ПОДХОД К АНАЛИЗУ СОЦИАЛЬНОГО ГРАФА СОТРУДНИКОВ КОМПАНИИ С ЦЕЛЬЮ ПОВЫШЕНИЯ УРОВНЯ ЗАЩИЩЁННОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОТ СИА[1]

Хлобыстова А. О., м.н.с. лаб. ТиМПИ СПИИРАН, студентка кафедры информатики СПбГУ,
aok@dscs.pro

Абрамов М. В., с.н.с. с возложениями обязанностей заведующего лаб. ТиМПИ СПИИРАН, ст. преп. кафедры информатики СПбГУ
mva@dscs.pro

Аннотация

В данной статье рассматривается одна из задач общего направления исследований — анализа защищённости информационных систем от социоинженерных атак (СИА). Подход, рассматриваемый в данной статье, основывается на знании социального графа сотрудников компании, данных о критичности документов, имеющихся в информационной системе, и распределении прав доступа к ним. Как правило, существует несколько подходов к распределению уровня доступа к критичным документам. В настоящей работе рассматривается распределение прав доступа, при котором каждый пользователь имеет доступ к документам определённого уровня критичности и ко всем документам нижнего уровня. Для такого распределения прав предлагается подход к нахождению наиболее критичной траектории распространения многоходовой социоинженерной атаки и приводится пример её расчёта.

Введение

Уже долгое время одну из наиболее серьёзных угроз для безопасности организации представляют социоинженерные атаки (СИА) [1-4]. Данный факт находит своё подтверждение как в отчётах крупных компаний по информационной безопасности [1, 2], так и прослеживается в самих инцидентах по кибербезопасности [3, 4]. Ранее в [5, 6] были предложены

[1] Работа выполнена в рамках проекта по государственному заданию СПИИРАН № 0073-2019-0003 и при финансовой поддержке РФФИ (гранты №18-01-00626, № 18-37-00323)

подходы к получению вероятностных оценок защищенности критичных документов и пользователей информационной системы (ИС) от СИА. В данной статье предлагается принять во внимание ценность критичных документов, которая, как правило, в высшей степени гетерогенна. То есть возникает вопрос о поиске наиболее критичных траекторий атак не с точки зрения вероятности поражения пользователя или документа, а с точки зрения ожидаемого ущерба. Целью статьи является предложить подход к нахождению наиболее критичной траектории распространения многоходовой СИА при условии, что распределение прав доступа пользователей организовано следующим образом: каждый пользователь имеет доступ к документам определённого уровня критичности и ко всем документам уровня ниже. Пример ИС с таким распределением прав доступа представлен на рисунке 1: слева обозначены группы пользователей, а справа — критичные документы с указанием уровней критичности.

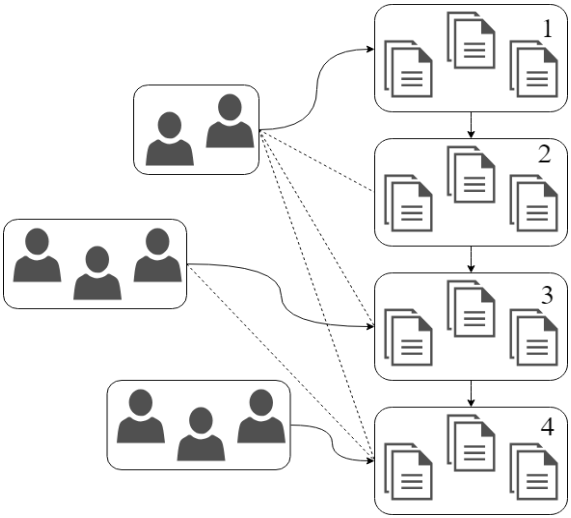

Рисунок 1: Пример ИС, в которой каждый пользователь имеет доступ к документам определённого уровня критичности и ко всем документам уровня ниже.

При этом для краткости будем предполагать, что нам доступна интегральная характеристика каждого пользователя по тому объему ущерба, нанесение которого можно ожидать, если злоумышленник сможет повлиять на пользователя в результате предпринимаемой социоинженерной атаки. Такая характеристика может быть построена на основе анализа возможностей и прав доступа пользователя к документам

различной критичности, однако алгоритмы ее синтеза являются предметом отдельного самостоятельного рассмотрения.

