Доверие и безопасность в информационном обществе

ПУБЛИЧНОСТЬ ОРГАНИЗАЦИИ КАК УЯЗВИМОСТЬ ПРИ ПРОВЕДЕНИИ СОЦИОИНЖЕНЕРНОЙ АТАКИ

Статья рекомендована к публикации членом редакционного совета А. А. Стрельцовым 30 мая 2023.

Хлобыстова Анастасия Олеговна

Санкт-Петербургский Федеральный исследовательский центр Российской академии наук
Санкт-Петербург, Российская Федерация
aok@dscs.pro

Абрамов Максим Викторович

Кандидат технических наук
Санкт-Петербургский Федеральный исследовательский центр Российской академии наук
Санкт-Петербург, Россия
mva@dscs.pro

Аннотация

Статья посвящена исследованию публичности организации, её широкой представленности в интернет-среде в качестве фактора, повышающего риски реализации социоинженерной атаки. Методы исследования основываются на отборе источников информации, которые могут быть задействованы злоумышленником на этапе «сбора информации» при совершении социоинженерной атаки, и построения на их основе сводного показателя оценки. Результатом исследования является математическая формализация параметров для оценки источников информации, а также построение на их основе сводной оценки, которая в свою очередь может лечь в основу новых моделей анализа успеха реализации социоинженерной атаки.

Ключевые слова

информационная безопасность; социоинженерные атаки; корпоративный сайт; параметры оценки

Введение

Интенсивная стадия развития информационного общества влечёт за собой повышение требований к обеспечению информационной безопасности. Одним из существенных рисков для кибербезопасности информационного общества в настоящее время является социальная инженерия [1, 2]. Сегодня существует большое количество различных систем, призванных снижать риски реализации программно-технических атак, но, как правило, в конечном счете с ними взаимодействует человек, которому свойственны свои уязвимости. Атаки на информационную систему организации, в рамках которых эксплуатируются уязвимости пользователей этой системы, называются социоинженерными [3, 4]. Социоинженерная атака (СИА) — набор прикладных психологических и аналитических приемов, которые злоумышленники применяют для скрытой мотивации пользователей публичной или корпоративной сети к нарушениям устоявшихся правил и политик в области информационной безопасности [3]. С каждым годом социоинженерные атаки происходят все чаще и наносят всё больший ущерб людям и организациям [4, 5]. В настоящее время разработан ряд подходов по повышению уровня защищённости как отдельных пользователей [6, 7], так и организаций в целом [3, 8–1615]. Однако существующие методы противодействия таким атакам [3, 6–16] не позволяют ликвидировать ассоциированные с социальной инженерией угрозы. Таким образом, есть потребность в модернизации существующих и создании новых методов анализа защищенности пользователей от социоинженерных атак, их обнаружения и противодействия им.

https://doi.org/10.52605/16059921_2024_01_85

Важным этапом в защите пользователей информационных систем от социоинженерных атак является анализ их защищенности. Анализ защищенности пользователей от социоинженерных атак позволяет наметить наиболее проблемные места в системе, дает информацию, необходимую для принятия мер по предотвращению инцидентов. В этой области уже есть наработки, формирующие подход к оценке защищенности пользователей от социоинженерных атак [3], но существуют ещё открытые задачи, на решение одной из которых направлена данная статья. При совершении социоинженерной атаки на первом этапе злоумышленники занимаются сбором информации об атакуемой системе и её пользователях [11]. Этот этап включает в себя определение потенциально полезных для совершения атаки источников информации, её непосредственный сбор, обработку и анализ [14, 15]. Сложность сбора и обработки сведений об информационной системе и её пользователях влияет на количество времени, требуемого для совершения социоинженерной атаки, и соответственно опосредованно на её успех. Чем сложнее найти необходимую информацию, тем больше времени требуется на ее поиск и, соответственно, тем ниже вероятность успеха атаки. При этом при анализе защищенности пользователей от СИА в моделях этап сбора информации не учитывается. Вместе с тем косвенная оценка уязвимости организации к СИА через анализ информации о ней, доступной в интернете, позволила бы иметь лицам, принимающим решения, больше индикаторов и рекомендация для соответствующих мер. Целью настоящей статьи является рассмотрение публичности организации, её широкой представленности в интернет среде в качестве фактора, повышающего риски реализации СИА.

