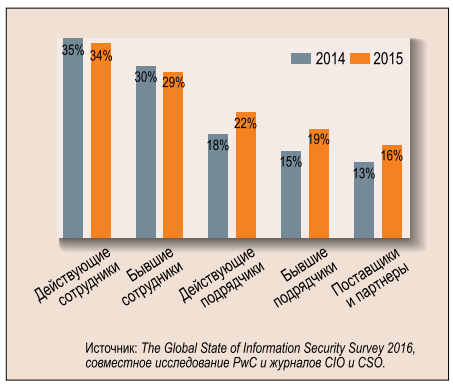
Человеческий фактор в информационной безопасности

ИГОРЬ ЛАПИНСКИЙ

Год за годом эксперты и аналитические компании, специализирующиеся в области информационной безопасности (ИБ), отмечают одну и ту же глобальную тенденцию: количество кибератак увеличивается, они становятся все изощреннее и приводят ко все более тяжелым последствиям. В этом смысле не стал исключением и прошлый год. Так, согласно данным исследования The Global State of Information Security Survey 2016, проведенного компанией PwC совместно с журналами CIO и CSO, "…в 2015 г. количество выявленных инцидентов в сфере информационной безопасности выросло на 38%". При этом, как отмечает Тим Клау, партнер, руководитель отдела анализа и контроля рисков PwC в России, в 2015-м в нашей стране существенно выросло не только фактическое количество атак, но и наносимый ими ущерб — по его словам, средний финансовый убыток от ИБ-инцидентов увеличился на 47%.

ОБЗОРЫ



Источник: The Global State of Information Security Survey 2016, совместное исследование PwC и журналов CIO и CSO.

Основные источники ИБ-инцидентов

Вместе с тем в ходе проведенного в рамках исследования опроса компаний (с охватом 127 стран мира) главными источниками ИБ-инцидентов были названы сотрудники компаний и организаций: настоящие (на это указали 34% опрошенных; годом ранее — 35%) и бывшие (29%; годом ранее — 30%).

Согласно другому недавнему исследованию, выполненному компанией Aite Group, действиями (злоумышленными или непреднамеренными) собственного персонала и связанных с ним внешних лиц обусловлено 44% ИБ-инцидентов в компаниях и организациях. При этом урон в таких случаях (имиджевый и финансовый) может быть даже больше, чем от внешних воздействий.

Сопоставимые цифры дает и статистика российской компании Solar Security, специализирующейся в сфере ИБ. "Ежеквартальные отчеты на базе данных Solar JSOC показывают, что больше половины инцидентов, зафиксированных в компаниях, связано с внутренними нарушителями и большую часть их составляют утечки информации, — делится Андрей Прозоров, руководитель экспертного направления в Solar Security. — Тут может быть как непреднамеренная утечка информации, допущенная по ошибке, так и умышленная, когда данные передаются конкурентам или копируются для последующего использования в личных целях".

Приведенные цифры не оставляют сомнений, что в настоящий момент человеческий фактор является одним из основных факторов риска с точки зрения информационной безопасности. "Как показывают последние зарубежные инциденты в нефтяной индустрии, человеческий фактор может свести на нет практически все усилия по защите инфраструктуры, — констатирует Сергей Халяпин, главный инженер российского представительства Citrix. — Чем больше у "посторонних" лиц возможностей для общения с сотрудниками компании, тем выше у нее риски утери информации или нарушения системы защиты".

