DOI: 10.51932/9785907271739_138
УДК 621.3

Н.И. Фаттахов, З.Х. Захарова
(г. Казань, Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ)

ИНФОРМАЦИОННАЯ СИСТЕМА ПРОВЕРКИ СОТРУДНИКОВ НА ЗАЩИЩЕННОСТЬ ОТ ФИШИНГА

INFORMATION SYSTEM FOR CHECKING EMPLOYEES FOR PHISHING PROTECTION

Дано определение понятия «фишинг». Приведены схемы алгоритма работы фишинг-системы для повышения информационной безопасности организации, а также реализация основных сущностей и функций информационной системы (ИС) проверки сотрудников на защищенность от фишинга. Определены основные тенденции развития ИС, а также предполагаемая эффективность ее работы.

The definition of the concept of "phishing" is given. The schemes of the algorithm of the phishing system to improve the information security of the organization, as well as the implementation of the main entities and functions of the information system (IS) for checking employees for phishing protection are presented. The main trends in the development of IP, as well as the expected efficiency of its work, have been determined.

Ключевые слова: информационная система, информационная безопасность, защита организации.

Keywords: information system, information security, organization protection, phishing.

Несомненно, информационная безопасность в современном мире является одним из важнейших элементов инфраструктуры компании.

При несоблюдении правил информационной безопасности предприятие рискует лишиться конфиденциальности своих данных. Конфиденциальная информация предприятия является достаточно широким понятием, в неё могут входить как данные о пользователях информационной системы, так и информация, составляющая коммерческую тайну предприятия. Ущерб, причиняемый утечкой информации, невозможно спрогнозировать заранее. Он может выражаться в незначительной сумме, но в некоторых случаях приводит к полной неспособности компании вести деятельность [1]. В корне проблемы несоблюдения правил информационной безопасности лежит человеческий фактор и неосведомленность о всех способах интернет-мошенничества [2].

Одним из самых распространённых способов мошенничества в интернете является фишинг (англ. phishing). Данный вид злоумышленных действий представляет собой способ получения конфиденциальной информации пользователя посредством рассылки электронных писем, содержащих ссылку

на поддельный сайт. После перехода пользователя по ссылке события могут протекать разными способами. В самом безобидном случае, с помощью психологического воздействия, злоумышленники могут попытаться заставить пользователя ввести свои конфиденциальные данные, тем не менее последствия могут быть и более серьезными: например, на персональный компьютер пользователя может быть скачана вредоносная программа, которая в свою очередь может вывести из строя всех участников локальной сети предприятия [3].

Для предотвращения таких ситуаций компании необходимо как можно тщательнее подготавливать своих сотрудников, а в крайнем случае и вовсе ограждать неответственных лиц от доступа к конфиденциальным данным [4].

Этим и обуславливается необходимость и актуальность разработки информационной системы проверки сотрудников на способность обнаруживать злоумышленные действия, далее именуемой фишинг-системой.

В данной статье предлагается рассмотреть простейшую реализацию алгоритма работы фишинг-системы.

Систему с минимальным набором функций можно реализовать с помощью следующих сущностей:

1. Рассылка – основная сущность фишинг-системы. Данная сущность является суперклассом для фишинг-писем.

2. Доменное имя – сущность, необходимая для создания рассылки и содержит данные для отправки письма с «подозрительного» адреса. Сущность имеет ряд полей для авторизации на выбранном почтовом сервере.

3. Шаблон письма – сущность, необходимая для создания рассылки и содержит все необходимые функции и мета-данные для того, чтобы отследить поведение сотрудника.

4. Фишинг-письмо – данная сущность представляет собой письмо, которое будет отправлено пользователю, имеет уникальный идентификатор.

5. Письмо безопасности - сущность, создаваемая при условии, что пользователь переслал фишинг-письмо в отдел безопасности. Содержит данные о пересланном письме, пользователе и мета-данные.

Алгоритм работы фишинг-системы проще всего проиллюстрировать с помощью диаграммы метода IDEF3 [5], представленной на рис. 1.

Для реализации данного алгоритма необходимо решить следующие нетривиальные задачи:

1. отслеживание открытия письма,
2. отслеживание перехода по ссылке,
3. отслеживание о сообщении сотрудником в отдел информационной безопасности.

