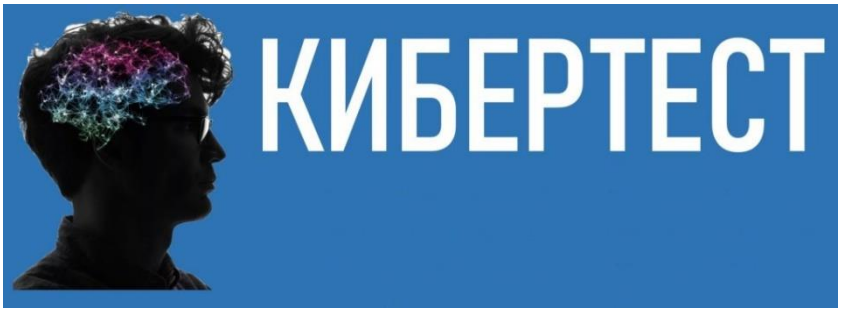
Общество с ограниченной ответственностью

КИБЕРТЕСТ



«СЕРВИС ПОИСКА ДУБЛИКАТОВ ПАРОЛЕЙ ЛОКАЛЬНЫХ ПОЛЬЗОВАТЕЛЕЙ»

Свидетельство о государственной регистрации программы для ЭВМ № 2023614426

Реестр российского программного обеспечения, запись №19353 от 04.10.2023

ПРИМЕР ПРИМЕНЕНИЯ СЕРВИСА

В ЗАКАЗЧИКЕ ИЗ ТОП-50 КРУПНЕЙШИХ КОМПАНИЙ РФ ПО ЧИСТОЙ ПРИБЫЛИ

Листов 3

2024 год

О заказчике

Компания ТОП-50 крупнейших в РФ по чистой прибыли, филиальная сеть в всех регионах России, более 100 тыс. сотрудников, более 100 серверов Domain Controller.

Проблема

В инфраструктуре заказчика отсутствует инструмент для расширенного контроля сложности паролей (проверка паролей на наличие в базах утекших паролей, которыми пользуются злоумышленники). Это приводит к тому, что пользователям и администраторам доступна возможность установки и использования «слабых» паролей и возможность установки паролей из известных словарей слабых паролей (пример: haveibeenpwned.com), которые удовлетворяют требованиям парольной политики AD, но являются уязвимыми для атак подбором по словарю. Тем самым повышаются риски проведения успешных атак на проникновение в информационную систему через подбор паролей по словарю и реализацию деструктивных действий, имеющих широкие последствия для бизнеса.

Цель

В результате внедрения Сервиса предполагается закрыть возможность использования паролей из известных словарей и контролировать, что пароли соответствуют всем требованиям информационной безопасности. Снизить бизнес-риски через минимизацию рисков информационной безопасности от атак на проникновение в информационную систему.

Что сделано

1) Предпроектное обследование:

- изучение и обследование ИТ-инфраструктуры в части размещения в ней системы,
- разработка архитектуры решения;
- изучение других инф. систем, с которыми требуется интеграция системы;
- изучение требований подразделений ИБ и ИТ в части настройки внедряемого решения, реализуемых им функциональных задач.

2) Проектирование (разработка проектной и эксплуатационной документации):

- пояснительная записка / проектное решение,
- руководство пользователя;

• руководство администратора;

• инструкция для технической поддержки;

• программа и методика испытаний.

3) Разработка версии «под Заказчика» (всего 4 релиза):

• функциональные требования,

• требования по информационной безопасности.

4) Внедрение:

• поставка ПО, активация лицензий и сертификатов технической поддержки,

• настройки системного и прикладного ПО;

• создание \ подключение учетных записей пользователей и администраторов;

• настройка резервного копирования;

• интеграция с сервисами заказчика;

• проведение приемочных испытаний;

• проведение опытной-промышленной эксплуатации;

• обучения работы с системой заинтересованных лиц;

• организация постпроектной технической поддержки.

Результат и ценность для Заказчика:

Сервис успешно внедрён, вышеуказанные риски снижены, благодаря чему подтверждено экономическое обоснование использования Сервиса.

Реализованы пожелания Заказчика:

- добавление собственных недопустимых в системе паролей,

- возможность запрещать использование паролей с заменой символов и слабым запутыванием (“password” - “P@ssw0rd” - “pa55word!” и т.п.);

- проверка нового пароля в момент смены пользователем;

- блокирование паролей с подряд идущими на клавиатуре символами;

- поддержка механизма регулярных выражений для фильтрации паролей;

- SLA по нагрузке и скорости работы Сервиса;

- наличие настраиваемых дашбордов для получения отчетности и аналитики.