УДК 528.71

Фишев Дмитрий Леонидович
магистрант
Сибирский государственный университет геосистем и технологий
г. Новосибирск, Россия
Шабурова Аэлита Владимировна
д.э.н., доцент
Сибирский государственный университет геосистем и технологий
г. Новосибирск, Россия

Изучение фишинговых атак с учетом влияния психологических аспектов социальной инженерии, как угроза безопасности производственных предприятии

Аннотация. Данная статья рассматривает фишинговые атаки с учетом влияния психологических аспектов социальной инженерии, как одну из самых больших угроз информационной безопасности производстенных предприятий. Приводится классификация техник социальной инженерии в контексте реализации угроз безопасности производственных предприятий. Анализируется на какой ущерб направлены фишинговые атаки в отношении пользователей информационной инфраструктуры производственных предприятий. Так же предлагаются комплекс мероприятий, направленных для повышения уровня безопасности от фишиновых атак производственных предприятиях.

Ключевые слова: информационная безопасность, социальная инженерия, фишинг, производственные предприятия.

Fishev Dmitry Leonidovich
graduate student
Siberian State University of Geosystems and Technologies
Novosibirsk, Russia
Шабурова Аэлита Владимировна
associate professor
Siberian State University of Geosystems and Technologies
Novosibirsk, Russia

The study of phishing attacks taking into account the influence of psychological aspects of social engineering as a threat to the security of industrial enterprises

Abstract. This article considers phishing attacks, taking into account the influence of psychological aspects of social engineering, as one of the biggest threats to the information security of manufacturing enterprises. The classification of social engineering techniques in the context of the implementation of threats to the security of industrial enterprises is given. It analyzes the damage caused by phishing attacks against users of the information infrastructure of manufacturing enterprises, and also suggests a set of measures aimed at improving the level of security against phishing attacks on manufacturing enterprises.

Keywords: information security, social engineering, phishing, manufacturing enterprises.

Введение. Современный этап развития общества характеризуется большим значением информационной сферы, которая является одной из основных сред реализации широкого спектра действий социума. В настоящее время сеть Интернет является ключевым элементом существующей информационной сферы. Значительная глубина интеграции сервисов сети Интернет в деятельность современного общества порождает большое количество проблем безопасности, одной из ключевых среди которых является использование информационного пространства для проведения информационно–психологических атак.

Вследствие этого, число осуществленных угроз, таких как фишинг, спам, смишинг и другие, с каждым днем увеличивается, что говорит о больших возможностях для злоумышленников по реализации многообразных негативных воздействий на определенного объекта или группу лиц. Производственные предприятия не являются исключением [1].

Целью данной работы является исследование фишинговых атак с учетом влияния психологических аспектов социальной инженерии, как угроза безопасности производственных предприятии, а так же защиты от них.

Для достижения цели необходимо решить ряд задач:

– изучить фишинговых атак с учетом влияния психологических аспектов социальной инженерии;

– провести анализ ущерба от фишинговых атак на производственных предприятиях;

– рассмотреть вопрос противодействия фишинговым атакам.

Изучение фишинговых атак с учетом психологических аспектов социальной инженерии

Социальная инженерия представляет собой комплекс психологических манипуляций и нетехнических методов, применяемых злоумышленниками с целью получения несанкционированного доступа к информации или системам хранения информации без использования технических средств. Суть социальной инженерии заключается в том, чтобы ввести в заблуждение жертву атаки или заставить её пренебречь разумом и стандартными мерами безопасности в угоду требуемых злоумышленнику действий [1,5].

Существуют различные техники социальной инженерии, которые тем или иным способом заставляют пользователя осуществить действия, влекущие за собой требуемые злоумышленнику целевые действия жертвы атаки, например запустить заражённый файл или открыть ссылку на заражённый веб-сайт [1,5].

Представим краткое описание наиболее популярных на сегодняшний день техник социальной инженерии в контексте реализации угроз безопасности производственных предприятий в таблице 1 [1,2,3,4,5,6].

Таблица 1 - Классификация техник социальной инженерии в контексте реализации угроз безопасности производственных предприятий

Наименование	Краткое описание
Фишинг	Техника, направленная на получение несанкционированного доступа к конфиденциальной информации злоумышленником, выдающим себя за того, кем он не является, например, за компанию или контаента. Как правило, фишинг может осуществляться с помощью e-mail писем, сообщений в мессенджерах, телефонных звонков и основан на психологических подходах к манипуляции жертвы атаки
Вишинг (голосовой фишинг)	Подвид фишинга, направленный на завладение конфиденциальной информации, основным инструментом которого являются звонки автоинформатора, автоответчика или представителя злоумышленника, выдающего себя за сотрудника силовых структур, банковских организаций, и т.д.
Смишинг	Подвид фишинга, направленный на завладение конфиденциальной информации, основным инструментом которого является рассылка смс-сообщений и сообщений в мессенджерах, например с ссылками на сайт злоумышленника
Бейтинг, или «дорожное яблоко»	Например, хакер оставляет возле офиса атакуемого предприятия флэш-накопитель с надписью «Крипто-кошелек». Расчет на то, что кто-то из сотрудников заинтересуется содержимым и откроет носитель на своей рабочей станции,

