
Компании и человек всегда были уязвимы перед утечкой информации. Среди опрошенных 800 компаний каждая вторая страдала от утечки данных. Почему же это происходит и кто в этом виноват? Разберем подробно «виды» сотрудников, которые так или иначе влияют на это.

Итак, верхний уровень составляют «граждане» - лояльные служащие, которые очень редко (если вообще когда-либо) нарушают корпоративную политику и этику и, в основном, не являются угрозой безопасности.

На втором уровне находятся «нарушители», составляющие большую часть всех сотрудников предприятия. Эти сотрудники позволяют себе небольшие фамильярности, работают с персональной веб-почтой, играют на рабочем месте в компьютерные игры и осуществляют онлайн-покупки. Представители данного уровня нарушителей создают угрозу информационной безопасности, но эти инциденты являются случайными и непреднамеренными.

На следующем уровне находятся «отступники» - работники, которые большую часть рабочего времени делают то, что они делать не должны. Эти служащие злоупотребляют своими привилегиями по доступу к Интернету. Более того, такие сотрудники могут посылать конфиденциальную информацию компании внешним адресатам, заинтересованным в ней. Таким образом, «отступники» представляют серьезную угрозу безопасности.

На самом нижнем уровне находятся «предатели». Это служащие, которые умышленно и регулярно подвергают конфиденциальную информацию компании опасности (обычно за финансовое вознаграждение от заинтересованной стороны). Такие сотрудники представляют реальную угрозу, но их сложнее обнаружить.

Обиженные. В эту категорию относят работников, которые были уволены по инициативе работодателя и при уходе с работы успели унести важную и/или конфиденциальную информацию. Позже они распространяют ее за плату или безвозмездно в отместку за нанесенную обиду.

Чаще всего информация «утекает» потому что, сотрудники компании делают следующее:

Переход по фишинговой ссылке с рабочего компьютера и заражение вредоносной программой корпоративной сети;

Хранение конфиденциальных данных на сменных носителях информации;

Пересылка информации с секретными данными по обычной электронной почте или через незащищенный мессенджер.

Например, я работаю в крупной компании, у нас огромная клиентская база, в которой собрана информация о нескольких миллионах человек, в том числе звезд и правительства. Перед тем как новому сотруднику доверить работу в данной системе, он проходит обучение безопасности клиентской базы. В офисе нет доступа к интернету, на всех компьютерах стоит защита, работает отдел безопасности, но даже несмотря на это у нас часто случаются атаки. Приходят письма на корпоративную почту, сами сотрудники рискуют и «сливают» информацию. В итоге, наша компания проводит инструктаж и далее мы подписываем бумаги о том, что мы знаем что делать в случае кибер атаки и какое наказание будет за утечку информации. И даже, если по вине сотрудника произошла утечка, а он этого и не хотел, ну случайно вышло-он все равно понесет наказание. (даже уголовное)

Поэтому, я считаю, что если компания владеет очень большой базой кл,то она должна сделать все, чтобы утечки не происходило, не экономить на защите, не давать открытый доступ в интернет( у всех сотрудников есть телефоны и интернет) проводить инструктаж, рассказывать что делать в случае атаки и тд.

Деля вывод, можно выделить следующее: меры по обеспечению информационной безопасности на предприятии должны разрабатываться и реализовываться постоянно, независимо от роли IT-инфраструктуры в производственных процессах.

К решению этого вопроса необходимо подходить комплексно и с привлечением сторонних специалистов. Только такой подход позволит предотвратить утечку данных, а не бороться с ее последствиями.