1 Релевантные работы

Анализ литературы позволил выявить ряд различных подходов, направленных на повышение защищённости пользователей от социоинженерных атак [3, 6–15]. Среди них можно выделить работы, в которых предлагается строить профиль уязвимостей пользователя [3, 8–10], в том числе, в данных работах подчёркивается необходимость учёта свойств личности при анализе защищённости пользователей. Другая часть существующих работ [6, 7, 11] направлена на поиск факторов, влияющих на реакцию пользователей на социоинженерное воздействие злоумышленника. Также есть решения по анализу естественного языка в целях распознавания социоинженерных атак, когда анализируются сообщения, направленные пользователю, на предмет наличия в них социоинженерных угроз [12, 13]. В рамках этих исследований были отобраны ресурсы для извлечения информации о сценариях совершения атак. Авторами [12] было отобрано 20 веб-сайтов, форумов и книг, содержащих описание инцидентов, связанных с социальной инженерией, которые в свою очередь могут быть полезны в рамках текущего исследования для идентификации источников информации об организации, используемых злоумышленниками, в частности, в качестве источника выступали аккаунты организации в социальных медиа. В [14–16] представлены исследования, направленные на описание концептуальной модели социоинженерной атаки, берущие за основу для этого реальные сценарии социоинженерных атак. Представленные в работах [14, 15] модели, хоть и содержат в себе этап сбора сведений об атакуемой системе, не могут быть впрямую использованы при построении вероятностных оценок успеха социоинженерной атаки, так как требуют тщательной проработки и математической формализации. Авторы [16], основываясь на [14, 15], предлагают моделировать социоинженерную атаку как совокупность атомарных атакующих действий, формализуя концептуальную модель при помощи графа атак. Такой подход позволяет приблизиться к созданию автоматизированной системы по анализу защищённости от социоинженерных атак, однако не учитывает большое количество деталей (например, в этап подготовки атаки не включены действия злоумышленника, направленные на поиск информации об атакуемой организации/пользователе), что отрицательно влияет на качество предложенной модели. Таким образом, анализ существующих работ доказал актуальность исследований, посвящённых анализу источников информации, разработке критериев для оценки их критичности.

Для определения критериев, влияющих на успех социоинженерной атаки, важно изучить информацию о том, какие источники могут дать злоумышленникам наиболее ценные сведения при подготовке атаки. Понятно, что чем проще злоумышленнику будет собрать информацию об информационной системе, тем проще ему будет совершить атаку. Такие сведения часто упоминаются в аналитических статьях организаций, специализирующихся на информационной безопасности [17, 18]. Согласно анализу Лаборатории Касперского [17], социоинженерные атаки зачастую планируются с учетом особенностей конкретной жертвы, при этом то, насколько много

информации об атакуемом сотруднике удаётся найти, часто зависит от публичности атакуемого сотрудника. В качестве источников информации упоминаются следующие: корпоративный сайт организации (в частности, такая информация о сотрудниках как его контактные данные и биография), а также личные страницы сотрудников в социальных сетях. Консалтинговая компания в области информационной безопасности Social-Engineer, LLC [18] в качестве источников информации об организации и её сотрудниках описывает следующие: корпоративные сайты (в том числе: продукты и услуги, физическое месторасположение, вакансии, контактные телефоны, сведения о руководителе или топ-менеджерах, общедоступные отчёты), аккаунты сотрудников в социальных сетях (интересы/хобби, окружение, информация о семье), поиск в интернете (корпоративные документы, отношения с поставщиками, названия рабочих должностей, протокол адреса электронной почты, план здания).

2 Модель оценки доступности и информативности корпоративного сайта организации

Согласно анализу литературы, приведенному выше, одним из основных источников информации об организации является её корпоративный сайт. Чем больше на нем размещено различной информации, тем проще злоумышленнику подобрать «ключ» к сотрудникам организации — выбрать метод воздействия. Представляя на сайте максимально подробную информацию о компании и сотрудниках, лица, принимающие решения, часто не инвестируются в оценку социоинженерных рисков, таким образом порождаемых. Это не значит, что не нужно насыщать сайт информацией, — важно размещать информацию осмысленно, учитывая тот факт, что публичность организации — это с одной стороны важный аспект эффективности ее экономической деятельности, а с другой особенность, которая может быть использована как уязвимость при социоинженерной атаке. Несмотря на то, что сайты различных организаций очень сильно отличаются друг от друга, их представляется возможным оценить по наличию информации, полезной для злоумышленников. При этом важно проработать формализацию оценки доступности информации, которая бы подлежала дальнейшей автоматизации. Далее введем показатели, характеризующие представленность той или иной информации на сайте организации, и продемонстрируем пример расчета значений этих критериев для сайта конкретной организации.

