УДК 004.056.53

МОДЕЛИРОВАНИЕ УМЫШЛЕННОГО ВОЗДЕЙСТВИЯ ИНСАЙДЕРОВ НА ИНФОРМАЦИОННУЮ СИСТЕМУ

Закиров В.И.[1], Пономарев Д.Ю.[1,2]

[1] ФГАОУ ВПО Сибирский федеральный университет, Красноярск, Россия (660041, г. Красноярск, пр. Свободный, 79), e-mail: ponomarevdu@yandex.ru;
[2] ФГБОУ ВПО Сибирский государственный аэрокосмический университет им. акад. М.Ф. Решетнева, Россия (660014, г. Красноярск, пр. имени газеты «Красноярский рабочий», 31), e-mail: ponomarevdu@yandex.ru

В настоящее время проблема инсайдеров довольно слабо изучена и описана, между тем это один из наиболее опасных видов угроз для любой организации. Данное воздействие сложно контролировать, а зачастую даже невозможно. Инсайдер может украсть и передать данные конкурентам, а пропажа так и останется незамеченной. В данной статье мы рассмотрим модель действия сотрудника, который совершает кражу информации, с целью получения выгоды от ее последующего использования. Данному инсайдеру не всегда будет необходимо подключение к информационной системе, так как он может элементарно сделать копии или даже сфотографировать интересующий документ. Представленная модель будет учитывать этапы, необходимые для реализации воздействия, независимо от способа хищения данных и достаточно полно описывает последовательность действий сотрудника, поможет проанализировать, на каком этапе воздействия должно быть организовано наибольшее сопротивление, в зависимости от возможностей и желания работодателя. Данная модель должна позволить снизить вероятность появления подобной проблемы и увеличить общую защищенность информационной системы в целом.

Ключевые слова: информационная система, защита, безопасность, инсайдеры, злоумышленник, правонарушение, сети Петри-Маркова, функция распределения.

MODELING OF INTENTIONAL EXPOSURE OF INSIDERS TO INFORMATION SYSTEM

Zakirov V.I.[1], Ponomarev D.Y.[1,2]

[1] Siberian Federal University, Krasnoyarsk, Russia (660041, Krasnoyarsk, Svobodny pr., 79), e-mail: ponomarevdu@yandex.ru
[2] Siberian State Aerospace University named after academician M.F. Reshetnev (31, Krasnoyarsky Rabochy Av., Krasnoyarsk, Russia, 660014), e-mail: ponomarevdu@yandex.ru

Now insiders rather poorly understood and described, but this is one of the most dangerous threats for any organization. These effects are difficult to control, and often even impossible. Insiders can steal and pass the data of competitors, and the loss will go unnoticed. In this article, we consider a model of actions when insider steals information in order to obtain benefits from its further use. This insider does not always have to be connected to the information system and insider can make a copy of documents or even take a photo of the interesting information. The presented model will take into account the steps necessary to implement the impact, regardless of the method of data theft and adequately describes the sequence of actions the employee and can help analyze at what stage of the impact should be organized more security, depending on the capacity and willingness of the employer. This model should to reduce the likelihood of this problem and improve the overall security of the information system.

Keywords: information system, protection, security, insiders, attacker, offense, Petri-Markov nets, distribution function.

Информационные технологии становятся все более важной составляющей нашей жизни, и в настоящее время каждая сфера деятельности в той или иной степени компьютеризирована. При этом каждый пользователь готов использовать такие блага цивилизации, как Интернет, социальные сети, электронные платежи и другие действия, для которых необходима довольно сложная информационная система. Так же существуют локальные сети предприятий и глобальные порталы для взаимодействия между

организациями, где пользователем выступает уже сотрудник той или иной организации [3]. Но помимо удобства использования существует множество проблем. Например, в коммуникационной сети вращается огромное количество данных, которые желательно держать в неведении от других, а иногда их защита довольно четко оговорена в законодательстве. Данный процесс сложен, и требует привлечения квалифицированного персонала, способного уберечь конфиденциальную информацию. Особенно это актуально для банковских систем, порталов государственных услуг и других систем, занимающихся обработкой большого количества данных, способных нанести вред определенному человеку. Но помимо этого существует и другая конфиденциальная информация – коммерческая тайна, государственная тайна, информация для служебного пользования и так далее. В большинстве случаев защита направлена на внешние воздействия, и довольно скудно учитывает внутренние угрозы, а регулирование и защита от своих же сотрудников осуществляется лишь на уровне принятия необходимой документации, а также ознакомления работников с инструкциями, правилами и ответственностью за совершаемый проступок. Но настолько ли эффективны меры защиты информации от противоправных действий коллег и подчиненных путем утверждения определенного пакета документов, и насколько верно делать уклон на внешние воздействия [1]. Скорее всего, никто не станет переживать о поставленной подписи, так как отследить утечку данных во многих случаях просто не удастся, и инсайдер останется безнаказанным. Зачастую средства защиты применяются только при наличии требований со стороны законодательства, а сотрудники по умолчанию определяются как преданные и законопослушные. В частности, вся безопасность информационной системы может сводиться к применению антивирусного программного обеспечения и указанию ответственности в трудовом договоре, что слабо защитит от злоумышленника [3] любого типа и направленности.

