ЭКСПЕРТНОЕ ЗАКЛЮЧЕНИЕ

по результатам проведения тестирования методом социальной инженерии компании 1

Даты проведения работ:

1-123  
Технический менеджер проекта:

1

Директор департамента аудита:

А.Н.Тюрин

[1. Введение 3](#_Toc495587372)

[1.1. Общие положения 3](#_Toc495587373)

[1.2. Принятые сокращения 3](#_Toc495587374)

[1.3. Резюме 3](#_Toc495587375)

[2. Принципы проведения работ 5](#_Toc495587376)

[2.1. Угрозы ИБ 5](#_Toc495587377)

[2.2. Модель нарушителя 5](#_Toc495587378)

[2.2.1. Внешний нарушитель 5](#_Toc495587379)

[3. Тестирование с помощью методов социальной инженерии 7](#_Toc495587380)

[3.1. Подготовка к проведению тестирования методом социальной инженерии 7](#_Toc495587381)

[3.2. Ход тестирования. Внешний нарушитель 8](#_Toc495587382)

[3.2.1. Сценарий №1. Перерасчет З/П 8](#_Toc495587383)

[3.3. Ход тестирования. Внутренний нарушитель 9](#_Toc495587384)

[3.3.1. Сценарий №1. Перерасчет З/П 9](#_Toc495587385)

[4. Заключение 11](#_Toc495587386)

[Приложение 1. Анализ уровня защищенности. Справочная информация. 12](#_Toc495587387)

[Анализ уровня защищенности 12](#_Toc495587388)

[Критичность реализации уязвимости 12](#_Toc495587389)

[Простота эксплуатации уязвимости 13](#_Toc495587390)

[Доступность уязвимости 14](#_Toc495587391)

[Вероятность эксплуатации уязвимости 14](#_Toc495587392)

[Риск уязвимости 15](#_Toc495587393)

1. Введение
   1. Общие положения

В настоящем экспертном заключении представлены результаты проведения тестирования методом социальной инженерии компании «1» (далее – Компания), а также предложены рекомендации по устранению выявленных уязвимостей и повышению уровня защищенности.

* 1. Принятые сокращения

*Таблица 1.2–1. Принятые сокращения*

|  |  |
| --- | --- |
| Сокращение | Расшифровка |
| ИБ | Информационная безопасность |
| ИС | Информационная система |
| КИС | Корпоративная информационная сеть |
| МЭ | Межсетевой экран |
| ПО | Программное обеспечение |

* 1. Резюме

В соответствии с договором 1 от 1 специалистами компании «Digital Security» в период с 1 по 123 были проведены работы по тестированию методом социальной инженерии.

Проведенные работы показали, что:

1. Сотрудники с осторожностью относятся к присылаемым письмам с фишинговыми сайтами. На данном этапе удалось получить X учетный записей.
2. Бдительность к письмам, содержащие excel-документы с макросами, существенно ниже. В данном случае было зафиксировано X запусков макросов.

В ходе проникновения методом социальной инженерии удалось получить ${result}.

Общий уровень защищенности Компании в целом можно охарактеризовать как «1».

Основной рекомендацией является повышение осведомленности сотрудников компании «1» в вопросах безопасности путем проведения соответствующих мероприятий. Например, периодическая информационная рассылка с описанием типичных атак на пользователей и мерами их выявления.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Сценарий** | **Всего**  **отправлено** | **Открыто писем** | **Скачивание вложений / переход по ссылке** | **Запуск / ввод данных** | **Запуск / ввод данных среди**  **открывших письмо** |
| Перерасчет ЗП (RU) | 44 | 42 | 32 | 4 | 10% |
| Перерасчет ЗП (UK) | 48 | 27 | 16 | 2 | 7% |
| Назначение премии (RU) | 14 | 13 | 6 | 3 | 23% |
| Назначение премии (UK) | 50 | 42 | 25 | 4 | 10% |
| Обновление сервиса (RU) | 6 | 6 | 2 | 0 | 0% |
| Обновление сервиса (UK) | 19 | 12 | 4 | 0 | 0% |
| Новый корп. сервис (RU) | 24 | 8 | 3 | 0 | 0% |
| Новый корп. сервис (ENG) | 34 | 14 | 5 | 0 | 0% |
| Изменение пароля в Google (RU) | 7 | 1 | 1 | 0 | 0% |
| Изменение пароля в Google (UK) | 33 | 4 | 0 | 0 | 0% |
|  |  |  |  |  |  |
| **Итого :** | **279** | **169** | **94** | **13** | **8%** |

1. Принципы проведения работ
   1. Угрозы ИБ

На информационные ресурсы Компании могут действовать следующие три угрозы ИБ: угрозы нарушения конфиденциальности, целостности и доступности.

Угроза нарушения конфиденциальности направлена на разглашение информации, имеющей в Компании статус конфиденциальной. При реализации угрозы информация становится известной лицам, которые не должны иметь к ней доступ – ряду сотрудников Компании, клиентам, партнерам, конкурентам, третьим лицам.

Угроза нарушения целостности направлена на модификацию или искажение информации, приводящее к изменению ее структуры или смысла, полному или частичному уничтожению.

Угроза нарушения доступности (угроза отказа в обслуживании) заключается в невозможности получения доступа к информационному ресурсу пользователями информационной системы.

Основным принципом проведения аудита ИБ является проверка возможности реализации указанных угроз, воздействующих на информационные ресурсы Системы, в рамках заданной модели нарушителя.

