Безопасность как преимущество

Бюджеты, выделяемые компаниями на обеспечение информационной безопасности, постепенно растут. Однако защищенность заметно не меняется — об этом говорит постоянно растущее число инцидентов. В данном случае мы видим яркий пример неоптимального расходования выделяемых на безопасность средств.

Одной из основных причин проблем становится неэффективный диалог между службами информационной безопасности и руководством компаний. Традиционно он строится на запугивании — иначе бизнес не желает вкладывать в безопасность хоть какие-то средства. Главное негативное последствие такого подхода — восприятие бизнесом службы безопасности исключительно как центра затрат. При этом остается открытым вопрос адекватности затрат достигаемым эффектам, а также соответствия принимаемых решений приоритетам бизнеса.

Сложности перевода

«Бизнес и службы информационной безопасности зачастую говорят на разных языках, и это объяснимо: у них разные ценностные ориентиры и различные задачи», — считает Джабраил Матиев, руководитель отдела информационной безопасности компании IBS Platformix. Если главная задача департамента безопасности заключается в защите критичной для бизнеса информации, то для бизнеса главный приоритет — зарабатывание денег, и любые ограничения мешают этому процессу.

«Хотя очевидно, что само возникновение конфликта идет на пользу. В процессе диалога, поиска компромисса и возникает правильное решение», — уверен Матиев. Пожалуй, наиболее верным можно считать подход, при котором бизнес вкладывается в безопасность, защищая себя от рисков. В этом случае затраты можно рассматривать как страховку. Однако никто не будет оплачивать страховку без понимания существующих рисков. Способность общаться с руководством компаний на языке бизнес-рисков является ключом к построению эффективного диалога между бизнесом и департаментом информационной безопасности (ИБ).

Следующий навык, важный для руководителей служб ИБ, — умение предлагать варианты действий. Если предлагается единственный оптимальный, с точки зрения его авторов, путь решения задачи, это сильно нервирует бизнес. Никто не любит, когда его просто ставят перед фактом и не дают возможности выбора. Предложенные варианты должны подразумевать несколько подходов к решению задачи, обеспечивающих разный класс безопасности и имеющих разную стоимость. Это позволяет бизнесу варьировать подходы, понимая свои риски и приобретаемые выгоды.

С этой точки зрения позитивным фактором становится изменение «портрета» типичного руководителя службы ИБ. Если несколько лет назад офицеров безопасности набирали только с определенным, профильным образованием, то сейчас ситуация меняется: сегодня мы видим большое число специалистов, перешедших в область безопасности из ИТ.

«Компаниям нужны люди, умеющие создавать решения ИБ, влияющие на конкурентоспособность. Образование и опыт в ИТ тут имеют решающее значение», — уверен Александр Парамонов, заместитель генерального директора, директор по развитию IBS Platformix. Процессы взаимодействия ИТ с бизнесом немного другие, больше способствующие взаимопониманию: ИТ-руководитель в процессе работы должен выявить бизнес-потребности и транслировать их в технический язык, инициировав внедрение тех или иных систем. Руководитель ИБ озвучивает бизнесу возникающие риски, предлагая варианты возможной защиты. На сегодняшний день в этом заключается принципиальное отличие: деятельность ИТ идет от потребностей бизнеса, а ИБ, наоборот, своими предложениями часто ограничивает эти потребности.

Именно поэтому часто на почве безопасности решений возникают конфликты: служба ИБ выдвигает требования к реализуемым системам, а ИТ-департамент заявляет, что это не позволит решить задачи бизнеса.

Джабраил Матиев, руководитель отдела информационной безопасности компании IBS Platformix

Бизнес умеет считать

Принимать на веру бездоказательные рекомендации служб информационной безопасности никто не желает. Бизнес требует объяснить возникающие риски, причем аргументировать свои взгляды с финансовой точки зрения. Это далеко не всегда получается: топ-менеджмент склонен упрощать проблему, не понимая технических нюансов.

В результате службе ИБ приходится «продавать» риск бизнесу. На самом деле постановка вопроса должна быть несколько другой. Главная задача, как уже говорилось ранее, не продавливать внедрение средств безопасности, а предлагать пути решения проблем. При этом важно, чтобы руководитель ИБ мог донести до бизнеса вероятную стоимость рисков и, возможно, предоставить методику их оценки, так как зачастую бизнес не знает, каковы потенциальные потери и чем проблема в итоге может обернуться.

