Информационная безопасность

КРОШИЛИН Сергей Викторович *- кандидат технических наук, доцент кафедры менеджмента и маркетинга Коломенского государственного педагогического института, лектор курсов МВА Акапдемии народного хозяйства при Правительстве РФ*

тел. раб.: (496) 615-13-19;

e-mail: Krosh_sergey@mail.ru

ИНСАЙДЕР – ВНУТРЕННИЙ ВРАГ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КОМПАНИИ

Как выжить в конкурентной борьбе в условиях кризиса – основной вопрос всех участников бизнеса сегодня. Информация сейчас - это главное оружие в конкурентной борьбе: знание ситуации, анализ и контроль для взвешенных и своевременных решений. Утечка информации за пределы компании может нанести непоправимый ущерб ее репутации и финансовому положению. Как правило, в 95 % случаях утечек информации задействован собственный персонал предприятия, то есть легальные пользователи. Именно такие утечки называют «инсайдерскими».

Само понятие «инсайдер» в различных источниках имеет разную трактовку. Это английский термин, который в нашем случае по классическому определению означает – «член какой-либо группы людей, имеющей доступ к информации, недоступной широкой публике». С точки зрения информационной безопасности, инсайдер – сотрудник компании, имеющий доступ к конфиденциальным данным, размещенным в компьютерной сети предприятия.

Обычно инсайдерами являются директора и старшие менеджеры, а также владельцы более 10% голосов компании. Однако это может быть и секретарша, по ошибке переславшая «не то и не туда», и злоумышленник, специально внедренный для кражи данных.

Чтобы эффективно бороться с врагом, надо знать его в лицо. Всех инсайдеров условно можно разделить на 4 группы: «послушные», «нарушители», «преступники», «кроты–предатели».

«Послушные» – это лояльные служащие компании (тихони), которые никогда или очень редко нарушают правила корпоративной политики и, в основном, не являются угрозой безопасности. В то же время, согласно статистике, от 80 до 90% всех зарегистрированных утечек данных были следствием неосторожности или безалаберности сотрудников.

«Нарушители» – в большинстве своем представители «планктона» и топ-менеджмента компании. Они позволяют себе небольшие фамильярности относительно информационной безопасности (ИБ): работают с персональной веб-почтой, играют в компьютерные игры и совершают онлайн покупки. Этот класс инсайдеров представляет угрозу ИТ-безопасности, но сопутствующие им инциденты являются случайными и неумышленными. Однако не следует забывать, что большинство внешних атак начинаются именно с ICQ или web-ящика сотрудников.

«Преступники» – работники, которые проводят большую часть дня за тем, чего они делать не должны. Как правило, это топ-менеджеры, которые злоупотребляют своими привилегиями: по доступу к интернету, самовольно устанавливают и используют различные приложения. Более того, такие сотрудники могут отсылать конфиденциальную информацию компании внешним адресатам, заинтересованным в ней. Этот класс инсайдеров представляет серьезную угрозу ИТ-безопасности.

«Кроты-предатели» – служащие, которые умышленно и регулярно крадут конфиденциальную информацию компании (обычно за финансовое вознаграждение от заинтересованной стороны). Такие сотрудники представляют собой самую большую угрозу и их сложнее всего поймать, так как обычно это достаточно опытные пользователи, «заметающие» за собой следы.

Не следует забывать об определенной специфике информации – ее неиссякаемости. Информацию можно продавать всем или несколько раз. В России давно привыкли брать то, что «плохо лежит», поэтому редко кто может устоять перед соблазном заработать на эксклюзивном доступе к данным.

В нашей стране значительно чаще, чем за рубежом, уволенные сотрудники забирают с собой оперативную рабочую информацию – например, контакты, сведения о бизнес-планах, персональные данные, финансовые отчеты. Инсайдеры «торгуют» финансовыми отчетами, деталями конкретных сделок и даже интеллектуальной собственностью компании (см. рис. 1) [3].

