УДК 004.056

Индивидуальный подход к построению системы защиты от фишинг-атак

Автор: М.А. Попов, Санкт-Петербургский государственный экономический университет, г. Санкт-Петербург

Научный руководитель: Е. В. Майорова, Санкт-Петербургский государственный экономический университет, г. Санкт-Петербург

На сегодняшний день самым уязвимым местом информационной системы чаще всего является человек. Зачастую злоумышленнику не приходится взламывать сети и проходить файрволлы, ему достаточно лишь воздействовать на человека, который уже имеет доступ к необходимой системе. Один из самых действенных способов воздействия – это фишинг, а, в случае получения несанкционированного доступа к конкретной системе, целевой фишинг.

Важнейшей задачей специалиста по безопасности является выстраивание системы защиты от такого рода атак, а это, в первую очередь, организационная работа с персоналом. О технических методах защиты также не стоит забывать, однако, к сожалению, в настоящее время они не столь эффективны, и, при желании, их не так трудно обойти. В данном случае, основным методом работы с персоналом является обучение, проведение лекций, и так далее. Главная проблема заключается в том, что за счет своих индивидуальных особенностей люди в разной степени воспринимают информацию, и, следовательно, коэффициент полезного действия у обучения может очень сильно колебаться.

Данное исследование направлено на поиск и разработку оптимальных методов работы с персоналом для обеспечения максимального уровня защищенности информационной системы компании от фишинг-атак, а также сравнение показателей защищенности до и после проведения мероприятий по обучению персонала. Исследование проводилось на базе Организации. Сначала, сотрудникам было предложено пройти тестирование, в котором необходимо было определить, является ли сообщение фишинговым. В результате, выяснилось, что 55% сотрудников не смогли верно определить все фишинговые сообщения, что является большим риском для компании. Затем, были определены основные векторы фишинг-атак и основные характеристики личности, влияющие на восприимчивость к данным векторам. На основе этих данных был составлен опросник, оценивающий эти характеристики, который затем прошли сотрудники. По результатам опросника были созданы относительно схожие группы, в которых проводилось обучение, акцентирующее внимание на то, что более необходимо для конкретной группы. После обучения снова было проведено тестирование, аналогичное ранее проводимому, и процент сотрудников, которые не смогли определить все фишинговые сообщения снизился до 15%.

Таким образом, данный метод можно рекомендовать в качестве эффективного способа повышения защиты от фишинг-атак в компании.

М.А. Попов

Е. В. Майорова