Подход к оценке вероятности успешности социоинженерной атаки[1]

Абрамов М.В., м.н.с. лаб. ТиМПИ СПИИРАН, м.н.с. лаб. социального компьютинга ИПИ МПГУ,

аспирант каф. информатики СПбГУ,
mva16@list.ru;
Санкт-Петербургский Государственный Университет
Санкт-Петербург, Россия

Аннотация

Обеспечение конфиденциальности корпоративных данных является актуальной проблемой в современном мире. Большое внимание специалистов области обеспечения информационной безопасности уделено защите программно-технических компонент информационной системы, в то время как пользователи информационной системы остаются без внимания и могут нарушить конфиденциальность корпоративных данных. В статье рассмотрено дополнение комплекса «информационная система — персонал — критичные документы» с помощью профиля компетенци злоумышленника.

Введение

За счёт глубокого проникновения информационных технологий в жизнь людей проблема обеспечения информационной безопасности стала очень актуальной. В последнее время атаки на информационные системы стали происходить чаще, приносить большие убытки и требовать больше ресурсов и времени для установления виновных в подобных преступлениях. Исследование 2014 года с участием компаний из США, охватившее семь стран, показало, что средний размер убытков американских компаний от киберпреступлений вырос более чем на 9%, до 12,7 миллиона долларов. В исследовании за 2013 год эта цифра составляла 11,6 миллиона долларов. Среднее время, необходимое для расследования атаки на информационные системы, также выросло. Теперь оно составляет 45 дней по сравнению с 32 днями в 2013

[1]Статья содержит материалы исследований, частично поддержанных грантами РФФИ 14-01-00580, 15-01-09001-а.

году [16]. В настоящее время большая часть исследований посвящена усовершенствованию технической базы, осуществляющей контроль информационной безопасности [7, 8]. Под термином «информационная безопасность» зачастую понимается защита информации с использованием программных, аппаратных и программно-ашпаратных решений [6]. В тоже время человеческий фактор играет существенную роль в системе защиты информации [9, 10]. Пользователь информационной системы, к данным которой злоумышленник пытается получить доступ, является одним из ее самых уязвимых мест [12, 15]. Сотрудник компании, имеющий доступ к конфиденциальной информации, может преднамеренно или непреднамеренно нарушить её безопасность (конфиденциальность, целостность или доступность) [14]. В [5] отмечается, что санкционированный пользователь информационной системы, вероятнее всего, знаком с рядом сотрудников, обслуживающих и администрирующих информационную систему; имеет ряд разрешений на доступ к документам, хранящимся в информационной системе; может знать парольную информацию коллег; обладает физическим доступом к некоторым компьютерам. В саязи с этим, взаимодействие пользователей информационной системы со злоумышленниками может нанести серьёзный ущерб компании. Ущерб от успешной атаки на информационную систему может приводить к серьёзным последствиям. Одним из ярких примеров уязвимости информационной системы последнего времени может служить похищение Эдвардом Сноуденом 1.7 млн секретных файлов специальных служб США [11]. Таким образом, проблема защиты пользователей от социоинженерных атак в настоящее время очень актуальна. Исследования в этой области помогут в создании многоуровневых систем безопасности, устойчивых к атакам злоумышленников. В статье рассмотрена модель анализа защищённости персонала информационных систем от социоинженерных атак, с учетом профиля компетенций злоумышленника.

Комплекс «информационная система — персонал — критичные документы»

В работе [1] были представлены компоненты моделей, входящих в комплекс «ИСПКД». Информационная система в этом комплексе включает в себя программно-технические устройства. В качестве моделей таких устройств могут выступать [13]:

- ПК и различные периферийные устройства;

- сетевые адаптеры для ПК и сетевые кабели;
- сетевое оборудование, такое как концентраторы и коммутаторы, которые соединяют между собой ПК и принтеры.

Каждой из моделей таких устройств сопоставлены модели информационных объектов (критичных документов), которые хранятся на этих устройствах или которые могут быть доступны через указанные устройства. Также в систему включена модель персонала информационной системы. Подобные модели охарактеризованы различными показателями, такими как различные права доступа, должность и ряд других характеристик. Кроме того, каждая модель сотрудника информационной системы содержит профиль уязвимостей пользователя [2, 3, 4].