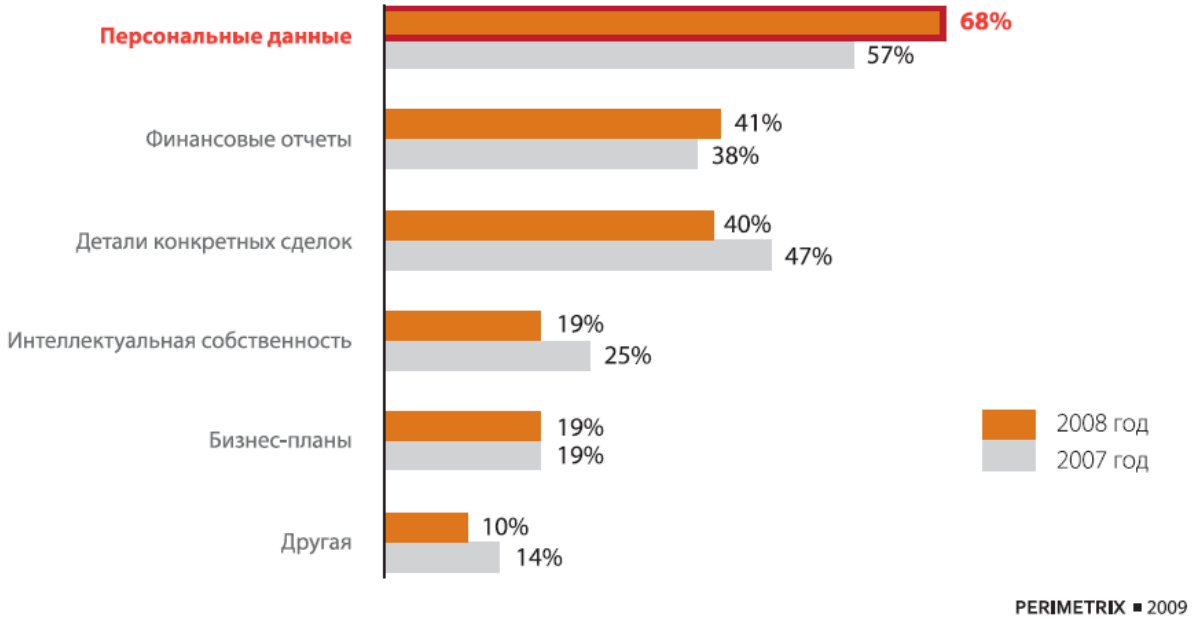

Рис. 1. Результаты исследований компании Perimetrix по вопросу «Информация, наиболее подверженная утечке (можно было выбрать до двух вариантов)»

Известна мировая формула, согласно которой утечка всего 20 % корпоративных секретов в 60% случаев приводит фирму к банкротству. В России примеров полного разорения компании после утечки информации не зафиксировано. Причина кроется во многих факторах, о которых мы еще скажем.

В России меньше знают об инсайдерах и утечках информации, чем за рубежом, так как случившееся многим проще «замять», дабы не выносить сор из избы. Так, например, в период «лихих 1990-х» многие НИИ лишились своих разработок, которые потом появились и успешно продавались иностранным компаниям. В наши дни продают финансовую отчетность из налоговых органов через интернет. Причины такой ситуации – в ощущении безнаказанности, ведь в российских условиях судебное преследование грозит лишь 9% инсайдерам. Максимум, что могут сделать – это уволить, иногда наложат штраф (в виде лишения премии). И всё. Для сравнения: в США всех внутренних нарушителей такого типа рано или поздно ждет крупный штраф и/или даже тюремное заключение.

К сожалению, несмотря на бурную законотворческую деятельность, российские предприятия еще очень далеки от практической реализации эффективной системы защиты персональных данных. Для справки: по нашим подсчетам, порядок работы с персональными данными в России регулируют более 30 законов (в том числе федеральных), указов, постановлений, приказов и распоряжений. Излишне говорить, что разобраться в этом нормативном буйстве очень сложно даже профессионалу. Тем более, приблизительно 7 млн. юридических лиц и ИП, которые согласно ФЗ «О персональных данных» оперируют этими самыми данными и обязаны соответствовать требованиям закона.