	тем самым заразит её вирусом и предоставит злоумышленнику те или иные возможности в информационной системе предприятия
Спуфинг	Техника, ключевой особенностью которой является маскирование действий злоумышленника под что-то, чему доверяет жертва. Например, злоумышленник может сделать копию профиля социальной сети друга жертвы, после чего написать жертве и попросить одолжить денежные средства.
Обратная социальная инженерия	Злоумышленник создает ситуации, в которых он не вредит сразу, а помогает своей жертве, чтобы вызвать у нее доверие. Так, например, злоумышленник сначала может пообещать жертве получить хорошую работу, но для получения тестового задания жертве нужно перевести немного денежных средств
Quid pro quo, услуга за услугу	Злоумышленник создает ситуации, в которых он принудительно настаивает на важности оказания помощи потенциальной жертве атаки. Например, злоумышленник звонит и говорит, что банковский счет жертвы заблокирован из-за атаки, которую совершают прямо сейчас. Но он вычислил атакующего и поможет защитить деньги, если жертва сообщит те или иные конфиденциальные данные.

Анализ ущерба от фишинговых атак на производственных предприятиях

Исследование фишинговых атак в отношении пользователей систем информационной инфраструктуры производственных предприятий, ущерб от реализации таких атак можно разделить, как:

1. Ущерб от получения злоумышленником несанкционированного доступа к персональным данным сотрудников - пользователей систем информационной инфраструктуры предприятия.
2. Ущерб от получения злоумышленником несанкционированного доступа к конфиденциальным данным предприятия, циркулирующим в информационных системах.

Повышение уровня безопасности от фишиновых атак на производственных предприятиях

Для противодействия фишинговым атакам на пользователей объектов информационной инфраструктуры с применением инструментов социальной инженерии, разделим на следующие мероприятия:

– мероприятия профилактики фишинговых атак с применением инструментов социальной инженерии;

– мероприятия предотвращения фишинговых атак с применением инструментов социальной инженерии.

Профилактические мероприятия направлены непосредственно на снижение эффективности протекания процесса реализации фишинговых атак на пользователей объектов информационной инфраструктуры производственного предприятия Такое направление включает в себя методы, применяемые для локализации процесса и нейтрализации негативных последствий, а также создания информационной базы для предотвращения схожих процессов реализации фишинговых атак с применением инструментов социальной инженерии в будущем. Такие мероприятия можно представить следующим перечнем:

– ограничение действий участников реализации фишинговых атак с применением инструментов социальной инженерии;

– информационное противоборство.

Предотвращающие мероприятия направлены непосредственно на блокирование реализации фишинговых атак на пользователей объектов информационной инфраструктуры производственного предприятия на самых ранних этапах. Такие методы можно представить следующим перечнем:

– фильтрация контента и трафика в целях выявления признаков реализации фишинговых атак с применением инструментов социальной инженерии;
– информирование пользователей объектов информационной инфраструктуры;
– настройка доступа пользователей объектов информационной инфраструктуры.

Заключение. В результате, можно сделать вывод, что фишинг – это не просто техническая угроза, а угроза, которая уходит в психологию человека. Для повышения уровня безопасности производственного предприятия необходимо знать и понимать техники социальной инженерии, понимать на что эти атаки нацелены, и для предотвращения от этих атак проводить и соблюдать мероприятия профилактики и предотвращения. Полученные результаты могут быть использованы государственными и коммерческими предприятиями для проектирования современных комплексных систем обеспечения безопасности.

Список источников

1. Абрамов К.Г. Распространение нежелательной информации в социальных сетях Интернета / К.Г. Абрамов, Ю.М. Монахов // Труды НТС. Комитет по информатизации, связи и телекоммуникациям, 2018. – 128 с.
2. Александров А.Г. Анализ угроз информационной безопасности при использовании фишинговых сайтов // Юристъ – Правоведъ, 2022. – С. 156 – 161.
3. Антонова Т. С. Фишинг как неизученное киберпреступление // StudNet, 2021. – С. 69 – 75.
4. Архипова А. Б. Технология формирования интегрированной антифишинговой системы в цифровом обществе // Вестник СибГУТИ, 2023. – С. 93 – 103.
5. Гончарова М.Н. Интернет-мошенничество как угроза экономической безопасности // Умная цифровая экономика. 2023. – С. 116 – 121.
6. Завьялов А.Н. Интернет-мошенничество (фишинг): проблемы противодействия и предупреждения // Baikal Research Journal. 2022. – С. 36 – 42.