1. C_1 — характеристика раздела «О компании» (или вариации «О нас» и т.п.), который включает в себя, как правило, цель компании, её миссию, историю, конкурентные преимущества, планы на будущее и др. Эта информация может давать сведения злоумышленникам о внутренних политиках, действующих в компании, ее ценностях и т.п. На текущем этапе для упрощения будем оценивать данную составляющую бинарно: $C_1 = 1$, если на сайте есть заполненный раздел «О компании» («О нас» или аналоги), $C_1 = 0$ — в противном случае. Значение этого параметра также можно рассматривать более гибко, оценивая наличие отдельных компонентов данного раздела.
2. C_2 — характеристика числа ссылок на социальные сети организации с ее сайта. $C_2=\frac{k}{n}$, где k — число ссылок на различные аккаунты в социальных сетях, n — число возможных ссылок на социальные медиа. Например, n может быть равно 3 в случае, если в качестве возможных ссылок рассматриваются ссылки на ВКонтакте, YouTube, Telegram.
3. C_3 — раздел «Новости» организации. «Новости» — $C_3 = 1$ при наличии данного раздела, в противном случае $C_3 = 0$.
4. C_4 — контакты организации. Для оценки контактов организации будем использовать взвешенную аддитивную свёртку набора критериев — $C_4 = \frac{1}{3}\sum_{i=1}^{3} C_{4i}$, где $\frac{1}{3}$ — нормирующий коэффициент, а C_{4i} обозначает один из следующих критериев:
   4.1. C_{41} — телефон. $C_{42} = 1$ при наличии, иначе 0;
   4.2. C_{42} — e-mail. $C_{42} = 1$ при наличии, иначе 0;
   4.3. C_{43} — адрес организации. $C_{43} = 1$ при наличии, иначе 0.
5. C_5 — информация о вакансиях. $C_5=\frac{k}{n}$, где k — количество различных вакансий. При этом, если вакансий больше 5, то будем считать $C_5 = 1$.
6. C_6 — информация о партнёрах. $C_6 = 1$ при наличии данного раздела, в противном случае $C_6 = 0$.

7. C_7 — информация о банковских реквизитах. $C_7 = 1$ при наличии данного раздела, в противном случае $C_7 = 0$.
8. C_8 — раздел «Сотрудники». Наполненность данного раздела предлагается рассчитывать на основе 7 различных критериев, взвешенная аддитивная свёртка по которым выглядит следующим образом: $C_8 = \frac{1}{10}\sum_{j=1}^{N}\left(\frac{1}{7}\sum_{i=1}^{7} C_{8i}^{j}\right)$, где N — количество сотрудников, информация о которых размещена на сайте организации ($N \leq 10$). При этом, если сотрудников больше 10, то среди всех сотрудников будут случайным образом выбраны 10. В случае отсутствия раздела «Сотрудники» $C_8 = 0$. Таким образом, в процессе расчёта оценки по каждому сотруднику организации сначала оценивается критерий C_{8i}^{j}, где i — номер критерия, приведённый ниже ($i = 1, \dots, 7$). Затем строится сводная оценка доступности и информативности информации по каждому сотруднику $\left(\frac{1}{7}\sum_{i=1}^{7} C_{8i}^{j}\right)$, на основе которых в свою очередь рассчитывается итоговая оценка по разделу «Сотрудники».
   8.1. C_{81}^{j} — указание должности/обязанностей. $C_{81}^{j} = 1$ при наличии, иначе 0;
   8.2. C_{82}^{j} — наличие фотографии. $C_{82}^{j} = 1$ при наличии, иначе 0;
   8.3. C_{83}^{j} — корпоративный телефон. C_{83}^{j}=1 при наличии, иначе 0;
   8.4. C_{84}^{j} — корпоративный e-mail. $C_{84}^{j} = 1$ при наличии, иначе 0;
   8.5. C_{85}^{j} — личный e-mail. $C_{85}^{j} = 1$ при наличии, иначе 0;
   8.6. C_{86}^{j} — ссылки на личные аккаунты в социальных сетях. C_{86}^{j}=1 при наличии, иначе 0;
   8.7. C_{87}^{j} — ссылки на личные мессенджеры. C_{87}^{j}=1 при наличии, иначе 0.