Взаимодействие с бизнесом имеет хорошие перспективы только в том случае, если регулярно выстраивать грамотный двухсторонний диалог, постоянно искать пути взаимодействия. Таким образом, в отличие от тактики запугивания обеспечивается постоянный информационный поток,

имеющий весьма высокую ценность с точки зрения бизнеса. Руководство привыкает к ежемесячным отчетам и ясно понимает свое отношение к озвученным рискам, видит варианты действий, свои приоритеты, четко осознает, с какими рисками оно готово мириться, а с какими — нет, так как они критичны для бизнеса.

«Принцип диалога несложен: озвучиваются риски и их вероятность, определяется величина возможного ущерба. Дальше идет речь о снижении вероятности наступления риска», — рекомендует Матиев. В этом случае ИБ становится если не источником доходов, то источником сокращения будущих расходов.

В данном случае обоснование необходимых инвестиций происходит по аналогии с построением плана обеспечения непрерывности бизнеса, где основными показателями являются количество потерянных данных и время восстановления. При этом простой систем измеряется не в секундах, а в реальных деньгах: бизнес сам должен определить, потеря каких средств для него критична, и уже на основании этого ИТ должно прорабатывать технические решения.

Разумеется, чем более высоких показателей необходимо достичь, тем большие требуются средства. Увидев стоимость работ, бизнес либо соглашается на них, либо начинает поиск компромиссных решений.

В безопасности происходит то же самое. Если грамотный ИБ-руководитель четко обосновывает стоимость рисков, пути решения проблем и во что это обойдется, проводится аналогичный выбор: бизнес решает, что для него критично, а что — нет. На основании этого определяется уровень инвестиций.

Не затратами едиными

«Не стоит уподоблять ИБ бронежилету для бизнеса: ее действие в не меньшей степени направлено вовнутрь, не только вовне», — подчеркивает Парамонов. Если защищается только периметр — это самый плохой и неэффективный пример работы службы ИБ. Она должна не просто нести в компанию информацию об изменениях в законах и появлении новых угроз — необходим анализ наиболее уязвимых мест внутри предприятия, вероятностей реализации тех или иных рисков и их последствий. Нужно не повышать защиту информационных систем как таковых, а проводить анализ обеспечения защиты конкретных бизнес-процессов внутри предприятия.

Если деятельность службы ИБ коснется не только информационных систем, но и бизнес-процессов, это подразделение действительно может стать ключевым звеном в организации. Такая работа гораздо важнее для предприятия, нежели попытки защитить какую-либо систему.

Если сеть предприятия взломали и об атаке стало известно, это еще полбеды. В таком случае можно предпринять какие-то действия по защите интересов компании и нивелировать последствия. Гораздо хуже, если факт взлома останется неизвестным, а компания продолжит работу, не замечая, что информация о клиентах перетекла к конкурентам. Задача ИБ — не столько внешняя защита, сколько обеспечение внутренних бизнес-процессов, защита внутренних потоков информации, к которым нужно относиться очень внимательно.

Бизнес часто не видит существующих угроз. Если руководитель ИБ способен помочь с методикой оценки рисков, в глазах руководства компании его роль повысится и, как следствие, появятся дополнительные рычаги влияния и бюджеты. В этом случае служба ИБ может быть выведена на более высокий уровень, вплоть до предоставления услуг клиентам и бизнес-партнерам компании.

Наконец, сфера деятельности ИБ сейчас распространяется не только на защиту данных, но и на их приобретение. Добыча информации из разных источников и умение правильно ее анализировать и интерпретировать становятся источником важных преимуществ.

Источник преимуществ

«Еще несколько лет назад ощущалось, что бизнес не видит добавленной стоимости в тех решениях и работе, которую выполнял департамент информационной безопасности, поэтому и диалог не получался», — полагает Парамонов. Сейчас ситуация меняется, приходит понимание того, что правильно выстроенные решения способны дать бизнесу конкурентные преимущества. Хороший отдел ИБ несет своему бизнесу не ограничения, необходимые для защиты бизнес-процессов, а продукт, который можно продать конечному заказчику. Например, банк часто выбирают исходя из критерия безопасности. Да, людям необходима финансовая свобода, но они не хотят жертвовать безопасностью операций. Если компания гарантирует защиту персональных данных и предоставит информацию о способах их защиты, она будет иметь преимущество даже в том случае, если у конкурентов более низкие цены.

Важно помнить, что в условиях нестабильности безопасность — одна из ценностей, выделяющих компании среди конкурентов. На этом можно построить стратегию развития информационной безопасности, которая вполне может служить маркетинговым преимуществом.

Александр Парамонов, заместитель генерального директора, директор по развитию IBS Platformix

Ключевые направления развития служб ИБ

- Главное — анализ и защита бизнес-процессов
- Создание преимуществ для бизнеса — защита клиентов и контрагентов
- Поиск информации и аналитика
- Регулярная отчетность
- Непосредственная защита систем и информации