Оценка вероятности поражения критичного документа при многоходовых социоинженерных атаках

А. А. Сулейманов[1], М. В. Абрамов[2], А. Л. Тулупьев[3]
Федеральное государственное бюджетное учреждение науки Санкт-Петербургский институт информатики и автоматизации Российской академии наук
Санкт-Петербургский государственный университет
[1]lex.suleimanov@gmail.com, [2]mva16@list.ru, [3]alexander.tulupyev@gmail.com

***Аннотация*. В данном материале освещается подход к анализу защищенности критичных документов в информационной системе компании при многоходовых социоинженерных атаках. Задача решается с использованием моделей комплекса «критичные документы – информационная система – пользователи – злоумышленник». Рассматриваются подходы к вычислению вероятности поражения критичных документов информационной системы. Предложены алгоритмы вычисления данных вероятностей путем анализа социального графа сотрудников компании.**

Ключевые слова: социоинженерные атаки; информационная безопасность; защита пользователя; защита информации; защита критичных документов; социальный граф; киберсоциальные системы

I. Введение

A. Объект исследования

В настоящее время многие компании подвергаются атакам на информационную безопасность, нацеленных компрометацию критичных документов. В результате этих атак компании терпят большие убытки [3], которые могут выражаться как финансово, так и репутационно. Обычно ущерб вызывается получением доступа злоумышленником к критичным документам [6]. Один из видов атак на информационную безопасность компании связан с применением методов социальной инженерии. Такие атаки называются социоинженерными, они не затрагивают технические аспекты получения доступа к критичным документам, а включают в себя различные манипулятивные воздействия на пользователей для этих целей. Зачастую атака на пользователя происходит не напрямую, а опосредованно, через нескольких пользователей [11]. Такие атаки называются многоходовыми. Важно оценивать защищённость критичных документов информационной системы при таких воздействиях. Оценка позволит сделать выводы о степени защищённости информационной системы компании, своевременно принять меры для повышения уровня безопасности. Данная статья посвящена решению проблемы оценки защищённости критичных документов при многоходовых социоинженерных атаках.

Работа выполнена в рамках проекта по государственному заданию СПИИРАН № 0073-2018-0001, при финансовой поддержке РФФИ, проект №18-37-00323; проект №18-01-00626

B. Предмет исследования

Предметом данного исследования является моделирование социоинженерных атак с помощью социальных графов взаимодействия сотрудников компании, основанном на комплексе моделей «критические документы – информационная система – пользователи – злоумышленник». Путем оценки вероятностей успешного проведения многоходовых социоинженерных атак на графе становится возможным определять наиболее вероятные траектории (некие множества сотрудников компании) проведения атак, что позволяет специализированным департаментам информационной безопасности принимать точечные меры по устранению угрозы взлома системы компании. Каждый сотрудник имеет доступ к ряду критичных документов, следовательно, имея влияние на него, злоумышленник получает доступ к этим документам. Информация об интенсивности взаимодействия сотрудников, использующаяся для оценки вероятности успешности социоинженерных атак извлекается из аккаунтов сотрудников в социальных сетях.

C. Цель исследования

Целью данного исследования является увеличение оперативности оценки вероятности поражения критичных документов информационной системы при многоходовых социоинженерных атаках. Для достижения цели решается задача построения алгоритма оценки вероятности успеха многоходовой социоинженерной атаки, основанного на анализе социального графа взаимодействия компании. В работе предложена реализация программного модуля прототипа комплекса программ, автоматизировано производящего расчёт оценок вероятности распространения атаки между пользователями, основанной на информации, извлекаемой из социальных сетей. Результатом же работы комплекса является список наиболее уязвимых к атакам участков информационной системы (путей в графе).

D. *Релевантные исследования*

Заделом для проведения данного исследования послужили наработки коллектива лаборатории теоретических и междисциплинарных проблем информатики СПИИРАН, посвященные проблеме анализа защищённости пользователей информационных систем от социоинженерных атак [7, 9–11]. Подход к оценке вероятности успеха многоходовой социоинженерной атаки был представлен в [9]. Однако, в данном подходе использовались экспертные оценки вероятности распространения влияния злоумышленника в системе компании (на дугах социального графа взаимодействия), что представляется ресурсозатратным, особенно для крупных компаний. Автоматизированная оценка распространения атаки (влияния) в информационной системе позволяет существенно повысить оперативность работы.

Помимо этого, были использованы результаты работ в других областях, связанных с оценками вероятности сложных событий [2, 4]. Данные материалы были использованы для разработки методики расчёта вероятности распространения влияния злоумышленника от одного пользователя к другому на основании информации об интенсивности их взаимодействия.

