из предложенных вариантов ответа или указать свой вариант ответа в свободной форме.

ВВЕДЕНИЕ

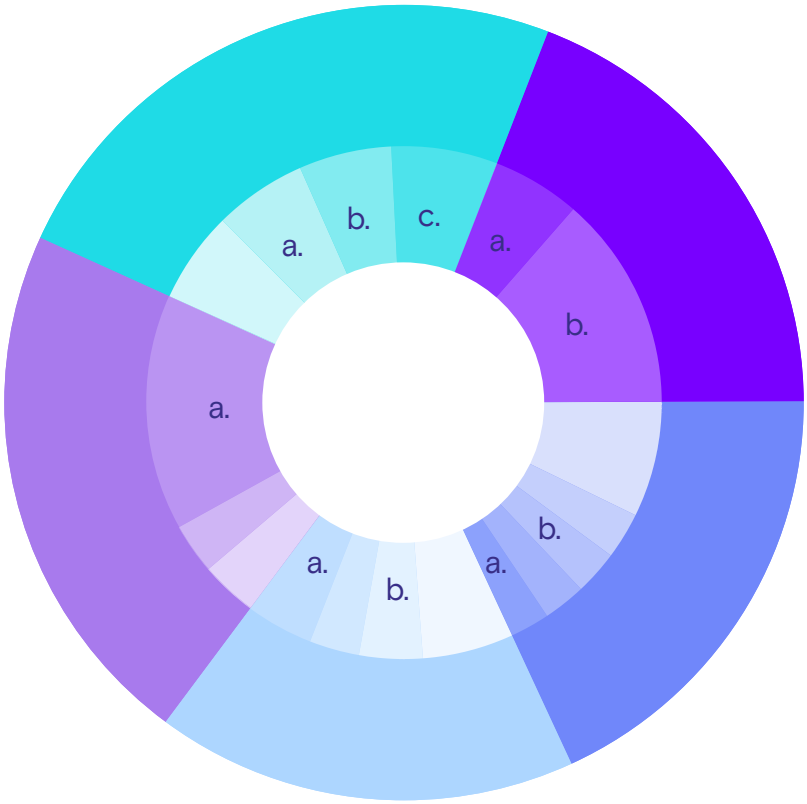
КОМПАНИЯ «РОСТЕЛЕКОМ-СОЛАР», НАЦИОНАЛЬНЫЙ ПРОВАЙДЕР ТЕХНОЛОГИЙ И СЕРВИСОВ КИБЕРБЕЗОПАСНОСТИ, ПРЕДСТАВЛЯЕТ ИССЛЕДОВАНИЕ «ОСОБЕННОСТИ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В ФИНАНСОВОМ СЕКТОРЕ».

Тематика исследования выбрана неслучайно: согласно данным отчета «2020 Q3 Report Data Breach QuickView» компании RiskBased Security[1], к концу 2-го квартала 2020 год стал худшим за всю историю наблюдений по объему скомпрометированных конфиденциальных данных в мире. А 3-й квартал добавил к этому «достижению» еще 8,3 млрд утекших записей, доведя их итоговое число к сентябрю до 36 млрд. И конечно же, именно финансовые данные, наряду с информацией о состоянии здоровья человека, являются самой чувствительной информацией – именно их утечка способна в кратчайшие сроки нанести максимальный ущерб.

Человеческий фактор продолжает быть движущей силой, наращивающей число скомпрометированных данных. При этом из 17% инцидентов компрометации данных внутри организации чуть менее 70% происходят по причине ошибочных действий персонала и лишь около 13% – по злому умыслу (в остальных случаях причину установить не удалось).

[1] Один из мировых лидеров в области анализа уязвимостей, данных о взломах и рейтингов рисков.

ФИНАНСОВАЯ СФЕРА – БАНКИ И СТРАХОВЫЕ КОМПАНИИ – ЗАНИМАЮТ ТРЕТЬЕ МЕСТО ПО КОЛИЧЕСТВУ ИНЦИДЕНТОВ КОМПРОМЕТАЦИИ ДАННЫХ, УСТУПАЯ ПО ЭТОМУ ПОКАЗАТЕЛЮ ЛИШЬ ЗДРАВООХРАНЕНИЮ И ИТ (СМ. РИС. НИЖЕ).



