Размышления о судьбе «безопасника»

МИХАИЛ САВЕЛЬЕВ

Директор Учебного центра «Информзащита»

К сожалению, практически любому ИБ-специалисту свойственно преувеличивать его вклад в жизнь предприятия. Да и как может быть иначе, если на многочисленных отраслевых конференциях без конца говорится о неоспоримой значимости ИБ-деятельности для работы и самого существования компаний. Попробуем разобраться в том, как должна измениться роль «безопасника» в новых условиях.

Эффект шестка

Когда рынок поступательно растет из года в год, когда те, кого называют «бизнес», относительно спокойны, и никто не спорит с необходимостью найма новых сотрудников для развития компании, большинство ее специалистов преисполнены чувства собственной значимости. Но когда возникает неблагоприятная экономическая ситуация, и тот самый бизнес начинает разбираться, кто и чем занят, считать деньги и определять экономическую эффективность работы подразделений, многим сотрудникам становится несладко.

Преувеличение собственной значимости зачастую обусловлено ограниченностью взглядов на бизнес с высоты колокольни, на которой сидит тот или иной специалист по информационной безопасности. Сотрудникам, деятельность которых связана с обеспечением ИБ, свойственно давать завышенную оценку тому, что обрабатывается в информационных сетях или имеет отношение к информационным технологиям.

Да, мы давно «подсели» на постоянную доступность всех и всем по телефону, электронной почте или конференц-связи, но в большинстве случаев эти сервисы вовсе не обязательны для бизнес-процессов. Например, в крупных компаниях существуют нормативы ответов на сообщения электронной почты в течение не более чем трех дней. Но насколько необходимы в таких случаях круглосуточная доступность почты и куча разнородных сложных технологий защиты, повышения мобильности, доступности и т. п.?

ИБ-специалисты могут бесконечно ломать копья по поводу необходимости приведения сетей и информационных систем в соответствие с требованиями регуляторов, в том числе закона о персональных данных. Однако размеры соответствующих штрафов несопоставимы с потенциальными последствиями приостановки бизнеса из-за невыполнения каких-либо лицензионных требований по основному виду деятельности.

Я вполне принимаю гневные выпады типа «каждый занимается своим делом, и то, что мы управляем малыми рисками, не означает бесполезности». Но хочу подчеркнуть, что стоимость решаемых нами проблем несопоставима, например, с уроном от воровства вагона металлопроката. Кроме того, порой ИБ-специалисты, непомерно сужая зону своей ответственности, упускают из вида даже смежные вопросы безопасности. Так, борцы с утечками корпоративных секретов готовы внедрять множество инструментов контроля лишь над одним каналом — передачи информации по сети. Борцы со зловредным ПО, которое проникает в информационную систему по сети, предлагают средства контроля исключительно над этой областью, начисто игнорируя не только остальные каналы появления «зловредов» внутри контролируемого периметра, но и все прочие способы воздействия на организацию (такие

как использование незаконных методов получения голосовой информации, разведопросы сотрудников, засылка или вербовка агентов и т. п.).

Можно упомянуть и о задаче обеспечения непрерывности бизнеса. Грустно осознавать, что «инфобезопасники» зачастую подразумевают под нею лишь мониторинг и план восстановления ключевых узлов все той же информационной сети компании. А гораздо более важные моменты (скажем, отказ от своих обязательств одного из поставщиков комплектующих, используемых предприятием) не рассматриваются, ибо это — «не наши задачи».

Опять-таки, да, я согласен с тем, что хоть какой-то контроль лучше, чем вообще ничего, но... С таким подходом не спасут никакие лекции о том, как правильно «продавать» ИБ руководству. И не стоит получать степень MBA, чтобы рассказывать бизнесу про межсетевые экраны на CEO-суржике. Далеко не с языком взаимодействия или с аргументами о необходимости внедрения связана пропасть непонимания между ИБ и бизнесом.

Треугольник мошенничества

Оптимизация «по живому» или комплексный подход?

Дай бог, чтобы пессимистичные прогнозы развития рыночной ситуации, связанные с санкциями и иными внешнеполитическими реалиями, не воплотились в жизнь. Но так или иначе дыхание этой ситуации почувствуют многие. Руководство компаний будет пристально наблюдать за деятельностью каждого сотрудника и нещадно оптимизировать «по живому». Скорее всего, для ИБ это означает сокращение числа соответствующих подразделений, серьезное урезание бюджетов с переходом в режим только насущно необходимых затрат и приостановку развития служб безопасности.

И тут самое время вспомнить о том, что обеспечение безопасности — комплексная дисциплина, роль которой в условиях кризиса будет только расти. А значит, у «безопасников» есть шанс доказать, что они не зря просиживают штаны и еще могут принести пользу своим работодателям.

