ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«САНКТ-ПЕТЕРБУРГСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, МЕХАНИКИ И ОПТИКИ»

Дисциплина:

«Теория информационной безопасности и методология защиты информации»

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №4

Выполнили:

Соловьев Артемий Александрович

Гр. P32151

Проверил:

Аспирант ФБИТ

Кондратенко Станислав Сергеевич

Санкт-Петербург

2023г.

Кейс:

Произошла утечка данных (имена, номера телефонов, адреса, IP) 2.2 млн пользователей.

Роли:

Представитель

Специалист по ИБ

Системный администратор

Этап 1

Произошла утечка, её заметило руководство, пока неизвестна причина и виновник.

Решения:

Представитель:

1. Дополнительно обратиться к сторонним специалистам по ИБ (+1)
2. Готовить комментарий по происшествию и параллельно обратиться к специалисту по ИБ для выяснения обстоятельств и оценки ущерба (0)
3. Сразу дать комментарий в СМИ (-2)

Специалист по ИБ:

1. Начать выяснять причины утечки и её содержание (+2)
2. Провести инструктаж перед сотрудниками (0)
3. Не оценивая уровень ущерба, сообщить начальству о незначительности утечки, надеясь, что её никто не заметит (-3)

Системный администратор:

1. Проверяет последние действия на сервере для выявления причины утечки (+2)
2. Ничего не делать (0)
3. Приостановить доступ к некоторым сервисам и документациям (-3)

Этап 2

Об утечке стало известно в СМИ

Решения:

Представитель:

1. Связаться с каждым пострадавшим и предоставить им полную информацию о том, что произошло, а также о том, как будут приняты меры для защиты их данных (+2)
2. Созвать совещание с руководством департамента и разработать стратегию по укреплению системы безопасности информации (0)
3. Попытаться замять скандал, дать взятку журналистам (-5

Специалист по ИБ:

1. Локализовать утечку данных (+4)
2. Ничего не делать (-4)

Системный администратор:

1. Ограничить доступ к базе данных, откуда произошла утечка (+3)
2. Бездействие (-2)

Этап 3

Попытка минимизировать урон от утечки.

Решения:

Представитель:

1. Нанять команду экспертов по безопасности данных, чтобы оценить ущерб и разработать план действий для восстановления утраченных данных (+3)
2. Сообщить пострадавшим о том, что департамент предпринимает меры для защиты их данных, но не давать конкретных деталей (0)
3. Не делать ничего и надеяться, что проблема решится сама собой (-4)

Специалист по ИБ:

1. Разработать план восстановления и внедрения новых мер безопасности, чтобы предотвратить будущие утечки данных (+2)
2. Сообщить руководству департамента о том, какие меры нужно принять, чтобы устранить уязвимости в системе безопасности (0)
3. Ничего не делать и надеяться, что проблема решится сама собой (-4)

Системный администратор:

1. Помочь команде экспертов по безопасности данных в устранении уязвимостей в системе безопасности (+3)
2. Сотрудничать с руководством департамента и специалистом по ИБ, чтобы разработать новые меры безопасности (0)
3. Отказаться от участия в процессе восстановления данных и не предпринимать никаких действий (-5)

Этап 4

Улучшение системы безопасности.

Решения:

Представитель:

1. Немедленно провести внутреннюю проверку и выявить слабые места в системе безопасности (+4)
2. Обратиться к юристам для оценки возможных юридических последствий (0)

Специалист по ИБ:

1. Внедрить двухфакторную аутентификацию для повышения уровня безопасности. Разработать и внедрить политику паролей для повышения безопасности доступа к системам и данным. Провести тестирование для проверки уровня защиты систем и выявления слабых мест. Организовывать регулярные бэкапы данных для минимизации потерь в случае кибератаки или сбоев в работе систем (+5)
2. Ничего не делать (-2)

Системный администратор:

1. Проверить ПО. Ограничить доступ к системам и данным только необходимым пользователям и группам. Использовать методы аутентификации, такие как двухфакторная аутентификация. Создать политику использования сети, чтобы ограничить доступ к внутренним ресурсам и защитить сеть от внешних угроз. (+5)
2. Ничего не делать (-1)

Этап 5

Прошло n-ное количество времени, шумиха начала утихать.

Решения:

Представитель:

1. Дать комментарий об улучшении ситуации с ИБ (+3)
2. Ничего не делать (0)

Специалист по ИБ:

1. Продолжить совершенствовать системы ИБ в компании (+2)
2. Ничего не делать (-1)

Системный администратор:

1. Следить за событиями, происходящими на сервере, вручную останавливать подозрительную активность (+1)
2. Ничего не делать (0)

Вывод:

В результате выполнения лабораторной работы были выявлены способы решения проблемы для каждой роли, а также были выявлены наилучшие способы ее решения.