ОРГАНИЗАЦИЯ СИСТЕМЫ ПАРОЛЬНОЙ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Д.В. Солодкий

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

В современном мире повсеместной цифровизации все большую значимость приобретает защита информационных ресурсов как юридических, так и физических лиц. По данным positive technologies общее количество успешных инцидентов, которые привели к негативным последствиям в 2022 году увеличилось на 20,8%. Связано это с возросшим напряжением в киберпространстве. Значительное влияние оказывает и рост рынка киберпреступности: злоумышленники расширяют теневой бизнес. Тем временем в связи с массовыми утечками данных появляется возможность проведения атак с использованием скомпрометированной информации о пользователях. В 2023 году эти же причины послужат еще большему росту числа атак. Базовой, а зачастую и основной защитой от злоумышленников является системы парольной аутентификации.

Анализ литературного материала показал, что несмотря на большое количество материалов по данной теме, проблема все еще актуальна, так как более 40 % успешных атак на организации связан с компрометацией учетных данных пользователей информационных систем.

Целью работы является изучение методов и средств получения доступа к учетным записям пользователей.

Для этого необходимо решить следующие задачи.

1. Определить способы компрометации учетных данных.
2. Освоить методы и средства получения доступа.
3. Провести пинтесты на типовых информационных системах.
4. Определить средства противодействия данным киберугрозам.

Практическое применение результатов исследования возможно в целях повышения уровня защищенности информационных систем.

Выводы.

1. Методы социальной инженерии являются действенным средством атак.
2. Противодействие уязвимостям нулевого дня (и прочим программным уязвимостям) требует высокой скорости реакции от служб ИБ.
3. Противодействие современным вызовам в сфере ИБ требует комплексного подхода к системам защиты.

Рекомендации: при проектировании информационной системы необходимо учитывать разные виды угроз и применять комбинированные методы и средства ЗИ. Современная система ЗИ обязательно должна включать в себя UTM, SIEM и DLP модули, настроенные и взаимосвязанные между собой.

Список литературы

1. Актуальные киберугрозы: итоги 2022 года [Электронный ресурс]. – 2023. – Режим доступа: https://www.ptsecurity.com. – Дата доступа: 04.04.2023.
2. Атаки на домен [Электронный ресурс]. – 2023. – Режим доступа: https://habr.com. – Дата доступа: 06.04.2023.
3. Бесконтрольный привилегированный доступ: как снизить риски для бизнеса [Электронный ресурс]. – 2023. – Режим доступа: https://www.anti-malware.ru. – Дата доступа: 09.04.2023.