Риски растут

Данные вышеупомянутого исследования PwC говорят о том, что по сравнению с предшествующим годом влияние человеческого фактора как источника ИБ-инцидентов в целом по миру чуть снизилось, однако разница оказывается на уровне статистической погрешности исследования. Так что говорить о каком-либо прогрессе здесь пока не приходится. И в этом нет ничего удивительного. Как утверждает, в частности, Дмитрий Шумилин, директор центра информационной безопасности компании RedSys, "человеческий фактор — то самое слабое звено, которое хуже всего поддается защите". Более того, там, где нельзя обойтись без человека, исключить негативное влияние человеческого фактора не представляется возможным в принципе. "До тех пор, пока не будет создан искусственный интеллект, принимающий решения за людей, человеческий фактор будет играть важнейшую роль в информационной защищенности компаний, — констатирует Рустем Турсунбаев, архитектор систем ИБ ГК "Компьюлинк". — Это утверждение применимо и ко всем другим сферам деятельности, поскольку автоматизированные системы являются всего лишь инструментом в руках людей".

Так что первое обязательное условие движения в сторону более высокой защищенности заключается в осознании серьезности вопроса. Рост общего числа ИБ-инцидентов и размера среднего ущерба от них уже говорит о том, что ИБ-риски российских компаний, в том числе обусловленные действиями персонала, повышаются. Кроме того, есть основания полагать (особенно в условиях российских экономических реалий), что значимость человеческого фактора в просматриваемой перспективе будет скорее расти, нежели снижаться. Отметим некоторые из таких оснований.

Современные технологические тренды в сфере ИТ, в частности распространение в корпоративной среде мобильных и облачных технологий, обуславливающих вынос бизнес-процессов за периметр корпоративной сети, усложняют контроль за используемыми в таких бизнес-процессах данными. Обратная сторона стремительного технического прогресса, от которого мы никуда не уйдем (да и не хотим уходить), заключается также в том, что уровень внедряемых технологий нередко оказывается заметно выше уровня готовности персонала компаний к их безопасному практическому использованию. При этом не стоит забывать, что технические системы и организационные меры, которые должны предотвратить или свести к минимуму возможный ущерб от опасных действий персонала, тоже планируют, создают и внедряют люди. Между тем более половины профессионалов в области кибербезопасности, опрошенных фирмой ISACA и давших интервью на RSA Conference, сообщили, что достаточной квалификацией для должности специалиста по кибербезопасности обладает менее четверти претендентов. Не слишком оптимистично в этом смысле выглядят и данные общероссийского исследования состояния ИБ, проведенного аналитическим центром компании SearchInform. Как утверждается в подготовленном по его результатам отчете, в Москве и Казани только 32 и 31% компаний соответственно доверяют вопросы безопасности профессионалам. Больше только в Екатеринбурге — 38%. А, например, в Симферополе, Самаре и Краснодаре отдел ИБ есть всего у 5% предприятий. В остальных случаях вопросами информационной безопасности занимаются непосредственно руководители и ИТ-специалисты, которые, как отмечается в отчете, входят в "категорию риска" по утечкам.

Другое основание, которое уж точно нельзя сбрасывать со счетов в нашей стране, — непростая общая экономическая ситуация, вынуждающая компании урезать ИТ- и ИБ-бюджеты, в том числе расходы на программы обучения персонала, сокращать штат сотрудников, причем иногда при одновременном увеличении нагрузки на тех, кто продолжает работать. "Динамика (влияния человеческого фактора на уровень ИБ. — *Прим. автора*) остается негативной, это связано, на наш взгляд, с общим экономическим состоянием России, — констатирует Андрей Прозоров. — Особенно остро данная тенденция проявляется там, где начинаются проблемы с выплатой зарплат, с сокращением персонала или премий. В такой ситуации некоторые сотрудники могут захотеть уйти из компании "в плюсе", и здесь не исключено, что они попытаются забрать ту информацию, которая, на их взгляд, может представлять определенную ценность".

В кризисные годы человеческий фактор становится драйвером роста нарушений в сфере ИБ, выражает общее мнение Сергей Вахонин, директор по решениям "Смарт Лайн Инк", подводя общую черту в этом обсуждении: "Ошибки или недоработки в системе безопасности, возникающие вследствие недостаточной компетентности либо чрезмерной загруженности ИБ-специалистов, обуславливают наличие уязвимостей, которые в сочетании с низкой квалификацией и слабой лояльностью персонала создают высочайший риск для кибербезопасности компаний".

