Баланс безопасности.

Как ИБ и бизнесу понять друг друга?

DEPOSITPHOTOS.COM/ELNUR_

Как известно, проблема отсутствия взаимопонимания – одна из самых сложных и животрепещущих проблем нашего общества. А что, если не достигнуто взаимопонимание между представителями службы информационной безопасности и бизнесом? Безусловно страдает бизнес в целом – он становится уязвимым, достижение его стратегических целей находится под угрозой. Давайте разберемся, насколько серьезной представляется данная проблема, рассмотрим ее со стороны бизнеса и безопасности, и постараемся найти необходимый баланс. Итак, бизнес vs ИБ – ищем точки соприкосновения.

Предположим, что в компании есть некий C-level менеджер, который в том числе курирует службу информационной безопасности, контролирует деятельность подразделения и выделяет бюджет на его нужды. Задумываясь об эффективности расходования ресурсов, он пристально смотрит на подотчетное ему направление и понимает, что… ничего не понимает. В то же время, с другой стороны баррикад, работает руководитель службы ИБ. Он глубоко погружен в вопросы технологий, сценарии атак, актуальные методологии и даже задумывается о минимизации ресурсов. Однако их встреча зачастую имеет негативный исход – эффективность работы ИБ-подразделения признается недостаточно высокой и бюджеты урезаются. Возникает конфликт.

Чего же бизнес хочет от ИБ?

Эксперты ИБ уверяют – проблема недостаточного взаимопонимания между ИБ и бизнесом не надуманная и действительно существует. И сразу конкретизируют, что вопрос заключается не только в непонимании бизнесом, на что расходуется бюджет. Это скорее уже следствие глубинных проблем. Ключевой момент заключается в том, что бизнес

просто не любит делать те телодвижения, смысла которых не понимает. А если у бизнеса нет понимания, как конкретное действие влияет на его конечный продукт или определенные ключевые показатели работы компании, то и выполнять это действие он не видит смысла. Ведь каждое неоправданное действие только плодит энтропию. И именно в этом заключается первопричина конфликта.

Итак, возникает вопрос – как бизнесу разглядеть реальные исчисляемые выгоды от функции информационной безопасности? И в то же время – как подразделению по информационной безопасности научиться наглядно демонстрировать эти выгоды? Постараемся ответить.

Недостаток менеджериальной зрелости руководителей ИБ

Любая организация выстраивает для себя иерархию целей, стремится сформулировать показатели эффективности. Затем она информирует об этих целях и показателях свои подразделения, включает инструменты планирования и контроля. Таким образом бизнес взаимодействует с функцией продаж, с функцией производства. Однако функция ИБ стоит в стороне. Бизнес так к функции ИБ не относится. Возможно, проблема заключается в том, что для постановки глубоко проработанных целей для ИБ нужно обладать пониманием технологий и методологии. Представители бизнеса такими знаниями не обладают. С другой стороны, у руководителей из сферы ИБ, как правило, пока еще недостаточно высокий уровень менеджериальной зрелости. Ведь ИБ, как отдельная функция в организации – достаточно молодая. Еще 15 лет назад никто не требовал от ИБ «бизнес-взгляда». И сегодня процесс обучения специалистов ИБ предполагает преподавание специальных технических предметов, организационных методологий, комплаенс-дисциплин. Из ВУЗов выходят отлично подготовленные в техническом плане специалисты, но, увы, недостаточно сильные менеджеры. Но сейчас приходит то время, когда бизнес начинает требовать от информационной безопасности «бизнес-взгляда» на то, что она делает и ожидает от информационной безопасности большего погружения в бизнес-модель, проактивной позиции и создания нового качества или нового свойства для бизнес-модели.

Эффективность ИБ = Достижение бизнес-целей?

В свою очередь бизнес так же должен уверенно и целенаправленно идти навстречу ИБ. Ведь сегодня мы зачастую сталкиваемся с ситуацией, когда в головах у бизнеса функция информационной безопасности вынесена за периметр бизнес-процессов, связанных с достижением бизнес-целей. Однако неправильно будет утверждать, что люди бизнеса никак не пытаются достичь взаимопонимания с ИБ. Многие из них следят за трендами технологического развития, за общей картой рисков, постоянно анализируют, каким образом его бизнес трансформируется, какие новые свойства ему для этого бизнеса нужны и так далее.

Такая ситуация характерна для крупного бизнеса. Но что же средние и малые компании? Думают ли они о том, как достижения информационной безопасности помогают достижению стратегических целей бизнеса? Воспринимают ли они информационную безопасность как нечто большее, чем установка антивирусного ПО? Ответ скорее будет отрицательным. Однако тотальный переход бизнеса «на цифру» не позволит ситуации оставаться прежней. И хочется верить, что вслед за революционной трансформацией ИТ функции, которая за последние 5–8 лет стала фундаментом цифрового бизнеса, и функция ИБ превратится в неотъемлемый модуль цифрового продукта. При этом сложно ожидать от компаний СМБ-сегмента высокого уровня зрелости бизнес-модели с хорошо сформировавшейся функцией информационной безопасности, но думать и погружаться в эту задачу сейчас просто необходимо.

Бизнес + ИБ, практические шаги навстречу

И все же, что делать, какие практические шаги предпринять, чтобы подружить бизнес и безопасность? Для ИБ, как и для любой функции, важно понимать, как она влияет на уровень показателей, как делает свою компанию лучше, свой продукт более продаваемым, а клиентов более счастливыми и так далее. Есть множество успешных кейсов, когда продукт наделялся неким свойством, обеспечивающим безопасность пользователям. К примеру, мессенджер Telegram получил большое число новых пользователей, потому что они восприняли его в первую очередь как безопасный продукт. Также существует множество примеров того, как функция ИБ удачно меняла внутренние системы и процессы – они становились быстрее, удобнее, прозрачнее, снимались ограничения, появлялись новые возможности для новых рынков. Или, скажем, отличный кейс – получение сертификата PCI DSS, который открывает для бизнеса возможность работы в определенном сегменте, а значит, влияет на позитивное изменение бизнес-модели, на рост бизнес-показателей и так далее.

Резюмируя, безопасность должна поддерживать те или иные показатели конкретного бизнеса, быть неким дополнительным модулятором, который влияет на остальные свойства. Уйти от постулата «безопасность должна быть безопасной» и действовать в парадигме «можешь сделать что-то быстрее – сделай; можешь что-то сделать менее отказоустойчивым – сделай; можешь снять какой-то серьезный риск, вероятность наступления которого очень велика – сделай». Это понятные хорошие конкретные шаги, которые стоит предпринять. ●