Finance and Insurance – 9,27%

a. Insurance (78)

b. Financial (196)

Public Administration – 8,77%

a. Federal Government (67)

b. Cities (70)

Professional, Scientific and Technical Services – 8,19%

a. Professional Services – NOC (73)

b. Accounting Services (72)

Information – 10,3%

a.Software Dev. & Web (260)

Healthcare and Social Assistance – 11,5%

a. Facilities (71)

b. Hospitals (117)

c. Practitioners (123)

В связи с актуальностью темы утечек конфиденциальных данных из финансовой сферы как в общемировом масштабе, так и в России эксперты «Ростелеком-Солар» подготовили данное исследование. Его результаты будут полезны как специалистам по информационной безопасности российских компаний, так и широкому кругу читателей, интересующихся тематикой утечек данных.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Тренды утечек конфиденциальной информации из финансового сектора

4/5 финансовых организаций, использующих системы DLP, фиксируют неоднократные утечки конфиденциальной информации. При этом в двух финансовых организациях, где был зафиксирован **наиболее масштабный** по объему ущерба «слив» конфиденциальной информации, **DLP-система не используется**. По оценке специалистов, ущерб в результате утечки данных платежных карт клиентов составил более 100 млн руб.

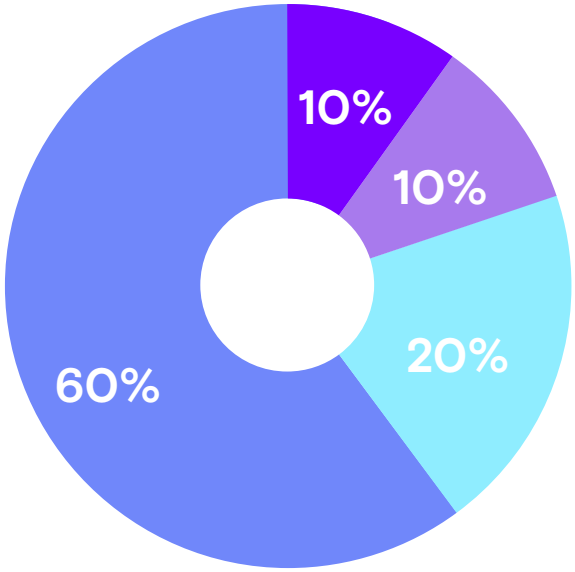
ВЫВОД

Покупка DLP-системы – это не гарантия отсутствия проблем. Ее настройка требует глубокого погружения службы ИБ и аналитиков, хорошо знакомых с внутренними бизнес-процессами организации. Собственно внедрение DLP-системы должно сопровождаться соответствующими методиками ее использования, которые наиболее компетентные DLP-вендоры специально разрабатывают для своих клиентов, а также набором организационных мероприятий по защите конфиденциальной информации. В то же время отсутствие DLP-системы является для финансовой организации потенциальным источником значительных рисков.

- Только 10 участников опроса уверены в том, что «удаленка» снизила угрозы утечек чувствительной информации в финансовой сфере; еще 10 респондентов считают, что количество утечек осталось на допандемийном уровне. **Абсолютное большинство участников опроса (80%)** отмечают увеличение объема утечек с переходом сотрудников на удаленный режим работы.

- Только 10 участников опроса уверены, что в ближайший год ситуация с утечками в финансовой сфере улучшится. Остальные респонденты считают, что уже в ближайшей перспективе (2021 год) потенциальный урон от утечек чувствительной информации для финансовой сферы станет выше.

Вырос ли объем утечек в финсекторе после перехода на удаленку?



- Нет, количество утечек даже снизилось
- Нет, остался на прежнем уровне
- Да, но незначительно
- Да, вырос значительно

ВЫВОД

Ожидать снижения количества утечек не стоит. На этот тренд явно указывают сами участники рынка. Что делать с этими прогнозами финансовым организациям, чувствительные данные которых все еще не защищены от «сливов», решать им самим. Однако обратить внимание на проблему следует уже сейчас, так как внедрение и настройка специализированных средств защиты DLP требует времени.