Таким образом, повсеместное внедрение компьютерной техники, объединение ее в локальные и глобальные сети далеко не всегда сопровождается необходимыми мерами безопасности, что может повлечь самые печальные последствия.

Инсайдер в информационной системе

В большинстве организаций имеется ряд сотрудников, обладающих фактически неограниченным доступом к информационным системам. Так, сотрудники отдела информационных технологий могут обладать знаниями логинов и паролей, структуры системы, иметь доступ к электронным подписям сотрудников, а также обладать возможностью чистки всех возможных данных, включая информации о возможной утечке [1]. Наиболее пагубна ситуация, когда компьютерными технологиями занимается всего один человек, который так же с большой долей вероятности будет отвечать и за информационную

безопасность. Такой работник совершенно не ограничен в действиях, так как организует работу сети предприятия по своему усмотрению, а его ответственность в лучшем случае прописана в документации по защите информации. Но в случае его желания навредить будет довольно проблематично, а скорее всего даже невозможно доказать его причастность, при этом в большинстве случаев правонарушение просто останется не замеченным.

Угрозу также может предоставлять любой другой сотрудник организации, в особенности, при отсутствии контроля доступа к данным. Помимо информации, хранящейся на серверах, компьютерах и электронных носителях, зачастую важные документы хранятся в бумажном виде, и они могут представлять значительную ценность. Особенно это актуально при работе с документацией, имеющей гриф секретности или же отметки для служебного пользования. Но данный момент касается в основном государственных организаций, в которых проходят проверки, проводимые органами надзора. Такие учреждения тщательно готовятся к данным мероприятиям, но существует проблема, заключающаяся в огромных промежутках времени между проверками, исчисляющимися годами. Во время отсутствия надзора в организации могут иметь место значительные нарушения, которые могут негативно отразиться, главным образом, на ее руководителе. Вопрос о защите информации не теряет своей актуальности и для коммерческих учреждений. Каждая компания обрабатывает персональные данные сотрудников, и, в зависимости от деятельности, информацию о клиентах, что влечет за собой необходимость соблюдения законодательства в области защиты персональных данных [5]. Но это требования законов, и их необходимо выполнять, хотя в данном случае компания не получает никакой выгоды для себя. И в данном контексте защита информации становится просто еще одной статьей расходов. Другое дело – защита данных и документов, связанных с непосредственно работой учреждения, таких как планы, стратегии, рекламные акции, информация о наличии проблем в той или иной степени. Перехват подобной информации конкурентами может довольно серьезно отразиться на жизни организации, вплоть до ее полного исчезновения с рынка.

Таким образом, защита информации в сегодняшних условиях становится очень актуальным вопросом, на котором не стоит излишне экономить, а тем более пренебрегать им. Все это влечет за собой довольно большое количество предложений по организации безопасности информационных систем предприятий, направленных на защиту от внешних угроз. Многие меры достаточно действенны и не позволят легко получить доступ к данным извне.

Но так ли необходимо для конкурентов использование дорогостоящего труда группы программистов [3], с целью неправомерного получения заветной информации [1]? Скорее всего, нет. Так как в большинстве случаев можно найти человека из требуемой организации,

который имеет достаточно прав и возможностей для беспрепятственной кражи данных у своего работодателя. А самое главное, что, скорее всего, данный поступок останется незамеченным.

Услуги подобного инсайдера будут значительно удобней, а главное, финансово выгодней, чем работа профессиональной команды хакеров или других злоумышленников, особенно, если средства защиты от внешних угроз хорошо проработаны и грамотно реализованы. В добавление к этому, риски и ответственность во многом переходят на плечи самого инсайдера. То есть внутренний нарушитель является практически идеальным орудием в подобном деянии – он знает, что и где искать, не имеет проблем с доступом, финансово выгоден, его действия сложно отследить, снимает часть ответственности с нанимателя, и даже может иметь некий личный мотив, помимо желания наживы.

Модель умышленного воздействия инсайдера

Инсайдеры могут быть совершенно разными, и соответственно, приносимый вред в значительной степени будет отличаться [1]. Существует множество возможностей для подобной деятельности, при этом основная масса инсайдеров даже и не подозревает о том, что они являются таковыми. Большая часть нарушений происходит неосознанно, либо из-за пренебрежения правилами, которые кажутся сотруднику лишними, либо по неопытности и неосторожности, возникших по вине недостаточной квалификации или огрехов при обучении. Так же, безусловно, возможны случайности, от которых не застрахован ни один человек.