Нахождение наиболее критичной траектории распространения

Как было выявлено ранее в [5] вероятность прохождения атаки от пользователя m до пользователя l — это

$$p_{ml} = \underset{\text{Trajectories}}{\text{Max}} \left(p_m \prod_{i,j} p_{ij} \right),$$

где $\text{Trajectories} = \{(\text{User}_m, E_{i_1}, ..., E_{i_k}, \text{User}_l)\}_{i_1,...,i_k}$ — множество всевозможных траекторий распространения многоходовой социоинженерной атаки между заданными пользователями, p_m — оценка вероятности успеха прямой социоинженерной атаки злоумышленника на пользователя m, p_{ij} — соответствующая оценка вероятности распространения атаки на пользователя j через пользователя i. Отметим, что при $m = l$ данная оценка превращается в оценку вероятности прямой социоинженерной атаки на пользователя m.

Согласно [7] оценка вероятности поражаемости критичных документов при условии, что каждый пользователь имеет доступ к документам определённого уровня критичности и ко всем документам нижнего уровня, выглядит следующим образом:

$$H_{r+1} = 1 - (1 - H_r) \prod_{k \in K_{r+1}} (1 - P_k),$$

где K_{r+1} — множество пользователей, которые имеют доступ к документам уровня критичности $r+1$, P_k — оценка вероятности того, что пользователь будет успешно атакован злоумышленником, H_r — оценка вероятности того, что критичные документы уровня критичности r будут поражены. Для $r = 0$: $H_0 = 0$. Заметим, что в случае многоходовой СИА P_k будет совпадать с $\underset{\text{User}_k}{\text{Max}}(p_{mk})$.

Пусть каждому уровню критичных документов дана оценка ожидаемого ущерба от их компрометации. То есть документу d_i уровня критичности r сопоставлен потенциальный ущерб организации при его компрометации: $L_r^{d_i}$. Тогда введём метрику, характеризующую критичность

траектории как:

$$\mathrm{CL}_t = \underset{r,\, d_i, \mathrm{User}_m, \mathrm{User}_k}{\mathrm{Max}} \left(\left(1-(1-H_r) \prod_{k \in K_{r+1}} (1-p_{mk}) \right) \cdot L_r^{d_i} \right),$$

где p_{mk} — вероятность прохождения атаки от пользователя m до пользователя l, H_r — оценка вероятности того, что критичные документы уровня критичности r будут поражены, $L_r^{d_i}$ — потенциальный ущерб организации при компрометации документов уровня критичности r. Наиболее критичной траекторий распространения многоходовой СИА в таком случае будет являться: $\mathrm{CL} = \underset{t \in \mathrm{Trajectories}}{\mathrm{Max}} \left(\mathrm{CL}_t\right)$.

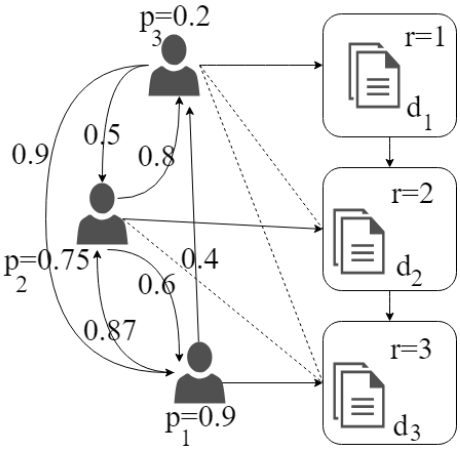

Рисунок 2: Пример социального графа сотрудников компании.