Что опаснее: халатность или умысел?

Говоря о человеческом факторе, эксперты традиционно выделяют две формы его негативного проявления. Андрей Прозоров характеризует их следующим образом: "Первая — ошибки и халатность персонала, вторая — личная мотивация (т. е. преднамеренные действия. — *Прим. автора*), которая может сказываться на принимаемых решениях". Вопрос о том, какая форма опаснее (чревата более тяжелыми последствиями), кажется риторическим. Но, как выяснилось, только на первый взгляд. Поэтому есть смысл представить мнения наших экспертов на сей счет, а также предлагаемые ими меры защиты.

"По нашему опыту, количество непреднамеренных нарушений значительно превышает количество умышленных. Однако степень ущерба от умышленных действий несоизмеримо больше, — утверждает Дмитрий Шумилин. — Поэтому повышенный контроль со стороны ИБ-службы должен осуществляться за пользователями с привилегированными правами доступа и администраторами. Организация такого рода контроля требует применения дорогостоящих средств защиты и дополнительных организационных мер".

В противоположном ключе высказывается Сергей Халяпин: "Я считаю, что в целом непреднамеренные действия наносят компаниям больший ущерб, чем целенаправленная умышленная деятельность. Если умышленную деятельность можно и нужно выявлять различными методами с участием ИБ- и кадровой службы, основываясь при этом на поведенческом анализе, то непреднамеренные действия трудно поддаются контролю, поскольку непредсказуемы. Кто-то потерял важные документы на флэшке; на рабочем месте в присутствии посетителей открыт документ, представляющий коммерческую тайну; сотрудник опубликовал в соцсетях информацию ограниченного доступа — подобные ситуации плохо предсказуемы, и здесь важен не столько контроль, сколько обучение и внедрение политик информационной безопасности. Причём сотрудники должны не просто подписать документ об ознакомлении с политиками ИБ, а внимательно его изучить. Кроме того, должен быть налажен контроль за тем, как они понимают и соблюдают политики".

В целом позицию г-на Халяпина разделяет и Андрей Янкин, руководитель отдела консалтинга Центра информационной безопасности компании "Инфосистемы Джет": "Безопасность традиционно видит потенциального врага в каждом сотруднике, но большинство нарушений совершается по незнанию или разгильдяйству, а не из злого умысла. Конечно, урон от умышленных атак может быть очень большим, но статистически эти потери с лихвой перекрываются уроном от непреднамеренных нарушений".

Наши эксперты

ИВАН БОЙЦОВ, *менеджер по продукту, "Код безопасности"*

СЕРГЕЙ ВАХОНИН, *директор по решениям, "Смарт Лайн Инк"*

АНДРЕЙ ПРОЗОРОВ, *руководитель экспертного направления, Solar Security*

РУСТЕМ ТУРСУНБАЕВ, *архитектор систем ИБ, ГК "Компьюлинк"*

СЕРГЕЙ ХАЛЯПИН, *главный инженер, российское представительство Citrix*

ДМИТРИЙ ШУМИЛИН, *директор центра информационной безопасности, RedSys*

АНДРЕЙ ЯНКИН, *руководитель отдела консалтинга Центра информационной безопасности, "Инфосистемы Джет"*

Более нейтрального мнения придерживается Иван Бойцов, менеджер по продукту компании "Код безопасности": "Если в организации нет полноценной системы защиты, то любой сотрудник может нанести значительный ущерб — украсть базу клиентов, вывести из строя технические средства, вызвать вирусную эпидемию и т. д. Если же технические меры по защите информации реализованы в полном объеме, то наибольший ущерб могут принести две категории сотрудников — специалисты ИТ-департамента и сотрудники ИБ-службы. Организовать контроль за ИТ-отделом можно при помощи дополнительных технических мер — на рынке существует множество продуктов по контролю за привилегированными пользователями. Контролировать ИБ-службу обязан начальник по информационной безопасности, и тут скорее должны преобладать организационные меры и тщательная проверка потенциального сотрудника до приема его на работу".

