Безопасность бумажная VS безопасность практическая, - управление ИБ в современных реалиях.

На прошедшем с 25 по 28 июля в Сочи Коде ИБ ПРОФИ тема управления безопасностью звучала на каждом мастер-классе. Но подход к этой теме у каждого из экспертов свой: кто-то призывает придерживаться международных регламентов и стандартов, а кто-то заявляет, что они бессмысленны при реальной кибератаке. Попробуем разобраться в доводах.

Бумажная безопасность представлена в России регламентами и стандартами, которые носят общее название «фрэймворки». Основаны они на требованиях регуляторов. Фрэймворки позволяют совместить в себе обеспечения соблюдения норм законодательства, экономику и потребности бизнеса в одном документе.

Один из самых распространенных в России документов по обеспечению безопасности – ISO27001. Он позволяет встраиваться даже в стандарты безопасности других стран, поэтому, «если ваш бизнес планирует выходить на международные рынки, то стоит реализовать у себя стандарт ISO27001», - комментирует **Андрей Прозоров**. Также, по мнению эксперта, этот документ может пригодиться при составлении должностных инструкций или методик оценки эффективности ИБ. Его дополнила **Наталья Гуляева** (Hogan Lovells): “Стандарты пригодятся вам при аудите, проводимом ФСТЭК или прокуратурой. С чего-то вам надо начинать, дать какие-то документы проверяющим, и тут вам на помощь придут эти регламенты».

Ряд экспертов на конференции выразил скепсис по отношению к составлению регламентов и бумаг в сфере управления информационной безопасностью. В их числе **Евгений Волошин** (BI.Zone): «Когда в компании назревает необходимость во фрэймворке, надо понимать, для чего в конечном счете это делается. Введя в работу какой-то стандарт в форме документа, вы «просто причесались», но должны быть какие-то внешние меры, которые актуализируются согласно внешним угрозам».

Антон Карпов (Яндекс) уверен, что «безопасность – это не про фрэймворки, безопасность в первую очередь, про людей». Любой внедренный стандарт, по убеждению спикера, не вреден, но при внедрении очень важно не перегнуть палку, чтобы оставить место для маневра в условиях

динамично меняющейся киберсреды. «С другой стороны, - подытожил эксперт, - если вы у себя в компании защитили все бизнес-процессы, то, наверное, нет смысла делать под это специальный регламент. Если все работает хорошо, значит, вы добились конечной цели».

«Безусловно, информационная безопасность компании начинается с формирования политики и регламентов, которые должны соответствовать определенным стандартам. Конечно, эту задачу упрощают различные фреймворки. Но изложенное на бумаге нужно эффективно воплотить в жизнь, при этом минимально повлияв на бизнес. Стремительно набирающие популярность решения класса PAM (Privileged Account Management) закрывают большое количество требований различных стандартов и политик, поскольку получение доступа к учетным данным привилегированных пользователей является главным направлением любых атак. Ценность Thycotic в быстром внедрении и простоте использования, что, несомненно, упрощает достижение бумажного идеала», - комментирует директор по развитию бизнеса Thycotic по России и СНГ **Илья Горюнов.**

Свое мнение относительно бумажной безопасности выразил программный директор конференции **Алексей Лукацкий:** «Злоумышленнику все равно, какой стандарт вы внедряли, он вас ломает не по стандарту». Для того, чтобы обезопасить бизнес в практическом смысле существует множество вендорских решений. Однако, по опыту экспертов Кода ИБ ПРОФИ, часто бюджеты на ИБ осваиваются эффективно, а на практике купленные решения не внедряются, а «лежат на полках» или остаются интегрированными в лучшем случае лишь на половину. Такую безопасность спикеры называют бессмысленной тратой денег.

Мастер-классы и практикумы, прозвучавшие на конференции охватили как вопросы, связанные с обеспечением бумажной безопасности, так и чисто технические вопросы ИБ.Участники Кода ИБ ПРОФИ отметили практическую значимость ворк-шопа **Льва Палея**, на котором отрабатывались навыки выбора и обоснования средств защиты.

Конференция продлилась 4 дня, два из которых профессионалы ИБ провели, погрузившись в освоение знаний и навыков, и еще два дня – в приключения в горах и на море.