MAKVES

Подход Makves к защите от киберугроз

Роман Подкопаев

MAKVES

Makves — российский разработчик ПО для аудита и мониторинга ИТ-ресурсов предприятия

Минцифры России

В реестре отечественного ПО.
Приказ Минцифры России
от 07.04.2020 №162.

РЕАЛИЗОВАННЫЕ ПРОЕКТЫ

МСП Банк
Элемент
ТРИНФИКО
РОСАТОМ
Агентство по страхованию вкладов
РОСНАНО
MECHEL
CAR CADE
ТАСС

ЗАЩИТА ДАННЫХ В СООТВЕТСТВИИ С ТРЕБОВАНИЯМИ РЕГУЛЯТОРОВ

ФЗ-152
Федеральный закон "О персональных данных"

GDPR
Общий регламент защиты персональных данных

PCI DSS
Стандарт безопасности данных платежных систем

ГОСТ Р 57580.1-2017
Защита информации финансовых организаций

Требования ФСТЭК
Обеспечение мер безопасности КИИ

СТО БР ИББС
Стандарт по обеспечению ИБ банков РФ

MAKVES

ЗАЩИТА ДАННЫХ КАК ОСНОВА ИБ-СТРАТЕГИИ

MAKVES

Для чего нужен DCAP

- ❑ Какие данные нужно защищать?
- ❑ Где они находятся и в каком объеме?
- ❑ Кто является владельцем и активным пользователем этих данных?

Как работает Makves DCAP

MAKVES

1

Сбор данных

Аудит Active Directory,
рабочих станций,
файловых серверов,
почтовых серверов

2

Поиск данных,
требующих защиты,
по содержимому
и внешним атрибутам

Анализ и категоризация

3

Создание матрицы доступа

Наглядная матрица
доступа пользователей
к файлам, папкам
и почтовым ящикам

4

Определение
избыточных
(нерегламентированных)
прав, нарушения доступа

Оценка рисков

5

Мониторинг

Непрерывный анализ
событий системы
и действий
пользователей

6

Поиск дубликатов,
устаревших данных и
учетных записей,
версий и активаций ОС

Актуальность файлов и ПО

Как DCAP помогает защититься от угроз?

MAKVES

1. Сокращает поверхность кибератаки
2. Позволяет оперативно выявить угрозу
3. Обеспечивает активную реакцию на инцидент
4. Помогает при расследовании инцидентов

MAKVES

Как защитить данные?

Присвоить категории информации на хранилищах

Использовать политики работы с данными / разграничение прав доступа

Анализировать угрозы и риски, связанные с хранением и доступом к данным