При построении итоговой модели оценок будем использовать метод сводных показателей [19], а именно взвешенное среднее арифметическое [20]. Тогда итоговая оценка доступности и полезности информации, размещённой на сайте организации, основывается на векторе значений критериев $(C_1, \dots, C_8)$ и имеет следующий вид: $C = \sum_{k=1}^{8} w_k C_k$, где w_k — весовые коэффициенты, учитывающие силу влияния показателя на успех атаки. Весовые коэффициенты будут рассчитываться индивидуально для каждой отрасли. В простейшем случае $w_k = \frac{1}{8}$. Если у организации нет сайта, то $C = 0$.

3 Пример расчёта оценки доступности и информативности корпоративного сайта организации

Применим представленную модель оценки доступности и информативности источников открытой информации к лаборатории теоретических и междисциплинарных проблем информатики «Санкт-Петербургского Федерального исследовательского центра РАН». Корпоративный сайт организации представлен по URL-адресу: https://dscs.pro/.

1. $C_1 = 1$ — характеристика раздела «О компании».
2. $C_2 = \frac{3}{3} = 1$ — характеристика числа ссылок на социальные сети организации с ее сайта (рассматриваются ссылки на ВКонтакте, YouTube, Telegram).
3. $C_3 = 1$ — раздел «Новости».
4. $C_4 = \frac{1}{3}(1 + 1 + 1) = 1$ — контакты организации. Так как:
   4.1. $C_{41} = 1$ — указан телефон.
   4.2. $C_{42} = 1$ — указан e-mail.
   4.3. $C_{43} = 1$ — указан адрес организации.
5. $C_5 = \frac{0}{5} = 0$ — на сайте отсутствует информация о вакансиях.
6. $C_6 = 0$ — на сайте отсутствует информация о партнёрах.
7. $C_7 = 0$ — на сайте отсутствует информация о банковских реквизитах.
8. C_8 — раздел «Сотрудники». На сайте представлена информация о более, чем 10 сотрудниках организации. Поэтому случайным образом были выбраны 10 из них. В таблице представлены

оценки C_{8i}^{j} по каждому из выбранных сотрудников. Итоговая оценка раздела «Сотрудники» рассчитывается следующим образом: $C_8 = \frac{1}{10}\left(\frac{6}{7}+\frac{6}{7}+\frac{6}{7}+\frac{6}{7}+\frac{5}{7}+\frac{5}{7}+\frac{5}{7}+\frac{5}{7}+\frac{4}{7}+\frac{3}{7}\right) = \frac{51}{70} \approx 0.729$.

Таблица 1. Расчёт критериев доступности и информативности по каждому сотруднику организации.

	C_{8i}^{1}	C_{8i}^{2}	C_{8i}^{3}	C_{8i}^{4}	C_{8i}^{5}	C_{8i}^{6}	C_{8i}^{7}	C_{8i}^{8}	C_{8i}^{9}	C_{8i}^{10}
C_{81}^{j}	1	1	1	1	1	1	1	1	1	1
C_{82}^{j}	1	1	1	1	1	1	1	1	1	1
C_{83}^{j}	1	1	1	1	1	1	1	1	1	1
C_{84}^{j}	1	1	1	1	1	1	1	1	0	0
C_{85}^{j}	0	0	0	0	0	0	0	0	1	0
C_{86}^{j}	1	1	1	1	1	1	1	1	0	0
C_{87}^{j}	1	1	1	1	0	0	0	0	0	0

Итоговая оценка информации, размещённой на сайте организации, основывается на векторе критериев $\left(1,1,1,1,0,0,0,\frac{51}{70}\right)$ и равна: $C = \frac{1}{8}\cdot 1+\frac{1}{8}\cdot 1+\frac{1}{8}\cdot 1+\frac{1}{8}\cdot 1+\frac{1}{8}\cdot 0+\frac{1}{8}\cdot 0+\frac{1}{8}\cdot 0+\frac{1}{8}\cdot\frac{51}{70} = \frac{331}{560} \approx 0.591$.

4 Выводы и дискуссия

Предложенная модель позволяет учитывать сложность сбора и анализа информации злоумышленником на этапе подготовки атаки, который в свою очередь оказывает влияние на дальнейший сценарий развития атаки. Так при недостаточном количестве собранных сведений, злоумышленнику будет сложнее инициировать и развить атаку. Однако, сбор большого числа сведений об организации и её сотрудниках не является гарантией успешной социоинженерной атаки, поэтому важно оценивать и уязвимость самих сотрудников к социоинженерным атакующим воздействиям. Вместе с тем не состоит упускать и тот факт, что публичность организации играет важнейшую роль в эффективности ее экономической деятельности, а именно помогает создать и повысить узнаваемость бренда, формирует и поддерживает репутацию организации, способствует расширению сети партнёров и обеспечению конкурентного преимущества. С этой точки зрения публичность является некой особенностью организации, которую нужно учитывать при создании систем обеспечения информационной безопасности. Учитывая данный факт, организации могут разработать меры безопасности, которые соответствуют их уникальным потребностям и особенностям.