На данный момент уже исследованы вопросы поиска и идентификации аккаунтов сотрудников компании в социальной сети [5]. Также предложены методы оценки степени выраженности особенностей личности пользователя, как основы для построения профиля уязвимостей пользователя [1].

II. Алгоритм и его реализация

Данное исследование является частью общего проекта, посвященного разработке систем анализа защищённости пользователей информационных систем от социоинженерных атак и систем упреждающей диагностики. Существенная часть данных для оценки параметров моделей комплекса «критичные документы – информационная система – пользователи – злоумышленник» извлекается из аккаунтов сотрудников компании в социальных сетях. Ниже представлена последовательность действий с их пояснениями, исполняемая программным модулем.

A. *Построение социального графа*

Программный модуль на основе списка сотрудников компании, строит социальный граф, вершины которого сопоставляются сотрудникам компании, а дуги – их взаимодействию между собой [13–14]. Вершинам графа соотнесены числовые значения, характеризующие вероятность успеха прямой атаки злоумышленника на пользователей системы, основанные на их профилях уязвимостей [9]. Дугам социального графа взаимодействия сопоставлены вероятности успеха распространения социоинженерной атаки между сотрудниками. Данные вероятности основаны на агрегации сведений об интенсивности взаимодействия сотрудников в социальных сетях [8, 12].

B. *Разрежение социального графа*

Отметим, что для относительно крупных компаний, состоящих из более чем ста сотрудников, процесс анализа является весьма трудоемким процессом. Обработка таких графов требует больших вычислительных мощностей. Для снижения нагрузки предлагается производить разрежение графа.

Разрежение графа происходит путем исключения из графа дуг с низкими значениями вероятностей распространения атаки по ним. Сжатие может производиться на основе порогового значения, при котором отбрасываются все дуги, вероятность распространения влияния по которым менее заданного порога, возможен вариант сжатия по экспертным данным, при котором включаются только интересующие нас взаимоотношения сотрудников компании.

C. *Анализ социального графа*

Главным и финальным шагом работы программного модуля является анализ социального графа взаимодействия сотрудников с целью выявления наиболее вероятных траекторий распространения атаки (влияния) злоумышленника в информационной системе компании. Для этого был разработан ряд подходов к оценке вероятности поражения критических документов. Данные подходы отличаются в первую очередь логикой организации анализа, это вытекает из целей, которые ставятся перед программным модулем:

- найти уязвимости в системе;
- найти наиболее вероятные траектории взлома конкретного документа;
- найти возможные последствия взлома конкретного сотрудника/ряда сотрудников.

Далее предлагается подробное описание алгоритмов, с указанием их преимуществ и недостатков, области применения и результатов, которые они достигают.

III. Алгоритмы анализа графа

Представленные ниже алгоритмы анализа графа применяются к социальному графу взаимодействия сотрудников, являющемуся результатом работы программы на предыдущих этапах работы. Подробнее шаги этих алгоритмов в, реализованных в программном модуле описаны в [12–14]. В рамках данной статьи рассматриваются графы, о которых известно, что:

- вершины графа сопоставлены сотрудникам компании;
- дуги свидетельствуют о наличии взаимоотношений между сотрудниками достаточной интенсивности;
- числовые значения у вершин соответствуют вероятностям успеха прямых социоинженерных атак на пользователей;
- числовые значения у дуг соответствуют вероятностям распространения атаки интенсивности взаимодействия сотрудников друг с другом.

Существуют разные подходы к оценке вероятности поражения критичных документов. Можно считать, что если злоумышленник распространил своё влияние на пользователя, то он имеет доступ к его множеству документов. Пусть каждый i -ый сотрудник имеет доступ к некоторому множеству критичных документов CD^i. Притом $\mathrm{CD}^i \cap \mathrm{CD}^j = \varnothing, \forall i, j \in K_U, i \neq j$, где K_U – множество пользователей информационной системы. В соответствии с этим подходом вероятность поражения некоторого множества критичных документов при многоходовой социоинженерной атаке будет совпадать с вероятностью успеха атаки на пользователя, которая приведена в [8].

Существуют иные подходы, в соответствии с которыми распространение влияния на пользователя не гарантирует получение доступа к его множеству критичных документов. Т.е. получение доступа к критичным документам пользователя, на которого распространено влияние, будет носить вероятностный характер. Таким образом, вероятность поражения некоторого множества критичных документов при многоходовой атаке будет выражаться следующим образом $P = P_{l..i} P_{\mathrm{CD}^i}$, где $P_{l..i}$ – оценка вероятности успеха многоходовой социоинженерной атаки по цепочке пользователей от l до i, а P_{CD^i} – вероятность поражения критичных документов, доступных пользователю, на которого распространено влияние злоумышленника.