* 1. Модель нарушителя

В качестве вероятного нарушителя информационной безопасности Системы Компании рассматривается лицо или группа лиц, состоящих или не состоящих в сговоре, которые в результате умышленных или неумышленных действий потенциально могут реализовать угрозы ИБ, осуществить посягательства на информационные ресурсы Системы и нанести ущерб интересам Компании.

В качестве угроз ИБ рассматриваются базовые угрозы нарушения конфиденциальности и целостности информации, а также угроза отказа Системы в обслуживании клиентов Компании.

Умышленно действующий нарушитель может преследовать следующие цели (а также их всевозможные комбинации):

* злонамеренный вызов отказа в обслуживании;
* повышение собственных привилегий;
* несанкционированный доступ к критичной с точки зрения бизнеса информации.

В ходе работы была использована модель внешнего нарушителя.

* + 1. Внешний нарушитель

При проведении теста на проникновение используются следующие модели внешнего нарушителя:

* внешний нарушитель из сети, не обладающий знаниями о тестируемой Системе и правами в ней;
* внешний нарушитель из сети, обладающий правами и знаниями пользователя Системы.

1. Тестирование с помощью методов социальной инженерии
   1. Подготовка к проведению тестирования методом социальной инженерии

В качестве подготовки к проведению теста, аудиторами были проанализированы популярные социальные сети (такие как vk.com, linkedin.com, twitter.com и другие), а также официальные ресурсы Компании.

Был составлен список сотрудников сервиса, который включал в себя:

* Рабочие почтовые адреса.
* Должность.
* Страницы в социальных сетях.
* Личные почтовые адреса.
* Возможные увлечения и род занятий.

На основе информации из открытых источников было проверено, подвергались ли аккаунты сотрудников взлому ранее.

* 1. Ход тестирования. Внешний нарушитель
     1. Сценарий №1. Перерасчет З/П

*Отправитель: Михаил Зеленцов, m.zelencov@passwordgpu.ru*

*Даты проведения атак: с 03.11.2016.*

*Тематика писем: договор франчайзинга.*

*Цель: получение учетных данных сотрудников, удаленный доступ на хосты сотрудников.*

Описание:

По списку email-адресов сотрудников производилась почтовая рассылка от имени отдела бухгалтерии. Файл, прикрепленный к письму, представлял из себя XLSM-документ с макро- сом. В случае запуска макроса на контролируемый сервер отправлялось имя текущего пользователя и его идентификатор.

Чтобы избежать просмотра документа в интерфейсе Почты, функциональность прикрепляемых файлов была имитирована в теле письма, технически вложения разме- щались на внешнем сервере и принудительно скачивались браузером.

В ходе тестирования фиксировались три состояния: открытие письма, сохранение вложения, запуск макроса.

Сценарий. Новый почтовый сервер.
Отправитель: Имя Фамилия, email.
Даты проведения атак: с 03.11.2016.
Цель: получение учетных данных сотрудников.
Описание:
По списку email-адресов сотрудников производилась почтовая рассылка от имени информационного отдела. Ссылка в письме ведет на фишинговый ресурс, внешне имитирующий настоящий Outlook. В случае ввода учетных перехода на сайт и ввода учетных данных, нами логировались эти данные и использовались для дальнейшего развития атаки.
В ходе тестирования фиксировались три состояния: открытие письма, переход по ссылке, ввод учетных данных.Сценарий. Яндекс.Диск
Отправитель: Имя Фамилия, email
Даты проведения атак: с 03.11.2016.
Цель: компрометация машин сотрудников.
Описание:
По списку email-адресов сотрудников производилась почтовая рассылка от имени информационного отдела. Ссылка в письме ведет на ресурс Яндекс.Диск, на который загружен вредоносный файл. В случае скачивания и запуска данного вложения машина становится подконтрольной.
В ходе тестирования фиксировались три состояния: открытие письма, сохранение вложения, запуск вредоносного вложения.

# Результаты:

Разослано писем: 44

Скачивание вложений: 32

Запуск вложения: 4

Сценарий. Новый почтовый сервер.
Отправитель: Имя Фамилия, email.
Даты проведения атак: с 03.11.2016.
Цель: получение учетных данных сотрудников.
Описание:
По списку email-адресов сотрудников производилась почтовая рассылка от имени информационного отдела. Ссылка в письме ведет на фишинговый ресурс, внешне имитирующий настоящий Outlook. В случае ввода учетных перехода на сайт и ввода учетных данных, нами логировались эти данные и использовались для дальнейшего развития атаки.
В ходе тестирования фиксировались три состояния: открытие письма, переход по ссылке, ввод учетных данных.Сценарий. Яндекс.Диск
Отправитель: Имя Фамилия, email
Даты проведения атак: с 03.11.2016.
Цель: компрометация машин сотрудников.
Описание:
По списку email-адресов сотрудников производилась почтовая рассылка от имени информационного отдела. Ссылка в письме ведет на ресурс Яндекс.Диск, на который загружен вредоносный файл. В случае скачивания и запуска данного вложения машина становится подконтрольной.
В ходе тестирования фиксировались три состояния: открытие письма, сохранение вложения, запуск вредоносного вложения.

1. Заключение

В результате анализа защищенности вебсайта «pentest.dev.rbp.raiffeisen.ru» специалистами Digital Security не было выявлено серьезных уязвимостей, с помощью которых злоумышленники потенциально могли бы нанести ущерб, как вебсайту, так и его пользователям.

Общий уровень защищенности можно охарактеризовать как «высокий».