Иван БАБЕНКО, МЭА

ИНСАЙДЕР: СУТЬ ЯВЛЕНИЯ, УГРОЗЫ, ПРОТИВОДЕЙСТВИЯ

Abstract: *This article contains information about malevolent insider problem. Here you will find described particularities of this phenomenon, it's classification, it's threats and basic counteraction methods.*

Все угрозы информационной безопасности принято классифицировать на внешние и внутренние. Предметом данной статьи является проблема злонамеренного инсайдера, входящего в группу внутренних угроз информационной безопасности. Это одна из самых сложных и непредсказуемых категорий этой группы, так как зачастую действия злонамеренных инсайдеров неумышленны либо наоборот, очень хорошо спланированы. И чтобы бороться с такой угрозой, необходимо использовать все навыки и средства, находящиеся в инструментарии офицеров информационной безопасности.

Перед тем как говорить о том, что такое инсайдерство, поговорим об особенностях понятия инсайдер, для того чтобы впоследствии иметь дело с той категорией людей и поступков, которым мы и планируем противостоять.

ИНСАЙДЕР (англ. *insider*, от *inside* – буквально «внутри») – лицо, имеющее в силу своего служебного или семейного положения доступ к конфиденциальной информации о делах компании. Речь идет о должностных лицах, директорах, основных акционерах корпорации с широким владением акциями и их ближайших родственниках. В эту группу включаются также лица, добывающие конфиденциальную информацию о деятельности корпорации и использующие ее в целях личного обогащения.

Так как инсайдер – лицо нейтральное, то говорить о противостоянии инсайдерам логически некорректно. Инсайдер может занимать негативную позицию и быть угрозой для предприятия, атакующим субъектом. Об этом субъекте мы и будем говорить далее. Для понятности и корректности назовём этого субъекта Злонамеренным Инсайдером (ЗИ).

На формирование ЗИ в организации может влиять совокупность социальных, экономических и психологических факторов.

Есть несколько подходов к классификации ЗИ: по мотивационным признакам (неумышленные и умышленные) и по сценариям деятельности. Каждый класс ЗИ требует своевременной идентификации, особого вида противостояния и индивидуального подхода даже внутри отдельного класса.

В РМ также были отмечены преступления, связанные с проблемой ЗИ. Можно сказать, что у нас такого типа угрозам наиболее подвержены финансово-банковская сфера, но нельзя исключать их появления и в других отраслях, особенно в малых и средних организациях.

Для любого типа ЗИ существуют внутренние риски предприятия, связанные с тремя стратегическими категориями организации: конфиденциальная информация и её целостность, оборудование, сотрудники и партнёры.

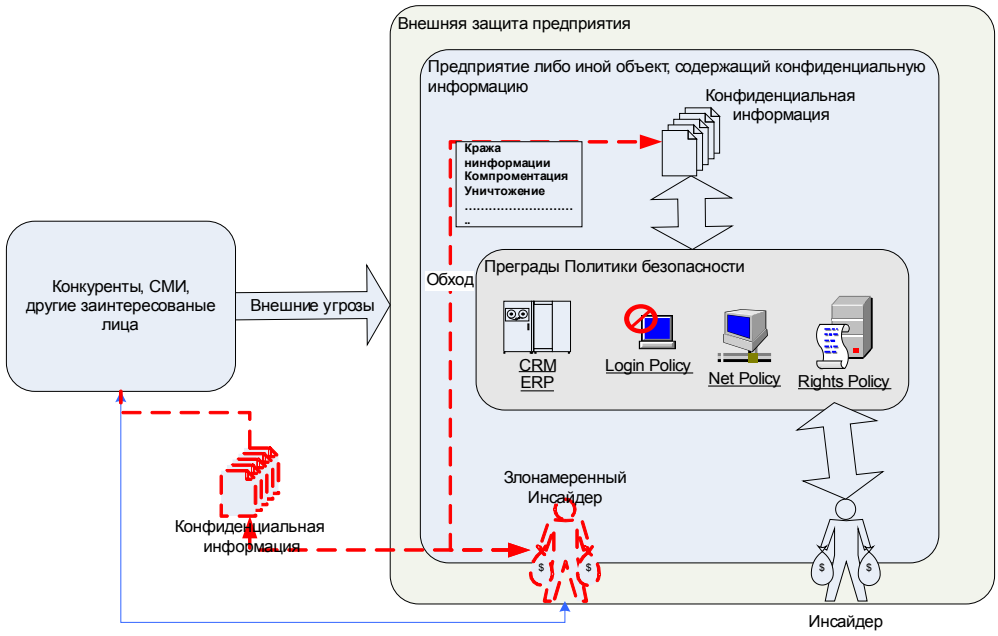
Риск возникновения на предприятии ЗИ приравнивается минимум к 25-35% на предприятии из «группы риска» и к 15-20% на среднестатистическом предприятии.

Методология противодействия ЗИ включает в себя широкий спектр инструментов противостояния, которые в свою очередь делятся на основные группы: социально-психологические методы, технические методы, финансово-экономическое урегулирование, нормативно-правовые методы. По сути проблема злонамеренного инсайдера не нова и присутствовала задолго до того, как человечество стало задумываться о вопросах информационной безопасности. Поэтому ни категории злоумышленников, ни методология противостояния с тех времён существенно не изменились, изменились лишь подход и функционал для работы с этой угрозой.

Для успешного противостояния обязательно необходимо знать портрет злоумышленника и владеть арсеналом, для успешной борьбы с ним.

Обобщим всё перечисленное выше и оформим объектную модель (Схема 1):

Схема 1. Объектная модель злонамеренного инсайдинга



Для борьбы с этим явлением – все средства хороши, только использовать их нужно рационально и продуманно.

Руководство предприятий должно быть всегда проинформировано о том, что нет абсолютно идеальной политики безопасности на практике, и определённая доля угрозы всегда висит над предприятием. Этот факт должен всё время подстёгивать для периодических проверок персонала, анализа и повышения степени электронной защиты информации. Но это не значит, что бюджет для таких мероприятий безграничен, напротив, он должен быть почти всегда ниже оценочной суммы риска появления такой угрозы и её ликвидации.

Для решения такой проблемы, как злонамеренное инсайдерство подходит выражение: «Нужно знать врага в лицо», а так как лицо «врага» в таких случаях и так «всегда на виду», то есть необходимость «узнать врага и изнутри».

Литература:

1. А. Доля. Классификация инсайдерских угроз: вероятные сценарии / http://www.cnews.ru/reviews/free/insiders2006/articles/classification.shtml
2. Защита от инсайдеров. Обзорный курс InfoWatch / http://www.pcmag.ru/elearning/course/index.php?COURSE_ID=7
3. А. Сабанов. Обзор технологий идентификации и аутентификации. / http://www.infosecurity.ru/cgi-bin/cart/arts.pl?a=_060920