Инсайдерские утечки - это целый спектр неприятностей: начиная от потраченных нервов, срыва сделок, ущерба репутации и заканчивая прямой угрозой бизнесу. По определению, бизнес – это самостоятельная, осуществляемая с риском, деятельность с целью получения систематической прибыли. А эту прибыль кто-то может получать вместо вас.

Российские компании обычно замалчивают об утечках, чтобы сохранить публичный имидж, а некоторые просто не в состоянии их учитывать. Исследования российской компании Perimetrix показывают, что в 2008 году 42% российских организаций затруднились назвать хотя бы приблизительное количество подобных инцидентов.

Причина кроется в нежелании нести дополнительные расходы на ликвидацию последствий утечек, оповещение пострадавших и возмещение понесенного ими ущерба. Очень часто в наших компаниях полагаются «на авось», считая, что утечку никто не заметит. Информация об инцидентах часто вовсе не доходит до руководства – сотрудники опасаются санкций со стороны начальства или просто не принимают их всерьез.

Кроме случаев, хоть как-то обнаруживаемых внутри компаний, существуют еще утечки-фантомы, о которых никто ничего не знает. Доля таких утечек особенно велика, поскольку далеко не все компании имеют средства для их выявления.

Напомним, что инсайдеров интересуют персональные данные, финансовые отчеты, детали конкретных сделок, интеллектуальная собственность и бизнес-планы. Эти виды информации присутствуют во всех сферах деятельности и отраслях. Однако угроза нарушения конфиденциальности данных растет пропорционально приближению организации к «живым» деньгам (банковская и финансовая сферы, коммерческая деятельность, торговля, производство и т.д.) и персональным данным (сотовая связь, телекоммуникации, налоговые органы, государственные учреждения любого учета и т.д.). Впрочем, нельзя недооценивать опасность и для среднего и малого бизнеса. Скажем, вынос перешедшим к конкуренту сотрудником списка клиентов небольшого дистрибьютора будет означать, как минимум, многократное снижение продаж, как максимум – банкротство организации.

Однозначно можно утверждать, что проблема защиты данных от инсайдеров – это проблема универсальная с точки зрения расположения, отраслевой принадлежности и размера бизнеса.

Несмотря на то, что утечки данных занимают первую строчку в рейтинге критических угроз бизнесу, на практике лишь 29% российских компаний используют специализированные системы защиты. По признанию экспертов, человек – самое слабое звено в системе безопасности, но и самое важное! На мой взгляд, здесь нет универсального рецепта. Известны организации, где насаждается обстановка тотальной слежки и есть торжество порядка. При этом они продолжают нормально функционировать и демонстрировать приемлемые показатели эффективности работы. В других организациях вполне логично делается упор на образование сотрудников, воспитание в них корпоративного духа, самосознания, чувства единения со стратегическими целями и задачами.

В этом вопросе не следует зацикливаться только на технологических особенностях систем защиты, многое зависит от моральных и этических норм в организации, корпоративного духа, кодекса этики. Эффективная защита возможна, только если в организации существует соответствующая корпоративная культура, предполагающая вовлечение руководителей в процесс обеспечения информационной безопасности. Ведь проблема эта сложна и многогранна, поэтому в отношении работы с персоналом следует делать больший упор на защиту данных от копирования на мобильные устройства, возможен контроль корпоративной почты части работников. Но такие действия никогда не должны быть публичными или анонсируемыми, так как ничего, кроме страха и напряжения, вызвать не могут. Однако, осуществляясь незаметно, такие действия способны уберечь ценную для компании информацию.

Литература:

1. *Крошилин С.В., Медведева Е.И. Информационные технологии и системы в экономике: учебное пособие. - М.: ИПКИР, 2008. - 485 с.*
2. *Крошилин С.В. Возможные угрозы безопасности экономических информационных систем и методы их устранения // Проблемы и методы управления экономической безопасностью регионов: Материалы межвузовской научной конференции профессорско-преподавательского состава. - Коломна: КГПИ, 2006. - С. 240-244.*
3. *Преображенский Е. Инсайдерские угрозы в России`09 // Управление персоналом. М.: Корпоративная Периодика. - 2009. - №7(209). - С. 6-10.*
4. www.it2b.ru – *Журнал «Технологии разведки для бизнеса»*