В дальнейшем кроме сайта организации может быть оценена информация, доступная в социальных сетях. Так в [3] предлагаются инструменты автоматизированного поиска аккаунтов сотрудников компании в социальных сетях; также существует ряд работ по сопоставлению профилей пользователей в нескольких социальных сетях [21–24], подходы по восстановлению недостающих анкетных данных, например, по определению возраста пользователей [25], сопоставлению профилей пользователя в различных социальных сетях [26], классификации постов для последующего построения оценок защищённости пользователей от социоинженерных атак [27] или методики для оценки различных параметров поведения человека [28–30], которые могут быть задействованы при построении профиля уязвимостей пользователя. Дополнение данных результатов новыми наработками позволит решить проблему моделирования действий злоумышленника и анализа защищённости организации, учитывая информацию не только о сотрудниках организации, но и представленность самой организации в открытых источниках. Кроме того, в дальнейшем планируется детализация оценки отдельных критериев, связанной с оценкой ценности информации. Для этого будут рассмотрены методы распознавания именованных сущностей (для оценки текстового контента) и образов (для оценки графического контента).

Заключение

Результатом работы является формализация оценок значений параметров для оценки источников информации, а также построение на их основе сводных оценок, которые в свою очередь могут лечь

в основу новых моделей анализа успеха реализации социоинженерных атак. Полученные показатели могут быть использованы как при первичной диагностике организации к социоинженерным атакам, так и будут полезны при более детальном анализе и поиске конкретных уязвимостей. Что в свою очередь позволит лицам, принимающим решения, формировать целостное представление об имеющихся уязвимостях и, как следствие, принимать эффективные меры по их уменьшению. Кроме того, построенная модель оценки может быть использована для рейтингования по доступности и информативности информации различных организаций между собой, что в свою очередь даст возможность лицам, принимающим решения, своевременно узнавать об имеющихся проблемах и принимать меры по их минимизации.

Благодарности

Работа выполнена в рамках проекта по государственному заданию СПб ФИЦ РАН СПИИРАН № FFZF-2022-0003 (выделение критериев оценки доступности и информативности источников открытой информации, обзор существующих систем защиты организаций от социоинженерных атак, построение сводных оценок); при финансовой поддержке гранта Президента МК-5237.2022.1.6 (отбор источников информации, которые могут быть задействованы злоумышленником на этапе «сбор информации» при совершении социоинженерной атаки).

Литература

1. Snyman D., Kruger H. A. External contextual factors in information security behaviour // Proceedings of the 6th International Conference on Information Systems Security and Privacy (ICISSP 2020). 2020. P. 185–194. doi: 10.5220/0009142201850194
2. 21 Social Engineering Statistics — 2022. FirewallTimes. URL: https://firewalltimes.com/social-engineering-statistics/ (дата обращения 17.01.2023).
3. Абрамов М. В., Тулупьева Т. В., Тулупьев А. Л. Социоинженерные атаки: социальные сети и оценки защищенности пользователей. СПб.: ГУАП, 2018. 266 с.
4. Wang Z., Sun L., Zhu H. Defining social engineering in cybersecurity // IEEE Access. V. 8. P. 85094–85115. doi: 10.1109/ACCESS.2020.2992807
5. Salahdine F., Kaabouch N. Social engineering attacks: A survey // Future Internet. 2019. V. 11. № 4. P. 89. doi: 10.3390/fi11040089
6. Shahbaznezhad H., Kolini F., Rashidirad M. Employees' Behavior in Phishing Attacks: What Individual, Organizational, and Technological Factors Matter? // Journal of Computer Information Systems. 2020. V. 61. № 6. P. 539–550. doi: 10.1080/08874417.2020.1812134
7. Williams E. J., Hinds J., Joinson A. N. Exploring susceptibility to phishing in the workplace // International Journal of Human-Computer Studies. 2018. V. 120. P. 1–13. doi: 10.1016/j.ijhcs.2018.06.004
8. Ye Z., Guo Y., Ju A., Wei F., Zhang R., Ma J. A Risk Analysis Framework for Social Engineering Attack Based on User Profiling // Journal of Organizational and End User Computing (JOEUC). 2020. V. 32. № 3. P. 37–49. doi: 10.4018/JOEUC.2020070104
9. Wang Z., Zhu H., Sun L. Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods // IEEE Access. 2021. V. 9. P. 11895–11910. doi: 10.1109/ACCESS.2021.3051633
10. Тулупьева Т. В., Абрамов М. В., Тулупьев А. Л. Модель социального влияния в анализе социоинженерных атак // Управленческое консультирование. 2021. № 8 (152). С. 97–107. doi: 10.22394/1726-1139-2021-8-97-107
11. Steinmetz K.F., Pimentel A., Goe W.R. Performing social engineering: A qualitative study of information security deceptions // Computers in Human Behavior. 2021. V. 124. P. 106930. doi: 10.1016/j.chb.2021.106930
12. Tsinganos N., Mavridis I. Building and Evaluating an Annotated Corpus for Automated Recognition of Chat-Based Social Engineering Attacks //Applied Sciences. 2021. V. 11. № 22. P. 10871. doi: 10.3390/app112210871
13. Lansley M., Mouton F., Kapetanakis S., Polatidis N. SEADer plus plus: social engineering attack detection in online environments using machine learning //Journal of Information and Telecommunication. 2020. V. 4. № 3. P. 346–362. doi: 10.1080/24751839.2020.1747001

