Зачем в природе нужен «безопасник»?

«Не подскажете номер счёта, где деньги лежат? Нет? И не надо – вон у Любочки из бухгалтерии он на стикере написан и на монитор приклеен! А платёжку мне по «мылу» пришлёт Верочка, она же логин и пароль для «клиент-банка» по «скайпу» сообщит, чтобы эту самую платёжку в банк отправить. Кто сказал нельзя платёжку по «мылу»? Какой-такой «безопасник»? Вечно они продуктивно работать мешают!»

Так кто же такой «безопасник»? Зачем он нужен, кроме как для нудного инструктажа о том, куда «не ходить» и что «не открывать»? И почему он бесцеремонно «нарушает» права сотрудников на личную жизнь, запрещая, например, бурлящую захватывающими событиями соцсеть «ВКонтакте»?

Обязанность подразделения информационной безопасности – прежде всего, конечно, оберегать от информационных угроз бизнес предприятия. В основном, это касается защиты информационных, финансовых и интеллектуальных (например, права на объекты интеллектуальной собственности) активов. Основные современные информационные угрозы (по количеству выявленных случаев и размеру ущерба) – утечка и изменение (включая удаление) конфиденциальной информации. Главной же целью злоумышленников при этом является, разумеется, хищение денежных средств.

Немного статистики: согласно глобальному исследованию компании InfoWatch, в 2015, по сравнению с предыдущим годом, количество утечек в мире выросло на 7,8%, а Россия который год подряд находится по этому показателю на 2-ом месте в мире. Отметим, что в 65,4% виновником утечки становился внутренний нарушитель, в 32,2% - внешний (в 2,4% случаев виновник не был выявлен). И, наконец, в 90,8% утечек их объектом стали персональные данные и платёжная информация, причём за 2015 в мире было скомпрометировано порядка 1 млрд записей.

По сути, подобная статистика говорит о том, что «безопасники» находятся на переднем крае «фронта» невидимой, но очень интенсивной и изощрённой по используемым средствам, битвы между предприятиями и киберпреступниками. И битва эта идёт буквально на выживание: утечка конфиденциальной информации может привести к прямому финансовому или косвенному репутационному ущербу, измеряемого в десятках и сотнях миллионов долларов или даже к полной потере бизнеса.

Противостоя постоянно совершенствующимся инструментам атак киберзлоумышленников, сотрудники подразделения информационной безопасности априори находятся в невыгодном положении обороняющихся. Добавьте ограниченность в средствах защиты, необходимость реагировать быстро (время реакции на многие угрозы должно составлять считанные минуты!) и большое количество потенциальных «точек прорыва» периметра обороны (которыми, как мы упомянули выше, могут стать как «чужаки», так и «свои») – в общем, нелёгкая работа.

Однако, любой банк (и ваш не исключение!) – организация, где подразделения тесно взаимодействуют друг с другом, а деятельность достаточно формализована. В итоге, как ни банально, общий успех работы зависит от сплочённости работы подразделений и чёткости выполнения ими заведённых правил. Поэтому и успех «безопасников» (хоть они многим и представляются специфической «кастой», эдакими «жандармами», присматривающими за другими) в битве с киберпреступниками сильно зависит от рядовых сотрудников, от того, чтобы они не становились теми «точками прорыва» обороны.

Будучи заинтересованными в этом, «безопасники» стараются вести «просветительскую деятельность»: проводят плановые и внеплановые инструктажи и тренинги по информационной безопасности, пишут для сотрудников популяризирующие вопросы обеспечения информационной безопасности статьи, предусмотрительно советуют, консультируют и рекомендуют.

Делают всё, чтобы в случае появления подозрительных обстоятельств для сотрудника главным правилом было - «Сомневаешься? Не делай - спроси безопасника!».

И ведь что важно: правила информационной безопасности актуальны и защищают не только интересы компании и её клиентов, но и личные интересы самого сотрудника, его персональные данные и финансовую информацию. Их соблюдение выгодно (подчас в буквальном, финансовом, смысле) каждому сотруднику!