INT-01 - “Как обучить специалистов по ИБ у себя в компании?

Эра цифровизации, эра, когда фильмы про восстания роботов уже не кажутся недействительной реальностью, эра, когда почти каждый человек в мире носит с собой устройство слежения - его телефон, эра, когда за считанные минуты можно установить связь на разных уголках планеты, эра, когда квантовое перемещение является перспективой следующих нескольких лет, эра “Киберпространства”.

Здравствуйте, я мистер Р - владелец компании Т. И я столкнулся с большой проблемой: вопрос информационной безопасности в эре “Киберпространства” стоит очень остро. Ежедневно мир сталкивается с банальной неграммотностью в области информационной безопасности. Информация - ценнейший ресурс, способный принести прибыль, это породило огромное количество интернет-мошенников, которые, и по сей день, вне зависимости от распространения правил пользования интернет-ресурсами, добиваются успехов в своих “делах”. Я уверен, что информация в моей компании принесёт большую прибыль злоумышленнику, если он до неё доберётся. В связи с этим я принял решение открыть отдел ИБ в своей компании и захотел наполнить его лучшими специалистами. И как оказалось, специалистов в области информационной безопасности почти нет... . А те, кто есть, уже давно разобраны лидирующими компаниями.

Я поехал в ВУЗы, которые готовят специалистов в области ИБ. Пообщавшись со студентами, пришло осознания того, что почти никто не понимает, что такое информационная безопасность. Если даже студенты, обучающиеся основам ИБ, не понимают, что им предстоит делать, то любой другой рядовой житель планеты уж точно не осознает значимость этой сферы. Ко мне пришло отчаяние, программы обучения устарели, ВУЗы выпускают специалистов, которые не готовы защитить мою компанию, а предприятия-

вендоры не могут гарантировать непрерывную защиту, без которой я не вижу полноценной защиты.

Немного обдумав, я пришёл к следующему пути: я связался с компанией-лидером в области ИБ и попросил отправить перечень фундаментальных знаний, которыми необходимо владеть специалисту по ИБ, далее я обратился к Интернет-ресурсам и начал изучать всевозможную литературу об информационной безопасности. Таким образом, я наткнулся на журнал “Хакер” и понял, что никто лучше не знает вопрос ИБ, как люди, которое бывали “по ту сторону” - этичные хакеры. Я связался с компанией, которая проводит курсы по повышению квалификации в области ИБ, и заключил договор: компания выделит мне группу специалистов, которые в течении полугода подготовят специалистов моей компании. Далее я связался с компанией, которая занимается предоставлением услуг по тестированию и проникновению в ресурсы компании, также заключил договор, по которому мне выделили пару человек. Задачей этих людей был контроль за обучением и участие в корректировке программы подготовки. Таким образом, программа подготовки специалистов по ИБ в моей компании совместила в себе теоретические и практические знания. Я вновь отправился в ВУЗы и посетил защиты дипломных работ, самым интересным, на мой взгляд, ребятам я предложил работу в своей компании. Исход: 7 человек приступило к обучению, отдел был сформирован.

Зачем я пишу этот рассказ? Я хочу, чтобы хороших специалистов по ИБ в нашей стране стало куда больше, а программы обучения были сформированы под требования современных условий. Поэтому я поделюсь программой обучения специалистов в моей компании. К слову, из одного кабинета мы сделали лабораторию, где и проводились практические задания.

Первый месяц курса обучающиеся разбирали вопросы технической защиты информации, почему-то о ней часто забывают, а ведь именно она является основой безопасности в компании. Для многих обучающихся стал большим удивление тот факт, что злоумышленник, не видя экран монитора, может его

воспроизвести, просто считав побочное электромагнитное излучение. В ходе модуля ТЗИ обучающиеся вспомнили законы физики, узнали, что такое утечка информации по техническим каналам связи, узнали, как проводятся специсследования. Результатом обучения стали умения использования отечественных аппаратных и программно-аппаратных средств защиты информации, таких как “заглушки”, “генераторы шума”, “Соболь”, SecretNet Studio. В роли аттестации выступила реализация защиты переговорного помещения (защищаемое помещение).

Второй месяц курса был посвящён компьютерным сетям, обучающиеся вспомнили какие устройства участвуют в построение сети, как и по каким уровням передаётся информация, что содержит в себе информация на каждом уровне передачи. Какие бывают протоколы, с какими портами они взаимодействуют. Были рассмотрены вопросы построения сети и различные виды атаки на них. Результатом обучения стали умения работы и настройки сетевого оборудования. В роли аттестации - cft-соревнование, в ходе которого обучающимся необходимо было отследить и заблокировать вредоносный трафик.

Третий месяц обучения был направлен на изучение вопросов администрирования операционных систем. Обучающиеся познакомились с различными дистрибутивами ОС Линукс, с возможностями серверных Windows. Результатом обучения стали умения настройки локальной сети: поднятие домена, разограничение прав доступа, настройка логирования. В роли аттестации была настройка сегментов локальной сети компании.

Четвёртый месяц обучения был посвящён языкам программирования. Хороший специалист ИБ всегда должен уметь читать чужой программный код. Обучающие познакомились с такими языками программирования как: Python, Java, JS. Результатом обучения стало базовое понимание синтаксиса популярных языков программирования. В роли аттестации выступило написание скрипта на любом из языков.

Пятый месяц обучения был посвящён изучению правовых аспектов ИБ. Все меры защиты информации регулируются соответствующими нпа. Специалисты моей компании точно должны уметь правильно составлять документацию по ИБ. Результатом обучения стало понимание, как работает законодательство в сфере ИБ и как его соблюдать. В роли аттестации выступило написание Политики безопасности для компании Т.

Шестой месяц и последний месяц обучения был посвящён веб-защите. Так как моё предприятие имеет доступ в Интернет, специалисты ИБ должны чувствовать себя в Интернет-пространстве свободно. Обучающиеся изучили основные угрозы, связанные с получением доступа к АРМ из глобальной сети. Результатом обучения стало понимания, как с помощью Интернет-выхода злоумышленник может проникнуть в компанию. В роли аттестации обучающиеся провели обучение остальных сотрудников компании, объяснив, что нельзя делать на рабочих машинах.

Благодаря тому, что я ответственно подошёл к организации отдела ИБ, моя компания уже третий год чувствует себя защищёно. Я ни капли не пожалел, что в своё время потратил большое количество средств и других ресурсов на организацию информационной безопасности в моей компании. Компания Т расширяется, а вместе с ней и отдел ИБ укомплектовывается новыми и отличными специалистами.