КЛАССИФИКАЦИЯ ИНСАЙДЕРОВ

Григорий Бортэ,
Молдавская Экономическая Академия (Республика Молдова)

The aim of this article is to study the ways of classifying insiders into different categories. Persons who give confidential information away from the company they work in are the object of this article.

Практически три четверти преступлений в сфере информационных технологий приходится, по статистике, на внутренние угрозы. Поэтому обеспечение внутренней безопасности становится одной из приоритетных задач практически любого учреждения.

Целью данной работы является исследование методов разделения внутренних нарушителей на группы.

Объектом исследования являются лица преднамеренно или непреднамеренно выдающие информацию, доступную узкому кругу лиц вовне.

Инсайдер – работник организации, имеющий доступ к конфиденциальной информации, недоступной другим лицам, или широкому кругу лиц. Также, слово может нести негативный оттенок. Например, лицо, опубликовавшее конфиденциальную информацию, или передавшее её лицам, не имеющим доступ к данной информации.

Виды инсайдеров по преследуемым целям:

- Непреднамеренные инсайдеры
- Использующие полномочия и доступ в личных целях
- Продающие конфиденциальную информацию вовне
- Сами использующие доступ и положение для получения материальных выгод

Непреднамеренных инсайдеров можно подразделить на:

- Манипулируемых
- Самостоятельных

Обе эти категории проявляют неосторожность по отношению к информации. В первом случае существует какой-либо движущий механизм, возможно, осуществляется попытка доступа к конкретным данным. Во втором случае работник сам выдаёт какие-либо данные, которые злоумышленник впоследствии «находит». К данным категориям применим термин «социальная инженерия».

Использующих полномочия и доступ в личных целях можно подразделить на:

- Желающих отомстить
- Любопытных

К первой категории могут относиться уволенные или каким-ли-

бо другим способом ущемлённые работники. Обычно, данный вид злоумышленников стремится нанести как можно больший вред компании, а не получить какие-либо материальны блага или ценности. Ко второй категории относятся люди, преднамеренно злоупотребляющие своими полномочиями с целью получения доступа, как к корпоративным, так и личным тайнам коллег. Часто, представители обоих категорий преследуют в качестве цели повышение чувства собственного достоинства.

Работники, продающие конфиденциальную информацию вовне, являются классическим примером инсайдеров. Их можно подразделить на 2 типа:

- Мотивированные
- Планирующие использовать информацию

К первому типу относятся люди, получившие конкретные предложения по покупке информации. Примером может служить бывший сотрудник лихтенштейнского банка LGT Хайнрих Кибер в феврале 2008 года продал приватную базу своего бывшего работодателя немецким и британским спецслужбам, выручив за нее более $7 млн. Пример Кибера наглядно показал, насколько прибыльным может оказаться банковский инсайд. В "базе Кибера" содержались сведения о банковских счетах немецких предпринимателей, которые использовали банки Лихтенштейна для уклонения от налогов. Для немецких спецслужб покупка оказалась крайне выгодной - уже спустя неделю она окупилась практически в шесть раз. Однако банку LGT и всей финансовой системе Лихтенштейна Кибер нанес поистине невосполнимый ущерб.

Ко второму типу относятся те, кто крадёт информацию с возможностью использовать её в перспективе, однако, не имеющим полной уверенности и гарантии того, что это удастся. Примером второго типа могут служить стажеры и практиканты, которые, получив доступ к информации, постарались сохранить себе как можно большую (или как можно более важную на их взгляд) её часть, не имея конкретного плана по дальнейшему её использованию.

Примером сотрудников, самих использующих доступ и положение для получения материальных выгод могут служить работники банков, получившие доступ к прогнозам курсов валют на определённый промежуток времени.

Заключение

Зная цели, преследуемые инсайдерами компании можно предложить следующий комплекс мер по борьбе с возможными утечками информации:

- Контроль исходящего и входящего трафика
- Контроль входящей и исходящей электронной почты

- Ограничение использования подключаемых к компьютеру устройств
- Строгое и чёткое разграничение доступа к информации
- Совершенствование законодательной базы
- Проведение специализированных тренингов для персонала

Литература:

1. Дамир Равилов «Методы классификации внутренних нарушителей» http://infocom.uz/2009/12/16/metodyi-klassifikatsii-vnutrennih-narushiteley/
2. Алексей Комаров «Защита от инсайдера» http://www.osp.ru/text/print/302/5157097.html

УГОЛОВНО-ПРАВОВАЯ ХАРАКТЕРИСТИКА ПРЕСТУПЛЕНИЙ ПРОТИВ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

(по законодательству Республики Молдова)

Светлана Грищук-Бучка,
Институт истории, государства и права АНМ
(Республика Молдова)

The paper is dedicated to the examination of the categories of crimes against computer safety. This article is based on the analysis of national criminal legislation of the Republic of Moldova.

Противоправные преступные деяния свойственны человечеству с древнейших времен. Однако с развитием цивилизации меняются не только предметы и методы преступного воздействия, но и сам объект преступного посягательства.

Одним из ярких примеров данной категории преступлений являются преступления в сфере компьютерной информации [1]. Активное развитие компьютерных технологий, доступность средств коммуникации, всеобщая информатизация населения стали с одной стороны, еще одной вехой развития цивилизации, а с другой стороны - серьезным испытанием для «права» и правового регулирования. «Наряду с очевидными преимуществами, которые получило человечество от развития информационных технологий, как