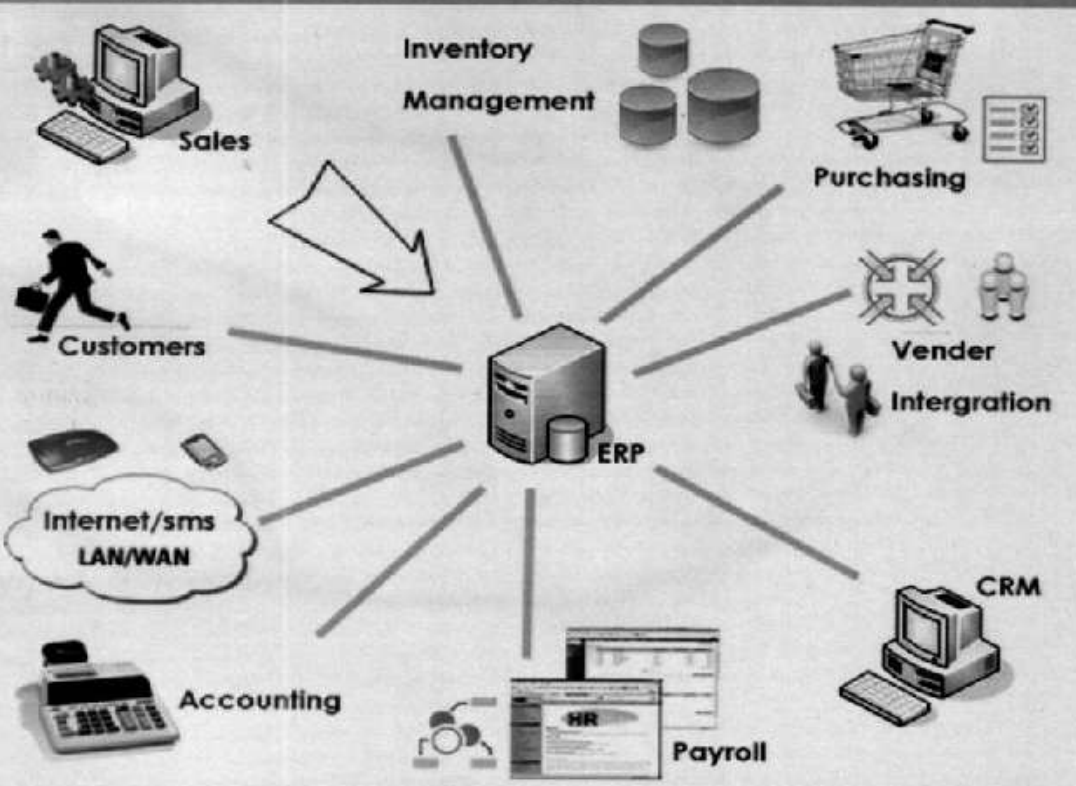
СТОПАНСКА АКАДЕМИЯ "Д. А. ЦЕНОВ" – СВИЩОВ

ПРОЕКТ „МЕТОДОЛОГИЯ ЗА ИЗГРАЖДАНЕ НА РАЗПРЕДЕЛЕНА БИЗНЕС ИНТЕЛИГЕНТНА СИСТЕМА В МАЛКИ И СРЕДНИ ПРЕДПРИЯТИЯ"

МЕЖДУНАРОДНА НАУЧНА КОНФЕРЕНЦИЯ

СИСТЕМИ ЗА УПРАВЛЕНИЕ НА БИЗНЕСА В МАЛКИ И СРЕДНИ ПРЕДПРИЯТИЯ



23 - 24 април 2010 г.
Свищов

МЕЖДУНАРОДНА НАУЧНА КОНФЕРЕНЦИЯ

СИСТЕМИ ЗА УПРАВЛЕНИЕ НА БИЗНЕСА В МАЛКИ И СРЕДНИ ПРЕДПРИЯТИЯ

ПРИРОДА ИНСАЙДЕРСТВА

Григорий Бортэ, Молдавская Экономическая Академия

This article aims to analyze the nature of data leaks from insiders. Classification of insiders' causes, goals and means as well as means of counteraction and protection are as well discussed.

В современном мире тяжело себе представить экономическое развитие какой-либо крупной компании без использования информационных технологий для хранения крупных массивов данных. Будь то крупная корпорация, зарекомендовавшая себя на мировом рынке, или маленькая фирма, каждый из них заинтересован в обеспечении конфиденциальности своей информации, своей коммерческой тайны. Известно немало случаев серьёзных атак на информационные системы извне, в результате которых компании несли колоссальные убытки, однако куда более опасны угрозы внутренние. Они намного более непредсказуемы и с ними тяжелей бороться. 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 изучение и описание природы инсайдерства как явления.