14. Mitnick K.D., Simon W.L. The art of deception: Controlling the human element of security. John Wiley & Sons, 2003. 351 p.
15. Mouton F., Leenen L., Venter H. S. Social engineering attack examples, templates and scenarios // Computers & Security. 2016. V. 59. P. 186–209. doi: 10.1016/j.cose.2016.03.004
16. Zheng K., Wu T., Wang X., Wu B., Wu C. A session and dialogue-based social engineering framework // IEEE Access. 2019. V. 7. P. 67781–67794. doi: 10.1109/ACCESS.2019.2919150
17. Гридасова А. Как злоумышленники собирают информацию для целевого фишинга. Проектная документация. «Лаборатория Касперского». URL: https://www.kaspersky.ru/blog/spearphishers-information/22228/ (дата обращения 17.01.2023).
18. Technical Methods of Information Gathering. Security through education. URL: https://www.social-engineer.org/framework/information-gathering/technical-methods-of-information-gathering/ (дата обращения 17.01.2023).
19. Хованов Н. В. Анализ и синтез показателей при информационном дефиците. СПб.: изд-во СПб ун-та, 1996. 196 с.
20. Хованов Н.В., Федотов Ю.В. Модели учета неопределенности при построении сводных показателей эффективности деятельности сложных производственных систем. Научные доклады. СПб.: НИИ менеджмента СПбГУ, 2006. № 28(R). 37 с.
21. Nurgaliev I., Qu Q., Bamakan S.M.H., Muzammal, M. Matching user identities across social networks with limited profile data // Frontiers of Computer Science. 2020. V. 14. № 6. P. 1–14. doi: 10.1007/s11704-019-8235-9
22. Srivastava D.K., Roychoudhury B. Words are important: A textual content-based identity resolution scheme across multiple online social networks // Knowledge-Based Systems. 2020. V. 195. P. 105624. doi: 10.1016/j.knosys.2020.105624
23. Wang L., Hu K., Zhang Y., Cao S. Factor Graph Model Based User Profile Matching Across Social Networks // IEEE Access. 2019. V. 7. P. 152429–152442. doi: 10.1109/ACCESS.2019.2948073
24. Li Y., Zhang Z., Peng Y., Yin H., Xu Q. Matching user accounts based on user generated content across social networks // Future Generation Computer Systems. 2018. V. 83. P. 104–115. doi: 10.1016/j.future.2018.01.041
25. Oliseenko V., Korepanova A. How old users are? Community analysis // CEUR Workshop Proceedings. RWTH Aahen University, 2020. V. 2782. P. 246–251.
26. Korepanova A. A., Oliseenko V. D., Abramov M. V. Applicability of similarity coefficients in social circle matching // 2020 XXIII International Conference on Soft Computing and Measurements (SCM). IEEE, 2020. P. 41–43. doi: 10.1109/SCM50615.2020.9198782
27. Oliseenko V.D., Tulupyeva T.V. Neural network approach in the task of multi-label classification of user posts in online social networks // 2021 XXIV International Conference on Soft Computing and Measurements (SCM). IEEE, 2021. P. 46–48. doi: 10.1109/SCM52931.2021.9507148
28. Социальные сети в России: цифры и тренды, осень 2021. Brand Analytics. URL: https://br-analytics.ru/blog/social-media-russia-2021/(дата обращения 11.01.2023)
29. Toropova A., Tulupyeva T. Comparison of Behavior Rate Models Based on Bayesian Belief Network // International Scientific and Practical Conference in Control Engineering and Decision Making. Springer, Cham, 2020. P. 510–521. doi: 10.1007/978-3-030-65283-8_42
30. Toropova A. V., Tulupyeva T. V. Approbation of the Behavior Rate Model with Hidden Variables Based on Respondents' Data on Recent Instagram Posts // 2021 XXIV International Conference on Soft Computing and Measurements (SCM). IEEE, 2021. P. 43–45.