Отметим, что P_{CD^i}, вероятно, будет зависеть от профиля уязвимостей пользователя и профиля компетенций злоумышленника. Т.е. $P_{\mathrm{CD}^i} = F\left(\left(A_i, S\left(A_i\right)\right), \left(V_j, D\left(V_j\right)\right), Q\right)$, где A_i – вид атакующего воздействия злоумышленника, $S\left(A_i\right)$ – владением этим действием злоумышленника, V_j – уязвимость пользователя, $D\left(V_j\right)$ – степень выраженности этой уязвимости у пользователя, а Q – матрица пороговых значений вероятностей [7]. Вероятно, эта оценка будет зависеть от более широкого круга параметров, таких как эмоциональное состояние пользователя в момент атаки, уровень критичности документа, доступ к которому предпринимается попытка получить, потенциальный ущерб для компании при его утрате и др. Получение точного вида функции для оценки вероятности P_{CD^i} – предмет дальнейших исследований. В данной статье дальнейшие выкладки производятся для представленных моделей.

Для получения оценок $P_{l..i}$ необходимо агрегировать сведения, извлекаемые из социальных сетей. На основании этих сведения рассчитываются соответствующие оценки вероятности, которые служат основой для выявления наиболее критичных траекторий распространения атаки. Поиск таких траекторий осуществляется посредством анализа социального графа взаимодействия сотрудников компании. Рассмотрим алгоритмы анализа.

A. Поиск возможных векторов атаки на документ

Если мы рассмотрим сценарий, в котором нет информации о том, могли ли некоторые сотрудники уже подвергнуться атаке со стороны злоумышленника, но имеется информация о том, какие документы его интересуют, самым логичным будет рассматривать возможные векторы атак на документ, отталкиваясь от пользователей, имеющих к нему доступ.

Перед обходом графа первоначально следует провести подготовительный этап: необходимо упорядочить список сотрудников в порядке уменьшения их уязвимости к социоинженерным атакам. Это необходимо для получения промежуточных результатов работы программы, которые может использовать департамент информационной безопасности. Имея упорядоченный список сотрудников, программа может приступить к обходу графа.

Первый шаг – определение множества сотрудников, имеющих доступ к интересующим нас критичным документам и упорядочивание этого множества в порядке уменьшения уязвимости к манипулятивному воздействию.

Второй шаг – обход графа. Для каждого из интересующих нас сотрудников мы производим модифицированный обход графа в ширину. Модификация состоит в том, что из множества сотрудников, соединенных с рассматриваемой вершиной, мы приоритетно берем вершины, соответствующие сотрудникам, которые наиболее уязвимы к манипулятивному влиянию злоумышленника.

Третий шаг – проверка того, стоит ли учитывать взятую на предыдущем шаге связь или нет. Для этого необходимо вычислить итоговую оценку вероятности поражения критичного документа путем распространения влияния по данному пути. Высчитывается она по формуле:

$$\tilde{P}_{m-\ldots-i_k-\ldots-j} = P_m \prod_{k=1}^{n-1} \left(P_{i_k, i_{k+1}} P_{i_{k+1}}\right)$$

где $i_1 = m, i_n = j$, P_i – вероятность успешности атаки на i-ого сотрудника, если у злоумышленника есть на него выход, P_{ij} – вероятность выхода злоумышленника на пользователя j через пользователя i, если пользователь i уже успешно атакован.

Для отсева используется экспертно выданная оценка вероятности распространения влияния. Если вероятность социоинженерной атаки по сотрудникам, представленным путём в графе оказывается ниже оценки, то рассматриваемую вершину в результат мы не включаем. Обход проводится до тех, пока множество нерассмотренных ранее связанных вершин, не опустеет.

B. Поиск возможных векторов рапространения влияния от пользователя

Если мы обладаем информацией о том, что некий сотрудник/множество сотрудников уже подверглись атаке, тогда есть смысл определить возможные последствия взлома, путем определения множества сотрудников, которые могут подвергнуться манипулятивному

воздействию, а как следствие и множество критических документов.

Принцип работы данного алгоритма схож с описанным выше с той лишь разницей, что точка входа локализирована, а потому нам не нужно использовать упорядочивание вершин графа и мы можем делать обычный обход графа в ширину. Обход проводится до тех пор, пока множество вершин сотрудников, на которых может распространиться влияние злоумышленника не опустеет.

C. Общий поиск уязвимостей в информационной системе

В случае, если требуется провести общий анализ системы, то мы можем использовать полный обход графа. Для этого необходимо упорядочить вершины в порядке уменьшения значения уязвимости к манипулятивному воздействию.

Далее проводится полный обход графа в ширину для каждой вершины модифицированным алгоритмом. Если упростить, то мы применяем алгоритм, описанный в пункте *B* для каждой вершины графа. Путем применения усовершенствованного алгоритма обхода графа в ширину, программа может выдавать промежуточные результаты работы алгоритма в виде графов, с указанием уязвимых путей в графе, которые представляют собой последовательность применения манипулятивного воздействия на сотрудников компании.