Объектом исследования являются действия, производимые инсайдером, его мотивы, цели и средства.

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.

Для разработки эффективных методов борьбы с инсайдерством необходимо изучить его суть, то, что характерно для данного явления независимо от его проявления, черты, свойственные любому преступлению подобного рода - его природу.

Природа инсайдерства включает в себя следующие компоненты:

- Мотивы
- Цели
- Средства

Мотивы – движущая сила действий инсайдера. К мотивам, движущим тем или иным лицом при совершении злонамеренных действий можно отнести:

- Экономические – например, низкая заработная плата, тяжелое материальное или финансовое положение лица, совершающего правонарушение, или простая жадность[6][10]. Лицами, стимулирующими данный вид мотивации, могут выступать конкурентные предприятия (другими словами – промышленный шпионаж, конкурентная разведка), криминальные или государственные структуры, лица, способные извлечь из данной информации материальную, финансовую или иную выгоду.
- Личные – чаще всего, к личным мотивам относится желание отомстить[1][5] или простое любопытство[10]. Притом, часто подобные правонарушения наносят не финансовый или материальный урон, а вредят престижу, репутации фирмы, корпорации[7] или непосредственно определённой личности. Например, во время предвыборной кампании в марте 2008 года в США были уволены 2 сотрудника консульского отдела государственного департамента США за успешную попытку получения доступа к конфиденциальным данным представителя демократической партии Бараке Обама. Позже о подобных посягательствах заявили Хиллари Клинтон и Джон Маккейн. Скорее всего, данный инцидент был вызван простым любопытством и не понёс за собой существенного финансового и материального урона, однако, морально/этическая сторона вопроса обсуждалась очень длительный период времени[9].
- Непреднамеренная выдача информации – фактически, отсутствие мотива, как такового. Безалаберность, халатность, небрежность, невнимательность. По результатам исследований, подавляющая часть (более 75%[4]) преступлений относится именно к этой категории. Например, из-за халатности сотрудников разорившейся вследствие кризиса компании Union Mortgage Services, занимающейся предоставлением ипотечных услуг, пострадало большое количество законопослушных граждан. Работники данной компании вместо того, чтобы правильным способом уничтожить конфиденциальные документы, содержащие данные о клиентах (выписки из банковских счетов, кредитная отчетность, налоговые отчисления) просто выбросили эти бумаги в мусорный бак. В данном случае проявила свои недостатки законодательная база. За данный инцидент должна была отвечать компания, однако

обанкротившаяся компания уже не может нести ответственность.

К мотивам, предотвращающим то или иное лицо от злонамеренных действий, можно отнести:

- Идейность – лицо не будет проводить саботирующие действия в силу своих принципов или убеждений.
- Боязнь быть пойманным – данный мотив является психологическим барьером. Человек готов пойти на правонарушение в тех случаях, когда выполненяется одного или несколько условий из следующих:

a) Лицо уверено, что его невозможно поймать, вычислить в дальнейшем либо считает шанс быть пойманным незначительным

b) Считает, что выгода от совершенного правонарушения превысит потери от его выявления

c) Не задумывается о последствиях - халатность или неспособность предвидеть последствия.

Цель преступления – желаемый результат действий. К целям инсайдерской деятельности можно отнести следующие:

- Кража информации – самая часто преследуемая цель. Обычно, внутренней информацией компании могут быть заинтересованы конкуренты, государственные органы, криминальные структуры, а также компании, заинтересованные во внедрении каких-либо новых для себя технологий. Например, в 2008 году был задержан бывший сотрудник LG Electronics по фамилии Джанг. Ему было предъявлено обвинение в передаче третьим лицам конфиденциальной информации о заводе по производству плазменных панелей. По оценке экспертов LG Electronics, компании мог быть нанесён ущерб в размере полутора миллиарда долларов[9].
- Саботаж – создание помех нормальному функционированию предприятия или его части.

Средства – инструменты, используемые злоумышленником для реализации своих целей. Средства, используемые для совершения преступления можно подразделить на:

- Технические – компьютерная техника, ноутбуки, мобильные телефоны, фотоаппараты, принтеры.
- Программные – программы-шпионы, сканеры, программные средства получения доступа к компьютерам и т.д.

- Социальные – побуждение сотрудников организации к совершению действий, последствия которых отличаются от тех, которые они себе представляют.