PUBLICITY OF THE ORGANISATION AS A VULNERABILITY FACTOR IN A SOCIAL ENGINEERING ATTACK

Khlobystova, Anastasia Olegovna

St. Petersburg Federal Research Center of the Russian Academy of Sciences
Saint Petersburg, Russian Federation
aok@dscs.pro

Abramov, Maxim Viktorovich

Candidate of engineering sciences
St. Petersburg Federal Research Center of the Russian Academy of Sciences
Saint Petersburg, Russian Federation
mva@dscs.pro

Abstract

The article is devoted to the study of publicity of an organization, its wide representation in the Internet environment as a factor that increases the risks of implementing a social engineering attack. The research methods are based on the selection of information sources that can be engaged by an attacker at the stage of "information gathering" in the commission of a social engineering attack, and the construction on their basis of a composite assessment indicator. The result of the study is a mathematical formalization of parameters for assessing the sources of information, as well as the construction of a composite score based on them, which in turn can form the basis of new models of analysis of the success of the implementation of a social engineering attack.

Keywords

information security; social engineering attacks; corporate website; evaluation parameters

References

1. Snyman D., Kruger H. A. External contextual factors in information security behaviour // Proceedings of the 6th International Conference on Information Systems Security and Privacy (ICISSP 2020). 2020. P. 185–194. doi: 10.5220/0009142201850194
2. 21 Social Engineering Statistics — 2022. FirewallTimes. URL: https://firewalltimes.com/social-engineering-statistics/ (last access 17 Jan 2023).
3. Abramov M. V., Tulupyeva T. V., Tulupyev A. L. Sotsioinzhenernyye ataki: sotsial'nyye seti i otsenki zashchishchennosti pol'zovateley. SPb.: GUAP, 2018. 266 p.
4. Wang Z., Sun L., Zhu H. Defining social engineering in cybersecurity // IEEE Access. V. 8. P. 85094–85115. doi: 10.1109/ACCESS.2020.2992807
5. Salahdine F., Kaabouch N. Social engineering attacks: A survey // Future Internet. 2019. V. 11. № 4. P. 89. doi: 10.3390/fi11040089
6. Shahbaznezhad H., Kolini F., Rashidirad M. Employees' Behavior in Phishing Attacks: What Individual, Organizational, and Technological Factors Matter? // Journal of Computer Information Systems. 2020. V. 61. № 6. P. 539–550. doi: 10.1080/08874417.2020.1812134
7. Williams E. J., Hinds J., Joinson A. N. Exploring susceptibility to phishing in the workplace // International Journal of Human-Computer Studies. 2018. V. 120. P. 1–13. doi: 10.1016/j.ijhcs.2018.06.004
8. Ye Z., Guo Y., Ju A., Wei F., Zhang R., Ma J. A Risk Analysis Framework for Social Engineering Attack Based on User Profiling // Journal of Organizational and End User Computing (JOEUC). 2020. V. 32. № 3. P. 37–49. doi: 10.4018/JOEUC.2020070104
9. Wang Z., Zhu H., Sun L. Social Engineering in Cybersecurity: Effect Mechanisms, Human Vulnerabilities and Attack Methods // IEEE Access. 2021. V. 9. P. 11895–11910. doi: 10.1109/ACCESS.2021.3051633
10. Tulupyeva T. V., Abramov M. V., Tulupyev A. L. Model' sotsial'nogo vliyaniya v analize sotsioinzhenernykh atak // Upravlencheskoye konsul'tirovaniye. 2021. № 8 (152). C. 97–107. doi: 10.22394/1726-1139-2021-8-97-107