- **Утечки в банках чаще случаются «по неосторожности», чем «по злому умыслу».** Об умышленных утечках в чистом виде заявили только 20% респондентов. 30% опрошенных убеждены в том, что утечки носят случайный характер. Примерами таких «случайностей» могут быть необдуманная отправка данных третьим лицам или публикация служебной информации в таких открытых источниках, как социальные сети или мессенджеры. Остальные респонденты утверждают, что случайные и умышленные утечки существуют в их организациях в параллели.

ВЫВОД

Бесполезно вылавливать только тех злоумышленников, которые провоцируют утечки осознанно. Ущерб от действий сотрудников, неаккуратных в обращении с информацией, может быть не меньше. При этом проанализировать вручную огромный объем исходящего трафика, который характерен для любой крупной организации, никому не под силу. Необходима гибко настраиваемая автоматизированная система, которая будет «ловить» утечки вне зависимости от того, находится ли их источник под подозрением у службы ИБ.

Этика

Практически единодушно сотрудники служб информационной безопасности признают: персонал должен быть оповещен об установленных на рабочих станциях DLP-агентах. Против этого высказался всего 1 участник опроса.

С одной стороны, такая позиция – дань общей тенденции открытого и честного диалога бизнеса не только с внешними, но и с внутренними клиентами – собственными сотрудниками. Работодателю действительно проще честно предупреждать потенциальных злонамеренных сотрудников сразу. Кроме того, официальное предупреждение сотрудников о мониторинге корпоративных каналов коммуникации является обязательным условием для легитимизации использования DLP-системы в компании. В частности, это необходимо для сбора доказательной базы по инцидентам с целью ее передачи в суд.

С другой стороны, для добросовестного сотрудника, не подозревающего о том, что работодатель ведет непрерывный мониторинг его действий на рабочем компьютере, такой контроль – в случае его оглашения – может стать неприятным сюрпризом, а для компании-работодателя – большим репутационным риском.

Так, кратковременное отвлечение в течение рабочего дня на активности, напрямую не относящиеся к работе, является абсолютно нормальным для любого человека. Это может быть как просмотр прогноза погоды или новостей в поисковых системах, так и проверка входящих писем личной электронной почты с рабочего компьютера и так далее. В данном случае мониторинг личной почты сотрудника при отсутствии должных веских оснований и его заблаговременного предупреждения и есть то самое «узкое горлышко» для деловой репутации компании. Этот факт может стать поводом для судебных разбирательств о неправомерном вторжении в частную жизнь.

100% респондентов оправдали установку DLP-агентов на рабочие станции руководящих сотрудников организации, включая рабочие компьютеры высшего руководства. «Все под подозрением» или «Перед законом все равны»?

Виды нарушений и каналы

Такие экономические преступления сотрудников, как мошенничества с информационными активами работодателя, коммерческие сговоры и конфликты интересов, вызывают серьезное беспокойство лишь у 10% опрошенных представителей финансовых организаций. Столько респондентов указало на эту категорию нарушений как на мотив для установки в организации DLP-решения. 90% участников отмечают, что при покупке DLP-системы основной задачей был контроль утечек конфиденциальных данных (в первую очередь, это персональные данные и данные платежных карт клиентов).

При этом почти у всех респондентов гипотезы, за чем или кем в финансовой организации нужно наблюдать в первую очередь, подтвердились в процессе эксплуатации DLP-системы.

ВЫВОД

Ключевой актив финансовых организаций, подавляющее большинство которых являются банками, – это клиенты. Содержание любых других бизнес-процессов в финансовых организациях дает потенциальным нарушителям гораздо менее ценный и быстрый результат для обогащения, чем мошеннические операции с данными клиентов. Это говорит о том, что сотрудники, работающие с клиентами, должны относиться к группе особого контроля.

Респонденты отметили 6 преобладающих каналов утечек информации из финансовых организаций – это утечки через интернет (внешние облачные хранилища, интернет-почта и т.п.), мессенджеры, корпоративная электронная почта, съемные носители информации (USB и т. п.), печать на принтере и специализированные внутренние системы организации. На канал «утечки через интернет» приходится более 30% инцидентов. В 28% случаев данные утекают из организации через мессенджеры. Еще примерно в 24% случаев – через корпоративную электронную почту. Остальные 15% приходятся на съемные носители информации, печать на принтере и внутренние системы банка.

