Ян Сухих, Schneider Electric: «Взаимодействие ИБ- и ИТ-департаментов — ключевой элемент успеха в условиях цифровизации бизнеса»

Ян Сухих, руководитель направления по информационной безопасности Schneider Electric и спикер Делового завтрака «ИТ-безопасность бизнеса», рассказал CFO Russia о подходах к информационной безопасности в России и мире.

Какие подходы к информационной безопасности используют в Schneider Electric?

Для промышленных компаний, которые работают в условиях рынка, я бы выделил два основных подхода. Первый и, к сожалению, самый популярный на сегодняшний день — формальное соответствие требованиям локальных регуляторов. Такой подход подразумевает, что компания вкладывает в информационную безопасность минимальное количество ресурсов: ровно столько, сколько необходимо для приведения систем в соответствие с требованиями регуляторов. Очень часто такой подход подразумевает «бумажную» безопасность, когда реальную защищенность предприятий практически не повышают. Но такая система формально соответствует требованиям ФСТЭК.

Риск-ориентированный подход к информационной безопасности выбирают компании, которые направлены на долгосрочное устойчивое развитие. В этом случае в дополнение к требованиям регуляторов компания оценивает кибер-риски и проводит количественную или качественную оценку потерь от кибер-инцидентов. Тогда собственники, члены правления, генеральные директора могут принимать взвешенные решения о необходимости инвестиций в ту или иную систему, имея на руках данные о потенциальных убытках и стоимости защитных мер.

Наша компания выбирает второй подход, как наиболее ответственный и осознанный относительно ИБ. Для заказчиков, которые хотят двигаться по второму пути, но не знают с чего начать, мы проводим рабочие встречи и тренинги. Внедрение риск-ориентированного подхода — это долгий путь, который требует серьезных вложений. Не все компании сегодня готовы идти по нему.

С какими сложностями сталкивается компания в области информационной безопасности?

Промышленные предприятия традиционно отстают в сфере ИБ от финансового сектора. Большинство финансовых организаций регулярно находятся под кибер-атаками, и для них работа в таких условиях уже давно стала нормой. В таких компаниях вопросы ИБ поднимают на самом высоком уровне. В промышленности все иначе. Высшее руководство промышленных компаний редко уделяет большое внимание вопросам информационной безопасности. А поддержка руководства — краеугольный камень ИБ. Подразделение ИБ для компании всегда убыточно. А если учесть, что хорошие специалисты стоят дорого, то такие подразделения бывают сильно убыточными. Прибыль они не создают по определению, а предотвращенные убытки от кибер-атак в отчет «О прибылях и убытках» не положишь. Поэтому самая главная сложность, с которой сталкивается большинство компаний, — отсутствие поддержки высшего руководства. Быстро исправить эту ситуация невозможно, здесь нужна долгая системная работа по повышению осведомленности высшего и среднего управленческого персонала компаний.

Другая тяжелая проблема — отсутствие или острый дефицит квалифицированных кадров. Очень часто имеющихся на предприятиях ресурсов недостаточно для проведения работы по оценке рисков. Даже на должное обслуживание систем защиты информации у многих компаний не хватает кадров. Выхода из этой ситуации в краткосрочной и даже среднесрочной перспективе, кроме использования услуг третьих поставщиков, я не вижу. Но такая модель все еще не очень популярна в России.

Что необходимо для успешного взаимодействия ИБ- и ИТ-департаментов?

Взаимодействие ИБ- и ИТ-департаментов — ключевой элемент успеха в условиях продолжающейся цифровизации бизнеса. Именно эти подразделения должны найти тот компромисс между ИТ-нововведениями и безопасностью, который позволит компании успешно развиваться. На мой взгляд, ключевой элемент успешного взаимодействия ИБ- и ИТ-департаментов — это наличие арбитра, человека или группы лиц, которые будут ориентированы на бизнес и будут понимать важность информационной безопасности. Не так важно в какой структуре ИБ, ИТ или вне этих структур будет находиться этот человек. Важно, что он должен иметь «вес», полномочия и ресурсы в компании. Учитывая последние тренды в бизнесе, на эту роль могут претендовать CDTO (Chief Digital Transformation Officer – *прим. ред.*). Эта роль подразумевает развитие бизнеса через внедрение новых цифровых технологий и процессов. А это невозможно делать осознанно без всестороннего анализа и учета, как возможностей, так и рисков, в том числе ИБ-рисков. При наличии достаточных полномочий и ресурсов именно эта роль может стать драйвером, который сделает взаимодействие подразделений ИБ и ИТ прозрачнее и эффективнее, а принятие решений о внедрении тех или иных технологий и сервисов — более взвешенным.

Задать свои вопросы Яну Сухих и узнать больше об опыте Schneider Electric вы сможете на Деловом завтраке «ИТ-безопасность бизнеса», который состоится 28 июня 2019 года в Москве.

Мария Кириченко, CFO Russia