С чем бороться при комплексном подходе к обеспечению безопасности? На результаты работы компании влияют как внутренние, так и внешние факторы. Проблем, приходящих извне, хватает: на любое предприятие воздействуют, и зачастую неблагоприятно, конкуренты, поставщики и подрядчики, охотники за тем или иным бизнесом — рейдеры, коррумпированные чиновники, даже клиенты. И чем тяжелее период, тем агрессивнее и жестче могут быть методы нечистоплотной конкурентной борьбы.

Один из распространенных видов внутренних противоправных действий — это воровство. Воруют товары, секреты, деньги, причем в тяжелые времена воруют больше. Не надо забывать и про искажение сотрудниками отчетности, сокрытие каких-либо фактов, откаты, ложь, некомпетентность и многие другие действия и факторы, оказывающие негативное воздействие на предприятие изнутри.

Для объяснения того, почему человек решается причинить вред своей компании, придумана хорошая модель — «треугольник мошенничества». Вершины этого треугольника таковы: возможность совершить и некоторое время скрывать свой

поступок, давление обстоятельств, способность оправдать свои действия перед самим собой.

Во время кризиса обстоятельства давят все сильнее. К «стандартным» причинам противоправных действий, таким как тяжелые болезни родственников, безответственно взятые кредиты и т. п., добавляются новые: родственники и друзья теряют работу, работодатели сокращают премии и бонусы, а порой и снижают зарплаты, банки индексируют выплаты по кредитам в соответствии с ростом курса валют.

Ну а оправдывать противоправные действия перед самим собой тем легче, чем сложнее проблемы, вызвавшие эти действия. Оправдание может иметь эмоциональный характер: например, это желание насолить несправедливому начальнику или даже «наказать всю систему». Иногда характер оправдания становится классовым: «руководство с жиру бесится, а мы страдаем». А порой, особенно в случаях хищения денежных средств, оправданием служит возможность выбраться из своих финансовых затруднений и, бывает и такое, со временем возместить неправедно полученные деньги.

Специалист по информационной безопасности может влиять на сотрудников компании с целью предотвращения инцидентов, внушать им, что все неправомерные действия с использованием средств вычислительной техники обязательно будут выявлены и не останутся безнаказанными. К слову, информирование сотрудников на протяжении всей их трудовой деятельности о таких возможностях службы информационной безопасности, формирование у них стойкой демотивации к противоправным действиям — это одна из задач, подразумевающих взаимодействие кадровых подразделений и служб безопасности.

Время новых возможностей

На нынешнем неблагополучном экономическом этапе я вижу единственный способ сохранения статусов и рабочих мест специалистов по ИБ: нужно предлагать себя работодателям как мощный инструмент защиты того самого бизнеса, которому эти специалисты прежде хотели «продавать» информационную безопасность.

Нет, я вовсе не предлагаю «безопасникам» переквалифицироваться в лихих оперативников со знанием информационных технологий — это удел немногих людей с определенным складом характера. Да и нет смысла выбрасывать на свалку накопленные ранее опыт и знания. Но научиться воспринимать задачи обеспечения безопасности компании «со стороны» (так, как ее видят другие подразделения) — дело обязательное. Это умение позволит переосмыслить и точнее расставить текущие приоритеты, понять задачи смежных подразделений и добиться от них взаимодействия.

В обеспечение комплексной безопасности должны быть вовлечены подразделения корпоративной защиты и оценки рисков, кадровые отделы, специалисты по ИБ и непрерывности бизнеса, юристы. А главное, это вовлечение должно быть не формальным, а вполне реальным и плодотворным.

Основными партнерами «безопасников» становятся кадровики. В условиях возможного сокращения штатов всех ИТ-подразделений специалистам по ИБ необходимо добиваться от сотрудников знания и неукоснительного соблюдения инструкций и регламентов, повышать уровень их осведомленности в вопросах безопасного использования информационных систем. Эти задачи хорошо интегрируются с программами повышения лояльности, обучения сотрудников и т. п., которые очень любят сотрудники кадровых служб. Обыгрывание в таких программах способов противодействия, например, методам социальной инженерии помогает донести до сотрудников отношение компании к обеспечению собственной безопасности без скучных непонятных объяснений, больше похожих на плохую агитацию.

К сожалению, проблемы взаимодействия всегда были и будут. Так, кадровые службы не контролируют уровень лояльности сотрудников, а их стремление быстро закрывать вакансии без взаимодействия со службами безопасности и экономить фонд заработной платы приводит к тому, что достаточно важные должности (такие как системный администратор) занимают, в лучшем случае, люди с низкой квалификацией (которые сами могут становиться источниками угроз для компании), а в худшем случае — корпоративные шпионы. В свою очередь, «безопасники» не делятся информацией и не обучают остальных. Основная причина этого — недооценка важности задач, связанных с обеспечением безопасности компании.

Пора меняться! Кризис — тяжелое время, но это и время новых возможностей. А раз так, надо смело смотреть вперед и строить планы выхода из кризиса с новыми опытом и знаниями.

Преувеличение собственной значимости зачастую обусловлено ограниченностью взглядов на бизнес с высоты колокольни, на которой сидит тот или иной специалист по информационной безопасности.