ВЫВОД

При выборе DLP-системы следует обращать внимание на ее способность перехватывать трафик по широкому кругу различных каналов. Потенциальные нарушители могут использовать любые из них. Принцип «чем больше – тем лучше» в этом случае работает на все 100%.

Несмотря на то, что значительная доля утечек происходит через мессенджеры, 55% респондентов либо высказались против полного запрета на использование сотрудниками на рабочих местах программ-коммуникаторов и социальных сетей, либо отметили необходимость «разумных ограничений для отдельных сотрудников с учетом занимаемой ими должности».

ВЫВОД

Тотальные запреты на коммуникации – не выход. При этом именно соцсети и мессенджеры являются потенциальным каналом злонамеренных утечек чувствительной информации, их пользователей зачастую отличает небрежное отношение к конфиденциальным данным. Молодые сотрудники не осознают, к каким проблемам может привести публикация в новостной ленте или отправка знакомым в чат корпоративного документа или инсайдерской новости, чтобы «обсудить, как время появится». Следить за информацией, передаваемой через мессенджеры и соцсети, нужно так же внимательно, как за перепиской по электронной почте.

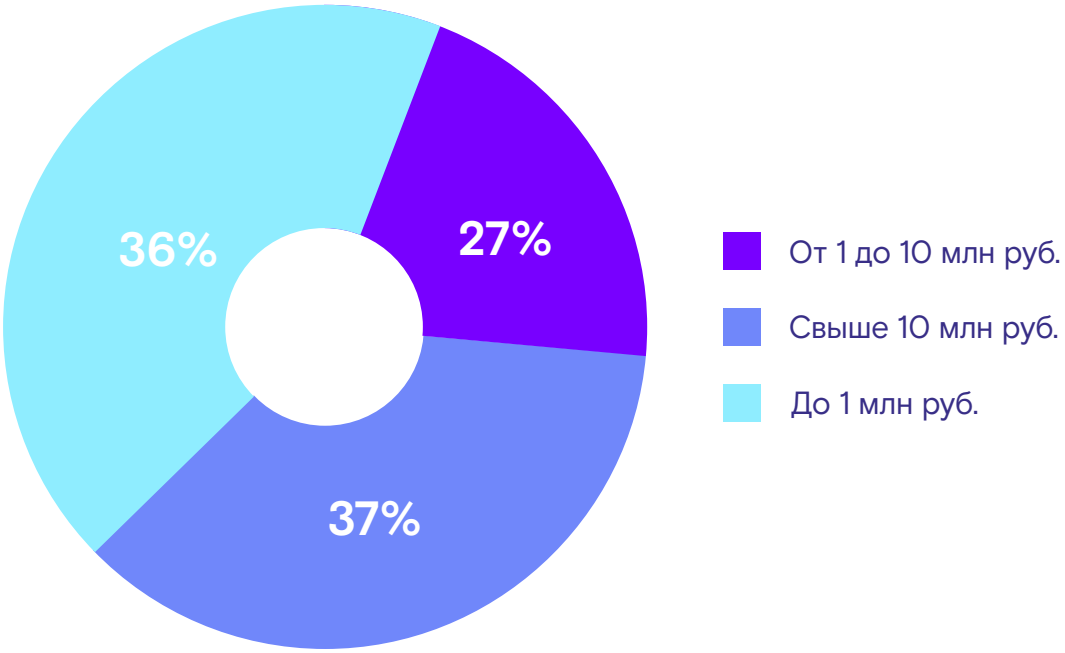
Оценка эффективности DLP-системы

В 2/3 случаев перед организациями, использующими DLP-систему, стоит задача оценки эффективности ее работы. При этом в 50% таких организаций эффективность определяется снижением размера экономического ущерба от случаев мошенничества, выявленных с помощью DLP-системы. Некоторые организации пытаются оценить репутационный ущерб от несостоявшихся утечек, предотвращенных благодаря DLP. Примерно в 20% организаций, использующих DLP-системы, несмотря на задачу оценки эффективности ее использования, конкретной методики ее определения нет. В 20% случаев наличие DLP-системы не нуждается в финансовом обосновании эффективности своей работы.