Но есть особая группа инсайдеров, которая предоставляет значительные сложности для компании. Эти сотрудники готовы на совершение правонарушений умышленно, с целью получения некой выгоды. Данная выгода может быть выражена в денежном эквиваленте, предоставлять инсайдеру новые возможности при смене работы, удовлетворять желание нанести вред своему начальству и компании, подставить коллегу и многое другое. Рассмотрим действия подобного инсайдера более подробно.

Совершение любого противоправного действия дело довольно рискованное и требует прохождения определенного количества этапов, начиная с желания нанести вред и заканчивая извлечением выгоды из своих действий.

Разработаем модель поведения инсайдера в информационной сети с применением математического аппарата сетей Петри-Маркова [4]. Основными объектами, чье поведение рассматривается в данной модели, будут: инсайдер, информационная система и данные, которыми хочет воспользоваться злоумышленник. Элементы сети обозначены следующим образом: S_j – позиции, t_i – переходы.

Для разработанной модели позиции и переходы могут быть определены как: S_1 – наличие мотивации и желания; t_1 – время принятия решения о готовности к правонарушению; S_2 – анализ рисков; t_2 – время, необходимое на анализ; S_3 – начало подготовительных мероприятий; t_3 – время подготовки; S_4 – вход в систему; S_5 – информационная система доступна и работоспособна; t_4 – время, необходимое для входа в систему; S_6 – поиск и получение доступа к данным; t_5 – время поиска; S_7 – данные найдены, проверка данных; t_6 – время проверки; S_8 – проверка окончена, копирование данных; t_7 – время копирования; S_9 – устранение следов правонарушения; t_8 – время устранения; S_{10} – использование данных; t_9 – время, необходимое на использование данных, в соответствии с поставленной целью; S_{11} – цель достигнута.

Вид данной сети, являющейся моделью поведения инсайдера в информационной сети предприятия или учреждения с вышеуказанными позициями и переходами, представлен на рисунке 1.

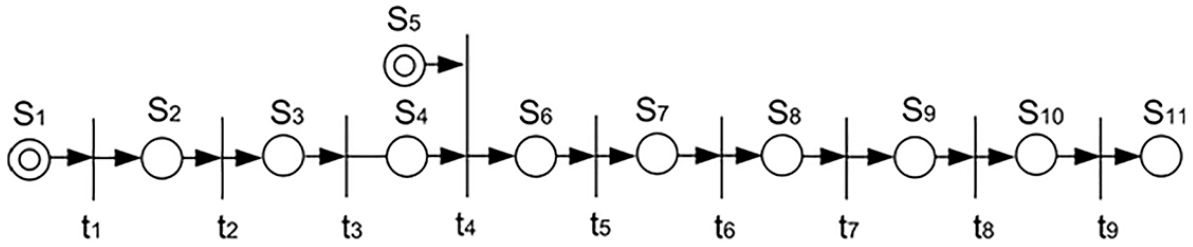

Рисунок 1. Модель умышленного воздействия инсайдера

Позиции не имеют инцидентных дуг, таким образом, вероятности перемещения из них в переходы будут равными единице [2].

Запишем матрицу, определяющую логические функции срабатывания сети (без учета направленности дуг графа):

$$V_{S_1t_9} = \begin{array}{c|cc|cc|ccccc} & t_1 & t_2 & & t_3 & t_4 & t_5 & t_6 & t_7 & t_8 & t_9 \\ \hline S_1 & 1 & 0 & & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ S_2 & 1 & 1 & & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ S_3 & 0 & 1 & & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ S_4 & 0 & 0 & & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ S_5 & 0 & 0 & 0 & & 1 & 0 & 0 & 0 & 0 & 0 \\ S_6 & 0 & 0 & 0 & S_4t_4 \bigcap S_5t_4 & & 1 & 0 & 0 & 0 & 0 \\ S_7 & 0 & 0 & & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ S_8 & 0 & 0 & & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ S_9 & 0 & 0 & & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ S_{10} & 0 & 0 & & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ S_{11} & 0 & 0 & & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}.$$

Для представленной сети Петри-Маркова срабатывание полушага из перехода в позицию происходит мгновенно, и динамика срабатывания сети будет определяться только вероятностью перемещения из состояния в переход, а также плотностью распределения времени нахождения процесса в каждом состоянии [2]. Таким образом, для данной сети достаточно рассмотреть процесс перехода из состояния S_1 в переход t_9.