Каналы утечки:

- Мобильные устройства - по результатам исследований, наибольшее число утечек произошло именно благодаря мобильным устройствам (около 50%[8]): телефонам, флешкам, ноутбукам, CD и DVD диски. Их недостатки заключаются в том, что их легко потерять, а также легко спрятать и вынести.
- Интернет – самый простой в использовании канал, через него происходит порядка 17%[8] утечек.
- Неправильная утилизация отработанных материалов – халатность и безалаберность. Например, неправильная утилизация резервных копий данных, бумажных носителей информации.
- Электронная почта – проста в использовании, однако, чаще всего строго контролируется.
- Факс – в данный момент один из наименее распространённых вариантов. Не очень удобен в использовании, громоздок, заметен.

К средствам, позволяющим предотвратить злонамеренные действия можно отнести[3][11]:

- Технические – физическое ограничение доступа персонала на определённые участки предприятия, ограничение подключения дополнительного оборудования.
- Программные – антивирусные программные продукты, брандмауэры, программный контроль трафика, электронной почты, IPC-системы. Очевидно, что злоумышленник, скорее всего, будет осведомлён о наличии подобных средств защиты, и будет стараться их обойти.
- Социальные – специализированные занятия, семинары, тренинг, инструктаж персонала. Также, очень важный элемент – тщательный подбор персонала, доступное разъяснение необходимости мер безопасности, прав и ответственности. Сотрудник должен понимать, что его неправильные или неосторожные действия могут повлечь за собой значительный урон.

Инсайдерство по своей сути – шпионаж, независимо от того уровня, на котором оно осуществляется: будь то международный уровень или уровень одного человека. Ущерб от данного вида правонарушения трудно переоценить, будь он материальным, финансовым или моральным. Изучив природу инсайдерства можно лучше понять первопри-

чины и суть данного явления, разработать и внедрить более эффективные методы борьбы с ним и усовершенствовать уже существующие. Борьба должна осуществляться как на глобальном (международном и государственном) уровне, в виде законов, соглашений, договоров, так и на локальном (предприятие, фирма) уровне, в виде комплекса технических, программных и социальных мер пресечения. Элементы, рассмотренные в данной статье, достаточно широко описывают природу данного явления, однако, по своей сути оно куда глубже и опасней, чем может показаться на первый взгляд.

Литература

1. Равилов Д. *Методы классификации внутренних нарушителей* http://infocom.uz/2009/12/16/metodyi-klassifikatsii-vnutrennih-narushiteley/
2. Комаров А. *Защита от инсайдера* http://www.osp.ru/text/print/302/5157097.html
3. CSI/FBI Computer Crime And Security Survey http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf
4. Доля А. *Инсайдеры наступают* http://www.citcity.ru/14874/
5. Уволенный сотрудник - угроза безопасности компании http://www.seclab.ru
6. Лупанов В. *Банки: почти каждый инсайдер уносит миллион* http://sb.adverman.com/modules/myarticles/article.php?storyid=3
7. Анисимов Д. *Сколько стоит банковский инсайдер* http://www.pcweek.ru/spheres/detail.php?ID=111099&SPHERE_ID=13866
8. Глобальное исследование инцидентов внутренней информационной безопасности http://www.securitylab.ru/analytics/291018.php
9. Ульянов В. *Инсайд 2008: Самые громкие и самые глупые утечки* http://www.abipage.ru/novosti-otrasli/03-05-2008-gromkie-utechki-2008.html
10. Prince K. *The top 10 security threats of 2009* http://blogs.reuters.com/great-debate/2009/12/22/the-top-10-security-threats-of-2009/
11. Крупнейшие утечки 2009 года http://www.infowatch.ru/press/news/risks/2854/

АКАДЕМИЧНО ИЗДАТЕЛСТВО "ЦЕНОВ"

Управител: доц. д-р Богомил Трайков, тел. 0631/6 08 75
Зам. управител: Петър Папазов, тел. 0631/6 08 75
Компютърен дизайн корица:
Предпечат дизайн: Светла Петрова

СТОПАНСКА АКАДЕМИЯ "Д. А. ЦЕНОВ"
Свищов, ул. Ем. Чакъров, 2

АКАДЕМИЧНО ИЗДАТЕЛСТВО "ЦЕНОВ"
Свищов, ул. Градево, 24

МЕЖДУНАРОДНА НАУЧНА КОНФЕРЕНЦИЯ

СИСТЕМИ ЗА УПРАВЛЕНИЕ НА БИЗНЕСА В МАЛКИ И СРЕДНИ ПРЕДПРИЯТИЯ

Дадена за печат на 16.04.2010 г.
Печ. коли 20,5; формат 16/70/100; тираж 100 бр.

ISBN 978-954-23-0455-5