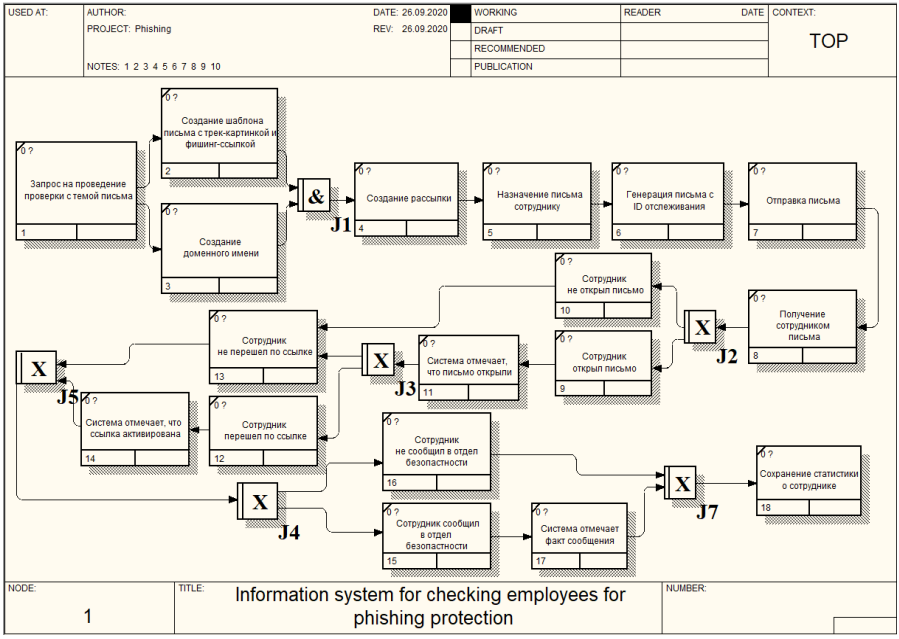

Рис. 1. Иллюстрация алгоритма работы фишинг-системы

При решении первой задачи предлагается использовать GET-запросы. В шаблон письма вложена ссылка на метод, возвращающий с сервера картинку. Мета-данные ссылки содержат идентификатор отправленного письма, по которому можно определить проверяемого сотрудника. При открытии сотрудником письма активируется ссылка, после чего сервер отправляет в ответ картинку, а система в свою очередь передает мета-данные в параметры функции отметки. Метод отметки идентифицирует сотрудника по уникальному ID письма (переданного в качестве мета-данных), и обновляет соответствующий пункт статистики сотрудника.

Вторая задача решается аналогично, за исключением того факта, что вместо отправки в ответ сервером картинки, происходит перенаправление сотрудника на официальный сайт «симулируемой» организации.

Для определения факта отправки пользователем письма в отдел информационной безопасности, предлагается следующий алгоритм:

1. С указанным интервалом на сервере включается метод получения всех писем с почтового сервера отдела информационной безопасности.
2. Производится сортировка писем по признаку содержания мета-данных, связанных с фишингом.
3. Для каждого письма производится идентифицирование сотрудника;
4. Обновляется соответствующий пункт статистики сотрудника.
5. Производится удаление обработанных писем с почтового сервера.

Реализация, рассматриваемая в данной статье, не претендует на оптимальность и требует доработки, однако уже в таком виде способна во много раз улучшить подготовленность сотрудников к фишингу, и позволяет качественнее оценивать защищенность конфиденциальных данных организации. С точки зрения совершенствования такой системы можно рассмотреть такие ее модернизации, как: определение скорости реагирования сотрудников, отслеживание использования сотрудниками «подозрительных» флэш-накопителей, отслеживание сотрудниками скачивания вредоносных программ и т.д.

В заключение можно сделать следующий вывод: использование предприятиями фишинг-систем, для обучения своих сотрудников правилам информационной безопасности, могут в несколько раз повысить защищенность компании, и тем самым обеспечить не только целостность и неприкосновенность хранимых данных, но и сохранить экономический потенциал предприятия.

Список литературы

1. Bitcop: [сайт] – Москва, 2020. – URL: https://bitcop.ru – Обеспечение информационной безопасности предприятия: потенциальные угрозы и средства защиты от них (дата обращения: 24.09.2019). – Текст: электронный.

2. Интегрус: [сайт] – Санкт-Петербург, 2018. – URL: https://integrus.ru/ Защищенность конфиденциальной информации в организации (дата обращения: 24.09.2019). – Текст: электронный.

3. *Горлов, А.П.* Автоматизированная система оценки эффективности программно-аппаратных средств защиты информации / Горлов А.П., Рытов М.Ю., Лысов Д.А. // Автоматизация и моделирование в проектировании и управлении - 2019г. №2.

4. *Тумбинская, М. В.* Защита информации на предприятии : учебное пособие / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2020. — 184 с. — ISBN 978-5-8114-4291-1. — Текст : электронный / Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/130184 (дата обращения: 24.09.2020). — Режим доступа: для авториз. пользователей.

5. *Гвоздева, Т.В.* Проектирование информационных систем: технология автоматизированного проектирования. Лабораторный практикум: учебно-справочное пособие / Е.В.Гвоздева, Б.А. Баллод. — 2-е изд., стер. – Санкт-Петербург: Лань, 2020. — 156 с. — ISBN 978-5-8114-5147-0. — Текст : электронный / Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/133477/#2 (дата обращения: 24.09.2020). — Режим доступа: для авториз. пользователей.

Материал поступил в редколлегию 13.10.20.