PERIMETRIX®

Комментарии к статье «О внутренних угрозах информационной безопасности предприятий» заместителя директора Регионального центра компетенций Perimetrix Максима Жарникова

Сполохи информационных войн

Статистика по утечкам данных, приведенная в статье коллег из InfoWatch, наверняка будет интересна читателям — руководителям фирм, IT-специалистам, безопасникам. В то же время большинство воспримет представленные цифры как нечто отвлеченное, относящееся к «большой» реальности и дистанцированное от «личной» действительности.

Новости об инцидентах в сфере информационной безопасности у таких гигантов бизнеса, как Apple, AT&T, British Airways, DreamWorks, Electronic Arts, Google, вполне могут лечь в основу остросюжетных блокбастеров с притягивающей зрителя ремаркой «Основано на реальных событиях». Ничего удивительного — вращающиеся там деньжищи способны спровоцировать корпоративные войны с коварными интригами, настоящими шпионами и высокопрофессиональными хакерами.

Но стоит ли бояться всех этих бондовских, джеймс-бондовских траблов руководству «обычной» компании, в которой работа с персональными данными — «как у всех», нет «сведений, содержащих государственную тайну», а конкурентами являются не монстры хайтека, а себе подобные организации — заводы, проектные институты, торгово-производственные предприятия?

Бояться — точно не стоит. Но задуматься и проницательно посмотреть на собственную компанию с точки зрения возможных информационных «свищей» нужно непременно.

Секреты, простые и сложные

«Секреты фирмы» есть почти у любой компании. Однако прежде чем начинать бороться с их утечками, нужно тщательно проанализировать, что же представляют собой тайны именно вашей компании.

Есть ли вообще они у вас? Какая корпоративная информация имеет дополнительную ценность для вашего бизнеса, будучи скрытой от посторонних?

Являются ли ваши секреты «простыми» по своей форме? Можно ли их банально записать на бумажном листе или унести в голове, чтобы затем воспроизвести заинтересованной стороне? Или же это, наоборот, «сложные» секреты, которые существуют исключительно в форме трудновоспроизводимых данных и документов, созданных благодаря работе значительного числа людей и оттого еще более ценных?

Если секрет «прост» и может быть похищен сравнительно легким способом (просмотром, пересказом, переписыванием, фотографированием) — не тратьте усилий на сложные технические защитные меры. Они все равно не помогут. Нацельтесь на мониторинг действий сотрудников, так как они суть основной «коммуникационный канал» вашей компании с внешним миром и от их дисциплины и лояльности будет зависеть сохранность секретов.

А вот если ваши секреты представляют собой сложные информационные продукты (чертежи, проекты, материалы исследований, базы данных), которые могут утечь только по «техническим каналам связи», то неприкосновенность подобных ценных сведений может достигаться уже с помощью специализированных защитных средств. Причем, как это ни покажется странным, сложная форма вашего секрета может упростить задачу по его защите.

Запрещено все, кроме того, что разрешено

Самое важное, что должен сделать хозяин секрета (владелец компании, топ-менеджер), — это описать и внедрить «правильный» процесс работы с информацией ограниченного доступа.

Но не стоит поручать это IT-специалистам. Зачастую, не имея четкого представления о том, какие бизнес-задачи и рабочие процессы связывают сотрудников и ценную информацию в компании, они придерживаются принципа «не навреди» (а то и «моя хата с краю») и предоставляют самим сотрудникам право определять допустимые действия с ценными сведениями. Что, безусловно, не способствует информационной безопасности и порядку.

Ситуация не меняется, даже когда доступ к важным данным оставлен только ограниченному числу сотрудников. Оставаясь вольными в своих действиях с ценной информацией, они неизбежно разбросают ее повсюду, потому что «им так удобнее». Но как нельзя быть «немножко беременным», так и сведениям нельзя быть «немножко секретными». Надо четко усвоить, что в отношении корпоративных секретов допустим только один принцип: «Запрещено делать всё, кроме того, что в явном виде разрешено».

Приведенные коллегами «10 самых распространенных ошибок сотрудников, приводящих к утечке», имеют одну первопричину — отсутствие в организации порядка в бизнес-процессах и документообороте, неустроенность жизненного цикла ценных данных.

Возьмите на себя труд пройти следующие шаги:

- дифференцируйте и классифицируйте ценную информацию, чтобы отделить ее от «просто» информации, утечка которой не повлечет ущерба;
- определите, как должна создаваться, храниться, копироваться, вообще двигаться ценная информация в рабочих процессах;
- определите и стандартизируйте, насколько это возможно, основные бизнес-процессы, чувствительные к вопросам информационной безопасности;
- минимизируйте до необходимой и достаточной степени ознакомление сотрудников с секретными данными;
- обучите и впоследствии требуйте от сотрудников дисциплинированно придерживаться разработанных правил.

В результате наведения порядка в работе с секретами значительно снизится вероятность «популярных» информугроз лично для вашей организации.