По данным отчета Аналитического центра InfoWatch, в первой половине 2014 года число утечек информации из компаний возросло и Россия оказалась на втором месте в мире по количеству таких инцидентов.

Россия вновь заняла уже привычное второе место (96 утечек), которое досталось нашей стране еще по итогам I полугодия 2013 года.

Результат сам по себе неприятный, но в действительности все еще хуже. Сравнивая количество утечек в России и западных странах, надо помнить о том, что в США, например, компании обязаны уведомлять общественность, и прежде всего пострадавших, о каждом случившемся инциденте. Это значит, что число утечек, получивших освещение в открытых источниках в США или странах Европы, довольно близко к реальному числу инцидентов. В России же, по оценкам аналитиков InfoWatch, достоянием общественности становится только 4—8% от общего числа утечек. Но даже этих 4—8% достаточно для того, чтобы занять и твердо удерживать второе место.

Откуда утекает информация?

Чаще всего, почти в половине случаев, от утечек информации страдают коммерческие организации.

Утечки по отраслям:

Статистика I половины 2014 года показывает, что государственные органы больше не задают тон в картине утечек. Хотя доля утечек из государственных учреждений в I полугодии 2014 года снизилась всего на 1,5 п. п., составив **28,7%**

Это вполне объяснимо: они обладают наиболее ценной и легко конвертируемой в деньги информацией. Это не только большие объемы персональных и платежных данных, но и специфическая информация о планах развития компании, ноу-хау, новых технологиях — все это имеет высокую ценность при продаже конкурентам. И, конечно, один из самых частых сценариев злонамеренной утечки — это кража клиентской базы компании менеджером, меняющим место работы. Такой инцидент оказывает серьезное негативное воздействие практически на любую компанию, но больше всего страдают обычно страховые, туристические и другие компании, чей бизнес напрямую зависит от лояльности клиентов — физических лиц. Заполучив базу клиентов, конкурент предложит им те же услуги по чуть более низкой цене. Конвертация при этом составит практически 100%. Убытки для компании, допустившей утечку, будут очень серьезными.

Кто виноват?

В 71% случаев в утечке информации — случайной или умышленной — виноват рядовой сотрудник компании. Предсказуемо, что обычно это человек, еще работающий в организации, ведь у него все еще есть легитимный доступ ко всем ресурсам, документации, чертежам и т. п. Но иногда организовать утечку могут и бывшие сотрудники, затаившие зло против компании.

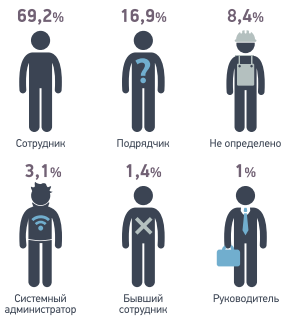
Достаточно часто проблема возникала на стороне подрядчиков компаний, и конфиденциальная информация утекала по их вине (8,4%). Топ-менеджеры же выдают секреты своей компании крайне редко — в 1% случаев.

Виновники утечек:

Велика доля утечек, случившихся на стороне подрядчиков, чей персонал имел легитимный доступ к охраняемой информации (8,4%). В 1% случаев виновными оказались высшие руководители организаций (топ-менеджмент, главы отделов и департаментов).

В **71%** случаев виновниками утечек информации были сотрудники компаний – настоящие или бывшие (69,2% и 1,4% соответственно).

Из этого следует, что внедрение технических средств для защиты от утечек информации непосредственно в компании поможет выявить и предотвратить около 70% всех инцидентов и спасти организацию от финансового и репутационного ущерба.



Что воруем?

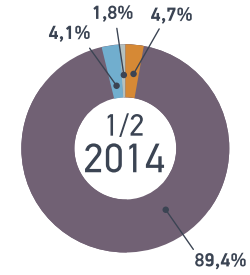
Чаще всего из компаний «утекают» персональные данные и платежная информация. Как уже говорилось, причина в том, что эти данные наиболее ликвидны. Коммерческая и государственная тайна, ноу-хау утекают реже, но стоимость одной такой утечки может быть гораздо выше, чем утечка персональных данных.

Типы информации:

В ходе 14 крупнейших утечек скомпрометировано более 430 млн записей клиентов и сотрудников компаний

- Персональные данные и платежная информация
- Коммерческая тайна, ноу-хау
- Государственная тайна
- Не определено

При этом персональные данные — это информация, которую современные системы защиты от утечек могут легко детектировать в общем потоке информации. Например, современные технологии DLP выявляют передачу данных паспортов и банковских карт как в текстовом формате, так и в виде изображений (сканов). Так же выявляется и другая персональная информация: ФИО, телефоны и пр.



Как утекает информация?

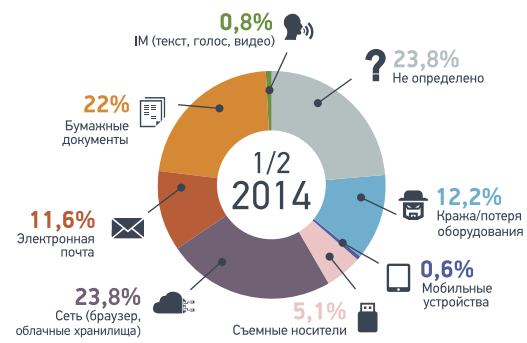
Чаще всего (в 23,8% случаев) сотрудники компании отправляют ценную корпоративную информацию третьим лицам с личной почты или загружают файлы в «облачное» хранилище. И примерно с той же частотой просто распечатывают конфиденциальные документы на принтере и выносят их из компании — 22%. Чуть реже компрометация корпоративной информации происходит в результате кражи или потери оборудования (например, ноутбука или планшета), на котором она хранилась. По электронной почте ценные данные уходят в 11,6% случаев.

Каналы утечек:

Процент снижения/увеличения количества утечек относительно прошлогодних показателей.

- 4,8% ↑ Не определено
- 12,1% ↑ Сеть (браузер, Cloud*)
- -17% ↓ Кража/потеря оборудования
- 3,9% ↑ Электронная почта
- -0,4% ↓ Мобильные устройства
- -3,4% ↓ Бумажные документы
- -0,1% ↓ Съемные носители
- 0% IM (текст, голос, видео)

* Облачные хранилища



Проанализировав данные исследования InfoWatch, можно сделать вывод о том, что и тип наиболее часто утекающей информации, и каналы, используемые для организации утечки, и даже потенциальные нарушители — все это уже давно и успешно контролируют технические средства для защиты от внутренних угроз. Внедрение такого решения если не обеспечит стопроцентную безопасность данных компании, то, по крайней мере, на порядок повысит уровень информационной безопасности и, следовательно, сократит издержки компаний, которые неминуемо возникают в результате каждой утечки.