Таким образом, мнения экспертов заметно разнятся, и в каком-то смысле объединяющей (или примиряющей) эти точки зрения можно, видимо, считать позицию Сергея Вахонина: "По большому счету важно лишь то, что компания понесла ущерб, а служба ИБ не предусмотрела такой сценарий утечки и не приложила усилий для его предотвращения организационными и/или техническими способами и средствами. Служба ИБ должна учитывать все модели угроз, прорабатывать различные сценарии, плотно работать с сотрудниками и руководителями подразделений, чтобы минимизировать любые группы рисков, при этом минимизация непреднамеренных и случайных действий пользователей является более простой задачей, а следовательно, её нужно решить в первую очередь. Тщательная проработка и исключение случайных сценариев утечки корпоративных данных, как правило, снижает и риски преднамеренных утечек, осуществляемых в основном через те же самые каналы передачи данных. Чем ниже уровень защищенности, чем хуже организация контроля корпоративных данных и каналов их распространения — и тем проще действовать злоумышленнику. Нет никакого смысла изобретать сложную тактику хищения, например, данных, составляющих коммерческую тайну, если можно воспользоваться простым способом".

Кто в зоне риска

Согласно данным вышеупомянутого исследования SearchInform, в ходе которого было опрошено более 1700 специалистов из 25 городов России и стран СНГ, в 2015 г. с утечками конфиденциальной информации столкнулись более половины опрошенных компаний (52%). Столь значительные цифры говорят о том, что вероятность избежать подобных инцидентов невысока фактически для любой организации.

"Традиционно в отечественных компаниях очень формально относятся к соблюдению политик и регламентов, особенно в части ИБ, — сетует Андрей Янкин. — По умолчанию все правила игнорируются, причем иногда даже самими безопасниками. Это приводит к тому, что система обеспечения ИБ, в том числе самая продуманная, в действительности не работает, открывая пути и для внешних атак, и для внутреннего мошенничества".

Прямое следствие подобной ситуации — широкое использование методов социальной инженерии при проведении атак, как в случае организованной 15 марта целевой атаки с рассылкой вредоносных писем на электронные адреса сотрудников десятков российских банков, о чем сообщила "Лаборатория Касперского".

"Атаки с использованием методов социальной инженерии традиционно чрезвычайно успешны, — подтверждает Андрей Янкин. — Пусть сотрудники обучены и крайне бдительны, кто-нибудь непременно поддастся. И всё: мостик в сеть компании проброшен. Злоумышленник может развивать атаку, не преодолевая внешний защищенный периметр. Причем атаковать проще самого рядового сотрудника, который почти ни за что не отвечает и которого учить и защищать будут последним. Раньше чаще всего атаковали банки, сейчас же злоумышленники атакуют всех подряд. В небольшой компании об ИБ зачастую и не слышали, а провести поддельную проводку на пару миллионов можно и тут".

Вместе с тем конфиденциальная информация может утекать и самыми неожиданными способами в результате непреднамеренных действий. Любопытный в этом смысле пример из практики партнеров приводит Рустем Турсунбаев: "В процессе работы сотрудникам приходится интенсивно переписываться с некой компанией-производителем. Иногда от этого вендора приходят письма, содержащие внутреннюю переписку по развитию их нового проекта. И только позже выясняется, что фамилия одного из сотрудников компании-партнёра совпадает с фамилией одного из разработчиков вендора. Вот таким образом мы иногда узнаем, как развивается продукт, задолго до его официального релиза". (Как тут не обратить внимание на данные исследования PwC, согласно которым следующим по значимости источником ИБ-инцидентов оказываются настоящие и бывшие подрядчики, поставщики и партнеры!)