Для большей наглядности предложенной метрики рассмотрим пример, представленный на рисунке 2. Пусть дан социальный граф, состоящий из трех сотрудников компании, с указанными оценками вероятностей распространения социоинженерной атаки от пользователя к пользователю. Также представим, что критичные документы, содержащиеся в ИС, имеют три группы разных уровней критичности. Каждый пользователь имеет доступ к документу определённого уровня критичности и всем документам уровня критичности ниже. Зададим следующие значения для $L_r^{d_i}$: $L_1^{d_1} = 3$, $L_2^{d_2} = 2$, $L_3^{d_3} = 1$. Посчитаем, оценки вероятности того, что критичные документы уровня критичности r будут поражены:

$$H_1 = 1-(1-0.6264) = 0.6264,$$
$$H_2 = 1-(1-0.6264)\cdot(0.6264\cdot 0.75) = 0.82448272,$$
$$H_3 = 1-(1-0.82448272)\cdot(0.9\cdot 0.75\cdot 0.6264) = 0.9257877837.$$

Тогда оценка наиболее критичной траектории распространения многоходовой СИА будет рассчитываться как: $\mathrm{CL} = \mathrm{Max}\left((0.6264\cdot 3),(0.82448272\cdot 2),(0.9257877837\cdot 1)\right) = 1.8792.$

Таким образом, $\mathrm{CL}=\mathrm{CL}_t = 1.8792$, где $t = (\mathrm{User}_1, \mathrm{E}_{12}, \mathrm{E}_{23}, \mathrm{User}_3)$, что соответствует атаке на критичный документ d_1 уровня критичности 1 через пользователя 3, атакованного посредством пользователей 1 и 2.

Заключение

В настоящей работе рассматривается распределение прав доступа, при котором каждый пользователь имеет доступ к документам определённого уровня критичности и ко всем документам нижнего уровня. Для такого распределения прав предлагается подход к нахождению наиболее критичной траектории распространения многоходовой социоинженерной атаки и приводится пример её расчёта. Данное исследование, с одной стороны, может служить основой для дальнейших теоретических исследований траекторий распространения многоходовых СИА, а с другой, может быть применено в разрабатываемом программном комплексе по анализу уровня защищённости и опосредовано служить для принятия своевременных мер по повышению уровня защищённости. В качестве дальнейшего направления исследований предлагается рассмотреть моделирование успеха распространения многоходовых социоинженерных атак с использованием аппарата байесовских сетей [8, 9].

Литература

1. Protecting People: A Quarterly Analysis of Highly Targeted Cyber Attacks, Proofpoint, [Электронный ресурс] // URL: https://www.proofpoint.com/us/resources/threat-reports/quarterly-threat-analysis (Дата доступа: 20.01.2019).
2. Cybersecurity threatscape: Q4 2018, Positive technologies, [Электронный ресурс] // URL: https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Cybersecurity-threatscape-2018-Q4-eng.pdf (Дата доступа: 23.02.2019).
3. Russia lost 600 billion rubles due to hacker attacks in 2017, [Электронный ресурс] // URL: https://ria.ru/economy/20181016/1530769673.html (Дата доступа: 18.10.2018).

4. Schifferle L. W. Romance scams will cost you [Электронный ресурс] // URL: https://www.consumer.ftc.gov/blog/2019/02/romance-scams-will-cost-you (Дата доступа: 02.04.2019).
5. Абрамов М.В., Тулупьева Т.В., Тулупьев А.Л. Социоинженерные атаки: социальные сети и оценки защищенности пользователей. СПб.: ГУАП, 2018. 266 с. ISBN 978-5-8088-1377-5
6. Абрамов М. В., Тулупьев А. Л., Сулейманов А. А. Задачи анализа защищенности пользователей от социоинженерных атак: построение социального графа по сведениям из социальных сетей //Научно-технический вестник информационных технологий, механики и оптики. 2018. Т. 18. №. 2.
7. Абрамов М. В. Методы и алгоритмы анализа защищенности пользователей информационных систем от социоинженерных атак: оценка параметров моделей: дис. на соискание степени канд. тех. наук. Санкт-Петербург, СПИИРАН, 2018. 129-157 с.
8. Харитонов Н. А., Золотин А. А., Тулупьев А. Л. Глобальная непротиворечивость в алгебраических байесовских сетях: матрично-векторное представление условий непротиворечивости //ББК 32.973. 202я43 Н 59. – 2017. – С. 178.
9. Харитонов Н. А. Поддержание интернальной непротиворечивости алгебраических байесовских сетей с линейной и звездчатой структурой //Научно-технический вестник информационных технологий, механики и оптики. – 2018. – Т. 18. – №. 6.