Григорий Бортэ,
Молдавская Экономическая Академия

СИСТЕМА ПРЕДОТВРАЩЕНИЯ УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Methods of data leak prevention in an organization are described in this article. It also offers several insider classifications and describes why are they to be concerned of. Methods of loss estimations are offered in the article as well.

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 демонстрация методов предотвращения утечки конфиденциальной информации из организации посредством сети Интернет, а также оценка убытков как от возможной утечки, так и от уже свершившейся.

Объектом исследования является информационная система предприятия, степень её защищённости, а также меры, предпринимаемые с целью предупреждения утечки информации.

Инсайдер – работник организации, имеющий доступ к конфиденциальной информации, не доступной другим лицам, или широкому кругу лиц, может нести потенциальную угрозу внутренней безопасности. Слово также может нести негативный оттенок. Например, лицо, опубликовавшее конфиденциальную информацию или передавшее её лицам, не имеющим доступ к данной информации.

Почему опасны инсайдеры?

- Имеют доступ к конфиденциальной информации.
- Знают внутренние нормы предприятия.
- Они обладают предоставленными работникам правами и полномочиями.

Чем опасны инсайдеры?

- Способны осуществить утечку конфиденциальной информации.
- Способны повредить информационную систему.
- Способны осуществить кражу личной информации.
- Способны превысить права и полномочия.
- Способны на противоправное использование прав и полномочий.
- Способны осуществить кражу техники.

Виды инсайдеров:

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

Согласно результатам исследования 2006 CSI/FBI Computer Crime and Security Survey[1] почти три четверти (74%) всех финансовых потерь вызваны четырьмя угрозами: утечкой конфиденциальной информации, кражей ноутбуков и мобильной техники, неавторизованным доступом и вирусными атаками.

Согласно результатам исследования, проведённого в России в 2006 году[2], внутренние угрозы беспокоят представителей ИТ-департаментов крупных государственных учреждений и частных компаний гораздо больше, чем внешние. Вредоносные программы находятся на третьем месте, уступив место краже информации и халатности сотрудников. Также выделяются саботаж и хакерские атаки. Больше всего опасаются нарушения конфиденциальности информации, то есть классической деятельности инсайдеров. Кражи информации (70,1%) руководство боится гораздо больше, нежели ее искажения (38,4%).

Опаснейшей угрозой является кража личной информации, которую аналитики Deloitte назвали «преступлением XXI века»[5]. Согласно исследованию «2006 Global Security Survey", защита от кражи личной информации и мошенничества со счетами являются двумя основными приоритетами, на которых большинство (58%) финансовых компаний сфокусируют свои усилия в следующем году.

Почему инсайдеры выдают информацию?

- Невнимательность и рассеянность.
- Желание заработать.
- Желание отомстить[3].

Почему возможна выдача информации?

- Уязвимости в программном обеспечении информационной системы.
- Непродуманность политики безопасности информационной системы.
- Человеческий фактор.
- Слабая законодательная база.

Оценка ущерба от действий инсайдеров.

Точно оценить ущерб от действий инсайдеров зачастую крайне сложно. Например, если работник банка «вынес» информацию о клиентах, то от этого последует как прямой, так и косвенный ущерб для банка. Прямой будет заключаться в исках от клиентов, прекращении действий контрактов, изъятия вкладов. Но намного сложнее оценить косвенный ущерб, который сложится из недополученной прибыли, в результате потери ряда клиентов. Также значительно пострадает репутация банка, и привлечение новых клиентов будет сильно затруднено.

Прямые затраты:

- Проведение расследования и выявление причины инцидента;
- Оповещение пострадавших в письменной форме;
- Организация помощи пострадавшим лицам;
- Оплата услуг консультантов по безопасности;
- Закупка и внедрение решений для минимизации риска аналогичных инцидентов;
- Оплата услуг юристов в случае судебных разбирательств;

- Проведение компании с целью успокоения общественного мнения;
- Выплата штрафов.

Косвенные затраты:

- Падение престижа и репутации фирмы в глазах существующих и потенциальных клиентов;
- Потеря ряда существующих клиентов;
- Затруднение в привлечении новых клиентов.

Согласно исследованию Ponemon Institute "2007 Annual Study: The Cost of data breach", более 56% ущерба приходится именно на косвенные затраты [6].

Как инсайдер может воспользоваться своим доступом? Во-первых, может использовать информацию сам. Во-вторых, может продать информацию третьим лицам с целью получения вознаграждения. Одно дело, когда поступил «заказ» на определённую информацию, другое – когда злоумышленник не знает, какую именно информацию он сможет продать. Встаёт два важных вопроса: «что украсть?» и «кому продать?». Ведь, покупая информацию, третье лицо рассчитывает на получение прибыли или каких-либо других выгод. Не всякая информация может быть интересна третьим лицам и не любая информация может быть интересна конкретному лицу. Наконец, инсайдер может использовать свой доступ в личных целях.

Ещё важен тот факт, что информацией могут воспользоваться не сразу. Утечка может выявиться только через определённый период времени. Это может уменьшить негативный эффект, а может и увеличить его.

Заключение.

На данный момент не существует панацеи от утечки информации, однако существует ряд мер по её предотвращению:

- 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] CSI/FBI Computer Crime And Security Survey http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf
[2] Алексей Доля. *Инсайдеры наступают*. http://www.citcity.ru/14874/
[3] *Уволенный сотрудник – угроза безопасности компании*. http://www.seclab.ru
[4] Вячеслав Лупанов. *Банки: почти каждый инсайдер уносит миллион* http://sb.adverman.com/modules/myarticles/article.php?storyid=3
[5] Данил Анисимов. *Сколько стоит банковский инсайдер*. http://www.pcweek.ru/spheres/detail.php?ID=111099&SPHERE_ID=13866