РАНЖИРОВАНИЕ ТРАЕКТОРИЙ РАСПРОСТРАНЕНИЯ СИА В ЗАВИСИМОСТИ ОТ ОЖИДАЕМОГО УЩЕРБА[1]

Хлобыстова А. О., м.н.с. лаб. ТиМПИ СПИИРАН, студентка кафедры информатики СПбГУ,

aok@dscs.pro

Корепанова А. А., м.н.с. лаб. ТиМПИ СПИИРАН, студентка кафедры информатики СПбГУ,

aak@dscs.pro

Аннотация

Для анализа защищенности пользователей от многоходовых социоинженерных атак используются социальные графы сотрудников компании. Траектории распространения многоходовых социоинженерных атак можно ранжировать по вероятности прохождения по ним злоумышленником и по размеру ущерба, наносимого организации в случае их реализации. В данной статье предлагается метрика для оценки критичности траектории распространения многоходовой социоинженерной атаки, учитывающая подход к распределению документов, при котором каждый пользователь имеет доступ к документам какого-то одного уровня критичности.

Введение

Задача повышения уровня защищённости сотрудников организации от социоинженерного воздействия уже долгое время остаётся одной из наиболее актуальных в области информационной безопасности. Атаки, производимые с помощью методов социальной инженерии, с каждым годом становятся всё эффективнее и приносят существенный ущерб компаниям [1-6]. Независимо от используемых организацией программно-технических средств обеспечения информационной

[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)

безопасности, в конечном счёте работает с ней именно пользователь, который может преднамеренно или непреднамеренно произвести действия, способствующие успешному инциденту.

Часто в социоинженерную атаку бывают вовлечены сразу ряд пользователей информационной системы (ИС). Такие социоинженерные атаки, включающие в себя взлом более чем одного сотрудника, и при которых взломанные сотрудники непосредственно участвуют в компрометации последующих жертв называются многоходовыми социоинженерными атаками [7]. При анализе защищенности пользователей от многоходовых социоинженерных атак используются социальные графы сотрудников компании [8, 9, 10]. Как правило, можно выделить некоторое множество траекторий распространения многоходовых социоинженерных атак. Прохождение социоинженерной атаки злоумышленника по различным траекториям имеет разные вероятностные оценки и различно по размеру наносимого ущерба. Т.е. траектории распространения многоходовых социоинженерных атак можно ранжировать по вероятности их прохождения злоумышленником [11] и по размеру ущерба, наносимого организации в случае их реализации. Таким образом, актуальной видится задача выявления наиболее критичной траектории или множества траекторий распространения многоходовой социоинженерной атаки.

Предлагаемый подход

Заметим, что права доступа к критичным документам в разных информационных системах могут распределяться по-разному. В настоящей статье будет рассмотрен подход, при котором критичные документы разбиты по уровням критичности, а пользователи имеют доступ к определённому количеству критичных документов каждого уровня критичности и только к нему. Пример такой системы представлен на рисунке 1.

Ранее были проведены исследования, направленные на выявление наиболее вероятной траектории распространения социоинженерной атаки между двумя пользователями [7, 11]. Под наиболее вероятной траекторией в рамках проведённых исследований понималась траектория, включающая в себя набор дуг, произведение вероятностей распространения атаки по которым максимально. Более формально, согласно [7] под оценкой вероятности прохождения социоинженерной атаки между двумя пользователями понимается наиболее вероятная траектория прохождения атаки между этими пользователями. Иными словами, 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 j, p_{ij} — соответствующая оценка вероятности распространения атаки на пользователя j через пользователя i.