Запишем систему интегро-дифференциальных уравнений, справедливую для данной сети:

$$\Phi_{S_1t_1}(t) = \pi_{11}\int_0^t f_{S_1t_1}(\tau)d\tau,$$

$$\Phi_{S_2t_2}(t) = \pi_{22}\int_0^t f_{S_2t_2}(\tau)\Phi_{S_1t_1}(t-\tau)d\tau,$$

$$\Phi_{S_3t_3}(t) = \pi_{33}\int_0^t f_{S_3t_3}(\tau)\Phi_{S_2t_2}(t-\tau)d\tau,$$

$$\Phi_{S_4t_4}(t) = \pi_{44}\int_0^t f_{S_4t_4}(\tau)\Phi_{S_3t_3}(t-\tau)d\tau,$$

$$\Phi_{S_5t_4}(t) = \pi_{54}\int_0^t f_{S_5t_4}(\tau)d\tau,$$

$$\Phi_4(t) = \int_0^t f_{S_4t_4}(\tau)\Phi_{S_5t_4}(\tau) + f_{S_5t_4}(\tau)\Phi_{S_4t_4}(\tau)d\tau,$$

$$\Phi_{S_6t_5}(t) = \pi_{65}\int_0^t f_{S_6t_5}(\tau)\Phi_4(t-\tau)d\tau,$$

$$\Phi_{S_7t_6}(t) = \pi_{76}\int_0^t f_{S_7t_6}(\tau)\Phi_{S_6t_5}(t-\tau)d\tau,$$

$$\Phi_{S_8t_7}(t) = \pi_{87}\int_0^t f_{S_8t_7}(\tau)\Phi_{S_7t_6}(t-\tau)d\tau,$$

$$\Phi_{S_9t_8}(t) = \pi_{98}\int_0^t f_{S_9t_8}(\tau)\Phi_{S_8t_7}(t-\tau)d\tau,$$

$$\Phi_{S_{10}t_9}(t) = \pi_{109}\int_0^t f_{S_{10}t_9}(\tau)\Phi_{S_9t_8}(t-\tau)d\tau,$$

где $f_{S_it_j}(\tau)$ – плотность распределения вероятности времени перемещения из состояния S_i к переходу t_j, $\Phi_{S_it_j}(t)$ – соответствующий закон распределения, π_{ij} – вероятность срабатывания перехода, причем вероятности срабатывания всех переходов на данной траектории не зависят от времени, вероятность перемещения по всей сети рассчитывается по формуле: $\pi_{рез} = \prod_{d_{ij}} \pi_{ij}$, где d_{ij} – все полушаги сети.

Данная модель описывает прохождение основных этапов при реализации умышленного воздействия инсайдера с целью получения выгоды, а также дано математическое описание данной модели, которое носит общий характер. Для более точного описание необходимо знание закона распределения, что представляет довольно большую сложность из-за особенностей человеческого фактора. Такое описание будет являться одной из тем будущих исследований в данном направлении.

Заключение

В ходе проделанной работы была предложена модель умышленного воздействия инсайдера на информационную систему с целью получения, построенная с использованием математического аппарата сетей Петри-Маркова. Приведена система интегро-дифференциальных уравнений для описания сети, которую, обладая необходимой информацией о законе распределения времени перемещения из состояния в переход, возможно применить при расчете времени прохождения этапов и вероятности реализации воздействия. Для дальнейшего исследования необходимо определить подходящий закон распределения, а также возможно усложнение модели, путем появления дополнительных переходов и состояний, которые более точно учитывают реальное поведение инсайдера. Этот процесс является весьма трудоемким, так как должен быть учтен в первую очередь человеческий фактор, и определено, от каких условий он будет зависеть.

Список литературы

1. Баранов В.А. Формализация определения понятия инсайдеров в вычислительных системах // Проблемы информационной безопасности. Компьютерные системы. – 2010. – №2. – С. 56-63.
2. Игнатьев В.М. Ларкин Е.В. Сети Петри-Маркова. Тула: Тульский государственный университет, 1997. – 163 с.
3. Защита от хакеров беспроводных сетей / Барнс К., Боутс Т., Ллойд Д. и др.– М.: Компания АйТи; ДМК-Пресс, 2005. – 480 с.
4. Радько Н. М., Скобелев И. О. Риск-модели информационно-телекоммуникационных систем при реализации угроз удаленного и непосредственного доступа. М.: РадиоСофт, 2010. – 232 с.
5. Федеральный закон от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) "О персональных данных" (27 июля 2006 г.)

Рецензенты:

Петров М.Н., д.т.н., профессор, ФГБОУ ВПО Сибирского государственного аэрокосмического университета им. акад. М.Ф. Решетнева, г. Красноярск;

Антамошкин А.Н., д.т.н., профессор, профессор кафедры САиИО ФГБОУ ВПО Сибирского государственного аэрокосмического университета им. акад. М.Ф. Решетнева, г. Красноярск.