Влияние человеческого фактора является сильным для предприятий всех отраслей, констатирует Андрей Прозоров. И все же, по его мнению, в государственных учреждениях и банках на данный момент оно наибольшее: "Это связано прежде всего с тем, что в госучреждениях работает много сотрудников, чей уровень компьютерной грамотности не очень высок, а в банковской сфере традиционно фиксируется большое количество мошеннических действий и внутреннего фрода".

И хотя в последние годы, как отмечает Андрей Янкин, у компаний появляются обученные сотрудники, которые передают информацию о подозрительной активности в службу ИБ, что раньше было большой редкостью, это скорее первые ласточки: "В целом картина весьма печальная — сотрудники массово становятся жертвами самых примитивных атак вроде письма от неизвестного отправителя с фразой «Это наша новая система удаленного доступа к почте. Проверьте ее, пожалуйста»".

Стандарты или здравый смысл?

В том, что касается обеспечения информационной защиты предприятия, важную роль играют требования регулирующих органов и отраслевые стандарты, несоответствие которым может не только обернуться штрафными санкциями, но и сам бизнес поставить под угрозу. Однако возникает вопрос, означает ли соответствие нормативным требованиям в том числе и то, что на предприятии приняты необходимые меры для снижения рисков, обусловленных влиянием человеческого фактора. Ведь, как справедливо утверждает, например, Сергей Халяпин, "…отраслевые стандарты и требования различных регулирующих органов позволяют создать основу для корпоративных правил и политик безопасности, поскольку, скорее всего, в этих стандартах и требованиях будут перечислены основные угрозы и риски, а также возможные механизмы их предотвращения".

Но одно дело — как должно быть, другое — как есть в действительности. "К требованиям регуляторов отношение формальное, — отмечает Андрей Янкин. — Частично это "заслуга" многих российских стандартов, которые безнадёжно устарели и не учитывают потребности бизнеса". Вместе с тем, по его словам, большинство стандартов в буквальном смысле "написаны кровью", и стоило бы внимательнее относиться к их требованиям, воспринимая их как лучшие практики и осмысленно перекладывая их нормы на свою организацию.

Пять признаков того, что ваша компания находится в группе риска

Оценки разных аналитических компаний и экспертов в области ИБ свидетельствуют: около половины инцидентов в сфере защиты данных связано с деятельностью инсайдеров. Аналитический центр Falcongaze подготовил список признаков того, что компании стоит озаботиться вопросом защиты от утечек информации. Приведём его.

1. Отсутствие корпоративной политики безопасности.
2. Высокая ротация кадров и частые сокращения.
3. Неконтролируемое использование сотрудниками мессенджеров, электронной почты, социальных сетей.
4. Наличие сотрудников, много времени проводящих в деловых поездках и командировках.
5. Неконтролируемый документооборот, вследствие чего доступ к конфиденциальным сведениям может получить кто угодно.

Есть и другие признаки, показывающие, что защите от утечек информации уделено недостаточно внимания, но, как утверждают в Falcongaze, если хотя бы один из перечисленных пунктов справедлив для вашей компании, она однозначно попадает в группу риска.

"Особое место здесь занимает группа стандартов ISO 27000. Немало здравых идей содержится и в стандартах ЦБ, PCI DSS, в свежей нормативной документации ФСТЭК России. Их использование поможет выстроить гораздо более устойчивую к воздействию человеческого фактора систему обеспечения ИБ", — считает эксперт.