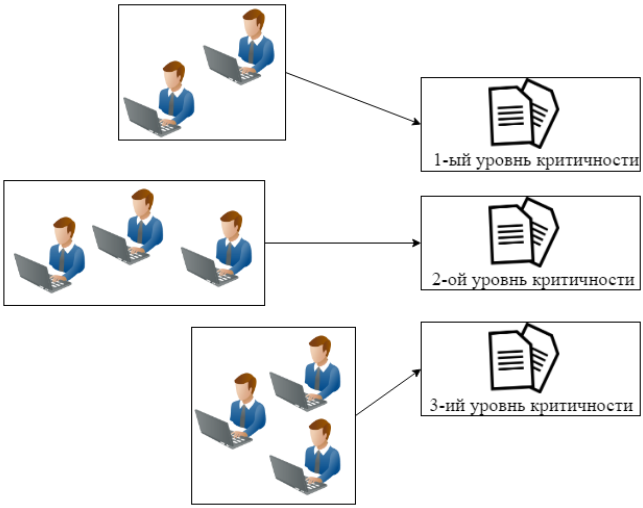

Рисунок 1: Пример распределения прав доступа в ИС

Как было отмечено выше, выявление наиболее вероятных траекторий без оценки ущерба от их реализации не даёт необходимой информации, которая позволила бы принимать своевременные меры, способствующие повышению уровня информационной безопасности в организации. В связи с этим, необходимо перейти от выявления наиболее вероятных траекторий к выявлению наиболее критичных траекторий. Наиболее критичной траекторией будем называть наиболее вероятную траекторию реализации социоинженерной атаки, которая принесёт максимальный ущерб организации. Для оценки критичности траекторий предлагается ввести соответствующую метрику, которая может быть формализована следующим образом

$$\mathrm{ct}_{\mathrm{ml}} = p_{\mathrm{ml}} \cdot \mathrm{loss}(\mathrm{l}, \mathrm{lc}),$$

где $\mathrm{ct}_{\mathrm{ml}}$ — оценка критичности траектории между пользователями m и l, p_{ml} — максимальная оценка вероятности прохождения социоинженерной атаки между данными пользователями, а $\mathrm{loss}(\mathrm{l}, \mathrm{lc})$ — потенциальный ущерб организации при компрометации критичных документов, доступных пользователю l, уровня критичности lc. Таким образом, необходимо найти траекторию ct: $\mathrm{ct} = \max_{\mathrm{User}_{\mathrm{m,l}} \in U} (\mathrm{ct}_{\mathrm{ml}})$.

Простейшим вариантом нахождения такой траектории является расчёт и ранжирование всевозможных вариантов значений $\mathrm{ct}_{\mathrm{ml}}$ для разных m и l. Однако указанный подход является ресурсозатратным. Для снижения ресурсозатратности можно двигаться в сторону сужения области перебора значений оценок вероятностей. Подобным фильтром может выступать задание нижнего порога для оценок вероятностей прохождения траекторий. А также задание порогового уровня критичности документа, убытка при его компрометации, при которых итоговое значение критичности траектории будет минимальным.

Заключение

В данной статье была предложена метрика для оценки наиболее критичной траектории распространения многоходовой социоинженерной атаки, учитывающая подход к распределению документов, при котором каждый пользователь имеет доступ к документам какого-то одного уровня критичности. В качестве дальнейшего развития направления исследований предполагается рассмотрение моделей, более детально описывающих контекст и учитывающих распределение вероятностей поражения доли документов, доступных пользователю, также в контексте данной задачи может быть рассмотрен аппарат байесовских сетей [12, 13].

Литература

1. Phishing campaign targets developers of Chrome extensions [Электронный] // URL: https://www.zdnet.com/article/phishing-campaign-targets-developers-of-chrome-extensions/, [дата просмотра: 08.10.2018].
2. One Coffee? Your Total Is Some Personal Data, [Электронный ресурс] // URL: http://nymag.com/selectall/2018/08/shiru-cafs-offer-students-free-coffee-for-harvested-data.html , [дата просмотра: 27.09.2018].

3. Cybersecurity threatscape: Q1 2018, [Электронный ресурс] // URL: https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2018-q1/ , [дата просмотра: 10.09.2018].
4. Cybersecurity threatscape: Q2 2018, [Электронный ресурс] // URL: https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2018-q2/, [дата просмотра: 20.10.2018].
5. The cyber-crooks became to withdraw money from the Russians' cards a new way, [Электронный ресурс] // URL: http://www.amur.info/news/2018/09/05/143017, [дата просмотра: 02.10.2018].
6. Russia lost 600 billion rubles due to hacker attacks in 2017, [Электронный ресурс] // URL: https://ria.ru/economy/20181016/1530769673.html, [дата просмотра: 18.10.2018].
7. 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
8. 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.
9. Абрамов М. В. Автоматизация анализа социальных сетей для оценивания защищённости от социоинженерных атак //Автоматизация процессов управления. – 2018. – №. 1. – С. 51.
10. Suleimanov A., Abramov M., Tulupyev A.: Modelling of the social engineering attacks based on social graph of employees communications analysis. // Proceedings of 2018 IEEE Industrial Cyber-Physical Systems (ICPS). — St.-Petersburg. — 2018. — pp. 801-805.
11. Khlobystova A.O., Abramov M.V., Tulupyev A.L. Identifying the most critical trajectory of the spread of a social engineering attack between two users // The Second International Scientific and Practical Conference "Fuzzy Technologies in the Industry – FTI 2018". CEUR Workshop Proceedings. — 2018. — pp. 38–43
12. 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.
13. 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.