Комплекс «критичные документы — информационная система — персонал — злоумышленник»

В работе [1] были предложены две модели имитации социоинженерных атак злоумышленника на пользователей информационной системы: на социальном графе пользователей и в комплексе «ИСПКД». Данные модели дают оценку защищённости пользователей от социоинженерных атак злоумышленника на основе связей между пользователями, в тоже время в данных моделях не учитывается профиль компетенции злоумышленника. Предлагается рассмотреть комплекс «критические документы — информационная система — персонал — злоумышленник» (комплекс «КДИСПЗ») вместо комплекса «ИСПКД», который позволит увеличить точность оценки защищенности пользователей информационных систем от социоинженерных атак за счёт вероятностных оценок действий злоумышленника. Профиль компетенций злоумышленника имеет большое значение наравне с профилем уязвимости пользователя для оценки успешности атакующего воздействия. Профиль компетенции злоумышленника может быть охарактеризован ресурсами, доступными злоумышленнику, а также известными злоумышленнику социоинженерными атакующими воздействиями. В качестве ресурсов могут выступать время на проведение социоинженерного атакующего воздействия, финансовые ресурсы для осуществления подкупа персонала и ряд других характеристик.

Тогда профиль компетенции злоумышленника может быть представлен в виде: $((R_1, D(R_1)), ..., (R_k, D(R_k)))$, где R_i — это ресурс, а

$D(R_i)$ — выраженность ресурса, его количество.

Для каждого злоумышленника строится свой профиль компетенций, то есть свой набор ресурсов. В качестве ресурсов будем считать деньги, время, знания социоинженерных атакующих воздействий. Таким образом, для каждого злоумышленника j профиль компетенций будет состоять из ресурсов и их количества $((R_1, D_j(R_1)), ..., (R_k, D_j(R_k)))$. Формализовав таким образом профиль компетенций злоумышленника, можно в простейшем случае, без учёта профиля уязвимостей пользователя перейти к оценкам вероятности p_{ij} , которые представляются следующим образом:

$$\underline{p_{ij} = D_j(R_i)}$$
$$M_i$$

, где $D_j(R_i)$ — выраженность ресурса R_i у злоумышленника j, M_i — максимальная выраженность данного ресурса, а p_{ij} — вероятность успеха социоинженерного атакующего воздействия j-ого злоумышленника с использованием i-ого ресурса. Таким образом, происходит переход от степени выраженности ресурса, используемого злоумышленником, к вероятности успеха социоинженерного атакующего воздействия на пользователя и профиль компетенций злоумышленника приобретает вид $(p_{1j}, ..., p_{kj})$.

Стоит отметить, что модели пользователя информационной системы сопоставлен профиль уязвимостей пользователя, в которую входят степени выраженности уязвимостей пользователя, на основании которых строятся вероятностные оценки успешности того или иного социоинженерного атакующего воздействия злоумышленника. Предполагается, что рассмотрение профиля компетенций злоумышленника позволит повысить точность вероятностных оценок защищенности пользователей информационных систем от социоинженерных атак.

Таким образом, разные злоумышленники с разной вероятностью успеха производят социоинженерные атаки на разных пользователей. Успех социоинженерной атаки j-м злоумышленником будет определяться выраженностью у него ресурса, позволяющего воздействовать на наиболее выраженные уязвимости атакуемого пользователя информационной системы. Формализация данного утверждения будет выглядеть следующим образом:

$$p_{ij} = \frac{D_j(R_i)S_k(V_l)}{M_i B_l}$$

, где $D_j(R_i)$ — выраженность ресурса R_i у злоумышленника j, $S_k(V_l)$ — выраженность уязвимости V_l у пользователя k, M_i — максимальная

выраженность ресурса R_i, B_l — максимальная выраженность уязвимости V_l, а p_{ij} — вероятность успеха социоинженерного атакующего воздействия j-ого злоумышленника с использованием i-ого ресурса на k-ого пользователя.

Заметим, что в ряде случаев формула даёт некорректные результаты. Так в случае, если пользователь обладает высоко выраженной уязвимостью, а злоумышленник имеет не слишком высокую компетенцию, то вероятность успешности социоинженерной атаки будет невысока. Справедливо и обратное, если злоумышленник имеет высокую компетенцию, а пользователь обладает низкой степенью выраженности соответствующей уязвимости, то вероятность успешности социоинженерного атакующего воздействия будет также мала. Изменим формулу следующим образом для получения более точных результатов:

$$p_{ij} = \frac{(\frac{S_k(V_l)}{B_l} - \alpha)(\frac{D_j(R_j)}{M_i} - \beta)}{(1-\alpha)^2(1-\beta)^2} \tag{1}$$