В схожем ключе комментирует ситуацию и Иван Бойцов: "Если говорить о технической защите информации, то нормативные документы дают четкое понимание того, какие средства защиты и где должны устанавливаться. Но по организационной части и нормативные требования, и отраслевые стандарты задают только общие правила игры. Формального выполнения организационных мер достаточно, чтобы не получить предписаний от регуляторов. Но их недостаточно для повышения уровня защищенности. Нормативные требования лишь подсказывают, какие меры нужно принять, но не регламентируют необходимый уровень их качества. Скажем, при защите персональных данных требуется регламентировать работу с конфиденциальной информацией, подготовить инструкции и ознакомить с ними сотрудников. По факту — из Интернета загружаются шаблоны документов, подставляется название своей организации, документы печатаются и убираются в стол. Организационные меры формально выполнены, все документы есть, но сотрудники не знают об их существовании и практической пользы от этих действий нет. Нормативную базу нужно прорабатывать на детализацию не только технических, но и организационных мер, требовать обязательного обучения персонала, проверять знание инструкций при проверках и т. д.".

Некую черту под обсуждением данной темы подводит Андрей Прозоров, который, не отрицая важности отраслевых стандартов и нормативных требований для обеспечения информационной безопасности, не готов назвать их роль ключевой: "Зачастую стандарты — это лучшие практики, и есть смысл ориентироваться на них. Но при построении системы информационной безопасности в компании идти всегда нужно от здравого смысла. Если вы будете выстраивать систему защиты, принимая во внимание бизнес-риски компании и ценность той информации, которая обрабатывается, подходя к этому вопросу системно, — это будет наилучший подход, а стандарты и требования могут быть подспорьем".

Обучение персонала — на что обратить внимание

Наряду с техническими мерами по ограничению возможностей утечки данных в результате тех или иных действий персонала важной составляющей в обеспечении защиты корпоративной информации является обучение сотрудников правилам безопасной работы. Хотя это не самый дорогой элемент в общей системе безопасности, соответствующие программы, как отмечает Андрей Янкин, "пока имеют недостаточное распространение".

Впрочем, и там, где такие программы внедрены, их качество нередко оставляет желать лучшего. "Эффективность программ обучения в первую очередь зависит от того, как поставлен этот процесс в компании, — констатирует Иван Бойцов. — Если обучение выполняется как формальность, то никакого эффекта, кроме потери времени, не будет. Но если оно проводится на регулярной основе, если информация дается четко и понятно, выбираются актуальные темы для освещения и организуются практические занятия, то положительный эффект будет огромным".

Многие компании, отмечает Андрей Янкин, уже сделали вывод о том, что классический подход с заучиванием регламентов — не самое лучшее решение. "Сейчас компании заказывают интерактивные инструменты обучения, похожие на игры. Используются привлекающие внимание плакаты, на рабочие станции в качестве заставки устанавливаются правила ИБ в виде запоминающихся картинок. В результате эффективность обучения многократно возрастает, — утверждает эксперт. — Но не стоит забывать и о контрольных процедурах. Регулярная проверка знаний сотрудников обязательна. Если ее не проводить, эффективность обучения падает на порядок".

В первую очередь правильно выстроенное обучение персонала может способствовать тому, что снизится вероятность непреднамеренного нарушения конфиденциальности и целостности информации, а также успешного проведения атак методами социальной инженерии, поясняет Иван Бойцов. При этом он указывает и на другой важный аспект, который следует иметь в виду при составлении обучающей программы: "Если упор сделать не только на обеспечение безопасности, но и на правовые нормы, то можно достичь снижения умышленных утечек. Рассказ об ответственности за нарушение режима конфиденциальности информации, процессов обработки персональных данных и т. п. позволяет уменьшить вероятность появления инсайдеров. Известно, что многие потенциальные нарушители идут на преступление, полагая, что никакой ответственности за это они не понесут".

Мы не случайно говорим лишь о снижении вероятности инцидентов. Ссылаясь на статистику проведенных тестов на проникновение, Дмитрий Шумилин констатирует, что не бывает компаний, где не нашлось бы чересчур беспечных и любознательных сотрудников. "Поэтому возможно только последовательное уменьшение этой уязвимости через структурированный процесс инструктажа сотрудника на всех этапах его пребывания в компании", — уверен эксперт.