IV. Заключение

В статье предложен подход к увеличению оперативности оценки защищённости критичных документов при многоходовых социоинженерных атаках. Рассмотрены алгоритмы анализа социального графа взаимодействия сотрудников в компании. Данные алгоритмы закладывают основу для разработки систем упреждающей диагностики и бэктрекинга инцидентов успешных социоинженерных атак. Подобные системы комплексного анализа защищённости пользователей информационных систем позволят лицам, принимающим решения, осуществлять своевременные меры по повышению уровня защищённости информационных систем.

Список литературы

[1] Bagretsov G.I., Shindarev N.A., Abramov M.V., Tulupyeva T.V. Approaches to development of models for text analysis of information in social network profiles in order to evaluate user's vulnerabilities profile //Soft Computing and Measurements (SCM), 2017 XX IEEE International Conference on. IEEE, 2017. P. 93-95.

[2] Bell D. C., Trevino R. A. Modeling HIV Risk [Epidemiology] // J. Acquir Immune Defic Syndr. 1999. Vol. 22, N 3. P. 280-287.

[3] Ponemon L. Cost of data breach study: Global analysis //Poneomon Institute sponsored by Symantec. 2013

[4] Samsonovich A. V. On a roadmap for the BICA Challenge // Biologically Inspired Cognitive Architectures. 2012. Т. 1. С. 100-107.

[5] Shindarev N., Bagretsov G., Abramov M., Tulupyeva T., Suvorova A. Approach to identifying of employees profiles in websites of social networks aimed to analyze social engineering vulnerabilities // Advances in Intelligent Systems and Computing. Proceedings of the Second International Scientific Conference "Intelligent Information Technologies for Industry" (IITI'17). Vol. 1. 2017. P.441-447.

[6] The Human Factor in IT Security: How Employees are Making Businesses Vul-nerable from Within [Электронный ресурс]// Kaspersky Lab. 2017. URL: https://www.kaspersky.com/blog/the-human-factor-in-it-security/ (дата обращения: 06.10.2017)

[7] Абрамов М.В., Азаров А.А., Тулупьева Т.В., Тулупьев А.Л. Модель профиля компетенций злоумышленника в задаче анализа защищённости персонала информационных систем от социоинженерных атак // Информационно-управляющие системы. 2016. №4. С. 77-84.

[8] Абрамов М.В., Тулупьев А.Л., Сулейманов А.А. Задача анализа защищённости пользователей от социоинженерных атак: построение социального графа по сведениям из социальных сетей // Научно-технический вестник информационных технологий, механики и оптики. 2018. № 2. С. 313–321.

[9] Азаров А.А., Тулупьева Т.В., Суворова А.В., Тулупьев А.Л., Абрамов М.В., Юсупов Р.М. Социоинженерные атаки: проблемы анализа. СПб.: Наука, 2016. 352 с.

[10] Мальчевская Е.А., Бирилло А.И., Харитонов Н.А., Золотин А.А. Развитие матрично-векторного подхода в алгоритмах локального априорного вывода в алгебраических байесовских сетях // Труды VII Всероссийской Научно-практической Конференции Нечеткие Системы, Мягкие Вычисления и Интеллектуальные Технологии (НСМВИТ-2017). Т. 1. С. 92-100.

[11] Суворова А.В., Тулупьева Т.В., Тулупьев А.Л., Сироткин А.В., Пащенко А.Е. Вероятностные графические модели социально-значимого поведения индивида, учитывающие неполноту информации // Труды СПИИРАН. 2012. Т. 3. №. 22. С. 101-112.

[12] Сулейманов А.А., Абрамов М.В. Автоматизация построения социального графа сотрудников компании на основе публикуемого ими контента в социальных сетях // Школа-семинар по искусственному интеллекту: сборник научных трудов. Тверь: ТвГТУ. 2018. С. 32-40.

[13] Сулейманов А.А., Абрамов М.В. Подход к построению и анализу социального графа сотрудников некоторой компании // Сборник научных трудов Первой Всероссийской научно-практической конференции (г. Ульяновск, 14-15 ноября, 2017 г.). Ульяновск, УлГТУ, 2017. С. 389-393

[14] Сулейманов А.А., Тулупьева Т.В., Тулупьев А.Л. Построение социального графа сотрудников компании на основании информации, получаемой из социальных сетей, для расчёта вероятности успеха социоинженерной атаки // Информационная безопасность регионов России (ИБРР-2017). X Санкт-Петербургская межрегиональная конференция. (Санкт-Петербург, 1-3 ноября 2017 г.): Материалы конференции. СПб: СПОИСУ, 2017. С. 431-432.