Ущерб

20% участников опроса утверждают, что масштабные утечки в их банках обернулись для организаций крупными штрафами со стороны регуляторов. Менее 10% респондентов отметили случаи, когда утечка в банке не повлияла ни на сам банк, ни на ответственных сотрудников. Более 70% участников опроса рассказали, что утечки чувствительной информации являются основанием для привлечения ответственных сотрудников к дисциплинарным взысканиям (вплоть до увольнения).

«Экономия в результате предотвращенных утечек, финсектор, 2020»



ВЫВОД

Тот факт, что банки в большинстве случаев привлекают к ответственности сотрудников, спровоцировавших утечку конфиденциальной информации, неудивителен. 36% участников опроса оценили потенциальную экономию средств в результате предотвращенных утечек в более чем 10 млн руб. за последний год.

При этом в 2 случаях реальный ущерб от случившихся инцидентов составил более 100 млн руб. В свете этого принимаемые меры реагирования со стороны руководства финансовых организаций выглядят более чем адекватными.

Самый значительный размер реального ущерба от произошедших утечек (свыше 100 млн руб.) зафиксирован в финансовых организациях, не использующих DLP-системы и базирующихся в регионах РФ.

ВЫВОД

Потенциально это может свидетельствовать о более низком уровне развития технологий или осведомленности об их правильном применении у региональных игроков по сравнению с крупными мультирегиональными участниками рынка. Эксперты «Ростелеком-Солар» рекомендуют финансовым организациям, локально базирующимся в отдельных субъектах РФ, особенно внимательно изучить ландшафт технологий защиты от утечек.

Содержание утечек достаточно однотипно. В 90% случаев «утекали» персональные данные клиентов и сотрудников организации, а также данные платежных карт. На долю первых пришлось около 60% случаев, на долю вторых – около 30%. Очевидно, что вероятность использования похищенных платежных данных в мошеннических операциях крайне высока. В этом случае прямой ущерб для клиентов становится зеркальным отражением репутационного ущерба для банка. И лишь в менее чем 10% случаев достоянием мошенников становится чувствительная коммерческая информация самого банка: данные маркетинговых исследований, информация о планах стратегического развития организации и др.

ВЫВОД

Недобросовестные сотрудники могут вынести за корпоративный периметр совершенно разную информацию, среди которой традиционно преобладают данные о клиентах и их финансовых инструментах. Поэтому просто приобрести и развернуть DLP недостаточно. Настройка DLP-системы, установленной в банке, должна быть достаточно гибкой и учитывать разные аспекты бизнес-процессов в организации.

ВЫВОДЫ

Результаты исследования показали, что представители финансовых организаций отмечают рост количества утечек, связанный с уходом сотрудников на удаленный режим работы.

20% участников опроса утверждают, что масштабные утечки в их банках обернулись для них крупными штрафами со стороны регуляторов. В 36% случаев компаниям удалось сэкономить более 10 млн руб. за последний год в результате предотвращенных утечек благодаря внедрению DLP-систем. При этом в 2-х случаях реально произошедшие утечки обошлись организациям, не применявшим DLP, в более чем 100 млн руб. Большинство респондентов убеждены, что уже в ближайшей перспективе (2021 год) потенциальный урон от утечек чувствительной информации для финансовой сферы возрастет.

В большинстве случаев из финансовых организаций «утекали» персональные данные клиентов или данные платежных карт. Защита этой информации – основной мотив приобретения DLP-системы. Однако несмотря на наличие DLP, 4/5 организаций по-прежнему фиксируют утечки данных. Это говорит о том, что внедрение DLP-системы – это не гарантия отсутствия проблем. Решения класса DLP требуют концентрации усилий в области проработки политик безопасности и постоянной синхронизации с бизнес-процессами, освоения методик использования систем защиты от утечек и внедрения организационных мероприятий по защите конфиденциальной информации. Только в этом случае данное средство защиты будет демонстрировать свою эффективность.

Ростелеком
Солар

rt.ru
rt-solar.ru

E-mail:
info@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, ул. Вятская, 35/4, БЦ «Вятка», 1-й подъезд