11. Steinmetz K.F., Pimentel A., Goe W.R. Performing social engineering: A qualitative study of information security deceptions // Computers in Human Behavior. 2021. V. 124. P. 106930. doi: 10.1016/j.chb.2021.106930
12. Tsinganos N., Mavridis I. Building and Evaluating an Annotated Corpus for Automated Recognition of Chat-Based Social Engineering Attacks //Applied Sciences. 2021. V. 11. № 22. P. 10871. doi: 10.3390/app112210871
13. Lansley M., Mouton F., Kapetanakis S., Polatidis N. SEADer plus plus: social engineering attack detection in online environments using machine learning //Journal of Information and Telecommunication. 2020. V. 4. № 3. P. 346–362. doi: 10.1080/24751839.2020.1747001
14. Mitnick K.D., Simon W.L. The art of deception: Controlling the human element of security. // John Wiley & Sons, 2003. 351 p.
15. Mouton F., Leenen L., Venter H. S. Social engineering attack examples, templates and scenarios // Computers & Security. 2016. V. 59. P. 186–209. doi: 10.1016/j.cose.2016.03.004
16. Zheng K., Wu T., Wang X., Wu B., Wu C. A session and dialogue-based social engineering framework // IEEE Access. 2019. V. 7. P. 67781–67794. doi: 10.1109/ACCESS.2019.2919150
17. Gridasova A. Kak zloumyshlenniki sobirayut informatsiyu dlya tselevogo fishinga. Proyektnaya dokumentatsiya. “Kaspersky Lab”. URL: https://www.kaspersky.ru/blog/spearphishers-information/22228/ (last access 17 Jan 2023).
18. Technical Methods of Information Gathering. Security through education. URL: https://www.social-engineer.org/framework/information-gathering/technical-methods-of-information-gathering/ (last access 17 Jan 2023).
19. Khovanov N.V. Analiz i sintez pokazateley pri informatsionnom defitsite. SPb.: SPbU publ., 1996. 196 p.
20. Khovanov N.V., Fedotov Y.V. Modeli ucheta neopredelennosti pri postroyenii svodnykh pokazateley effektivnosti deyatel'nosti slozhnykh proizvodstvennykh sistem. Nauchnyye doklady. SPb.: Research Institute of Management, SPbU, 2006. № 28(R). 37 p.
21. Nurgaliev I., Qu Q., Bamakan S.M.H., Muzammal, M. Matching user identities across social networks with limited profile data // Frontiers of Computer Science. 2020. V. 14. № 6. P. 1–14. doi: 10.1007/s11704-019-8235-9
22. Srivastava D.K., Roychoudhury B. Words are important: A textual content-based identity resolution scheme across multiple online social networks // Knowledge-Based Systems. 2020. V. 195. P. 105624. doi: 10.1016/j.knosys.2020.105624
23. Wang L., Hu K., Zhang Y., Cao S. Factor Graph Model Based User Profile Matching Across Social Networks // IEEE Access. 2019. V. 7. P. 152429–152442. doi: 10.1109/ACCESS.2019.2948073
24. Li Y., Zhang Z., Peng Y., Yin H., Xu Q. Matching user accounts based on user generated content across social networks // Future Generation Computer Systems. 2018. V. 83. P. 104–115. doi: 10.1016/j.future.2018.01.041
25. Oliseenko V., Korepanova A. How old users are? Community analysis // CEUR Workshop Proceedings. RWTH Aahen University, 2020. V. 2782. P. 246–251.
26. Korepanova A. A., Oliseenko V. D., Abramov M. V. Applicability of similarity coefficients in social circle matching // 2020 XXIII International Conference on Soft Computing and Measurements (SCM). IEEE, 2020. P. 41–43. doi: 10.1109/SCM50615.2020.9198782
27. Oliseenko V.D., Tulupyeva T.V. Neural network approach in the task of multi-label classification of user posts in online social networks // 2021 XXIV International Conference on Soft Computing and Measurements (SCM). IEEE, 2021. P. 46–48. doi: 10.1109/SCM52931.2021.9507148
28. Sotsial'nyye seti v Rossii: tsifry i trendy, osen' 2021. Brand Analytics. URL: https://br-analytics.ru/blog/social-media-russia-2021/ (last access 11 Jan 2023).
29. Toropova A., Tulupyeva T. Comparison of Behavior Rate Models Based on Bayesian Belief Network // International Scientific and Practical Conference in Control Engineering and Decision Making. Springer, Cham, 2020. P. 510–521. doi: 10.1007/978-3-030-65283-8_42
30. Toropova A. V., Tulupyeva T. V. Approbation of the Behavior Rate Model with Hidden Variables Based on Respondents' Data on Recent Instagram Posts // 2021 XXIV International Conference on Soft Computing and Measurements (SCM). IEEE, 2021. P. 43–45.