В зависимости от параметров α и β осуществляется сдвиг, позволяющий усилить влияние выраженности уязвимости пользователя или уровня компетенции злоумышленника на итоговое значение вероятности. На рис.1 представлен график

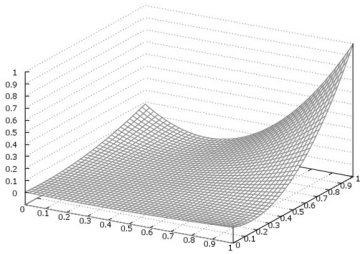

Рис. 1: Red, blue and green line

Заключение

В данной статье рассмотрено дополнение комплекса «информационная система — персонал — критичные документы» с помощью профиля компетенций злоумышленника. Предложена модель комплекса «критические документы — информационная система — персонал — злоумышленник» (КДИСПЗ). Формализован профиль компетенций злоумыш-

ленника, представлено выражение вероятности успеха социоинженерного атакующего воздействия j-ого злоумышленника с использованием i-ого ресурса в простейшем случае.

Список литературы

[1] Азаров А.А. Вероятностно-реляционные модели и алгоритмы обработки профиля уязвимостей пользователей при анализе защищённости персонала информационных систем от социоинженерных атак, Диссертация на соискание учёной степени к.т.н. 2013

[2] Азаров А.А., Тулупьева Т.В., Тулупьев А.Л. Прототип комплекса программ для анализа защищенности персонала информационных систем построенный на основе фрагмента профиля уязвимостей пользователя. Труды СПИИРАН. 2012. Вып. 21. С. 21-40.

[3] Ванюшичева О.Ю. Прототип комплекса программ для построения профиля психологически обусловленных уязвимостей пользователя. Дипломная работа. СПб.: СПбГУ, 2012.

[4] Ванюшичева О.Ю., Тулупьева Т.В., Пащенко А.Е., Тулупьев А.Л., Азаров А.А. Количественные измерения поведенческих проявлений уязвимостей пользователя, ассоциированных с социоинженерными атаками. // Труды СПИИРАН. 2011. Вып. 19. С. 34–47.

[5] Веденеев В.С., Бычков И.В. Средства поиска инсайдеров в корпоративных ИС // Безопасность информационных технологий. No1. 2014. С. 9–13.

[6] Дорохов В.Э. О рисках потери репутации организации вследствие инцидентов информационной безопасности // Безопасность информационных технологий. No2. 2014. С. 80–82.

[7] Котенко И.В., Степашкин М.В. Системы-имитаторы: назначение, функции, архитектура и подход к реализации // Изв. вузов. Приборостроение. 2006. Т. 49, No 3. С. 3–8.

[8] Котенко И.В., Юсупов Р.М. Перспективные направления исследований в области компьютерной безопасности. Защита информации. Инсайд. 2006. No 2. С. 46.

[9] Митник К.Д., Саймон В.Л. Искусство обмана. М.: Компания Ай-Ти, 2004. 360 с.

[10] Общая психология. Словарь / Под ред. А.В. Петровского // Психологический лексикон. Энциклопедический словарь в шести томах / Ред.-сост. Л.А. Карпенко. Под общ. ред. А.В. Петровского. М.: ПЕРСЭ, 2005. 251 с.

[11] Пентагон подсчитал, что Э. Сноуден похитил 1,7 млн секретных файлов // РБК / URL: http://top.rbc.ru/politics/10/01/2014/898589.shtml (дата обращения 01.03.2015)

[12] Сапронов К. Человеческий фактор и его роль в обеспечении информационной безопасности. URL: http://www.interface.ru/home.asp? artId=17137 (дата обращения 05.03.2015).

[13] Сергиевский М. Сети – что это такое // КомпьютерПресс. 1999, No10, С. 3-9.

[14] Суворова А.В., Тулупьев А.Л., Пащенко А.Е., Тулупьева Т.В., Красносельских Т.В. Анализ гранулярных данных и знаний в задачах исследования социально значимых видов поведения // Компьютерные инструменты в образовании. No4. 2010. С. 30–38.

[15] Тулупьева Т.В., Тулупьев А.Л., Азаров А.А., Пащенко А.Е. Психологическая защита как фактор уязвимости пользователя в контексте социоинженерных атак // Труды СПИИРАН. 2011. Вып. 18. С. 74–92.

[16] Убытки от киберпреступлений продолжают расти // URL: http:// www8.hp.com/ru/ru/software-solutions/ponemon-cyber-security-report/ index.html (дата обращения 04.03.2015)