MAKVES DCAP В ДЕЙСТВИИ

Как организовать процесс защиты информации в банке с соблюдением требований регуляторов

MAKVES
ТЕПЕРЬ ЧАСТЬ ГАРДА

В РЕЕСТРЕ МИНЦИФРЫ
1-й продукт класса DCAP
Запись № 6299 от 07.04.2020

СЕРТИФИКАТЫ
совместимости
с РедОС и Astra Linux

СЕРТИФИКАТ
ФСТЭК № 4744

Участник

MAKVES
ТЕПЕРЬ ЧАСТЬ ГАРДА

НЕСТРУКТУРИРОВАННЫЕ ДАННЫЕ. СКРЫТАЯ УГРОЗА

Информация на файловых хранилищах, которую сотрудники банка создают и используют в своей работе, хаотично перемещается в рамках корпоративной сети. Объем этой информации стремительно растет

Появляются новые сотрудники с различным уровнем доступа к информационным ресурсам. Они копируют, пересылают и экспортируют из баз данных документы, создавая их дубликаты в папках общего пользования

Отсутствие контроля над корпоративной информацией, правами и действиями пользователей может привести к нарушению целостности, доступности и конфиденциальности информации

В РЕЗУЛЬТАТЕ становится сложно определить где хранится конфиденциальная информация и кто имеет к ней доступ

РИСКИ

MAKVES ТЕПЕРЬ ЧАСТЬ ГАРДА

НЕСТРУКТУРИРОВАННЫЕ ДАННЫЕ. СКРЫТАЯ УГРОЗА

01 Компрометация персональных данных и банковской тайны

02 Штрафы и санкции за нарушение требований регуляторов

03 Финансовые и репутационные потери, связанные с утечкой и мошенническими действиями сотрудников

РЕШЕНИЕ – MAKVES

Первая российская DCAP система
для защиты неструктурированных данных

ЧТО ВХОДИТ В ПРОДУКТ

Аудит доменных служб

Выявляет нарушения прав доступа, информирует об изменениях и автоматизирует процесс управления учетными записями

Помогает оперативно обнаружить и устранить несанкционированные действия сотрудников и взломанные аккаунты

Аудит файловых хранилищ

Выявляет конфиденциальную информацию, места её хранения и права доступа

Информирует о действиях с файлами и папками: изменение, копирование, перемещение, удаление

Автоматизирует процесс управления данными на файловых хранилищах

Аудит корпоративной почты

Отображает пользователей и группы которые имеют доступ к данным почтового сервера и как эти права были получены

Выявляет наличие доступа к чужой почте, большие почтовые ящики, пустые почтовые ящики, ящики с высоким уровнем риска

MAKVES DCAP

MAKVES ТЕПЕРЬ ЧАСТЬ ГАРДА

ОПЫТ РОССИЙСКОГО БАНКА

БАНК*

30 тыс. сотрудников

320 ТБ данных на файловых хранилищах

Распределенная ИТ-инфраструктура

ЦЕЛЬ

получить эффективный инструмент для контроля над информационными ресурсами и предотвращения инцидентов информационной безопасности до того, как будет причинён ущерб

*В целях соблюдения конфиденциальности название банка обезличено

MAKVES DCAP

MAKVES ТЕПЕРЬ ЧАСТЬ ГАРДА

ОПЫТ РОССИЙСКОГО БАНКА. ЗАДАЧИ

Наведение порядка на файловых хранилищах

Поиск данных, содержащих конфиденциальную информацию, копий критичных документов в папках общего доступа

Получение оперативных уведомлений

о нарушениях, связанных с действиями пользователей и событиями с конфиденциальной информацией

Контроль

над правами и действиями пользователей. Своевременный отзыв доступа у уволенных пользователей

Хранение журналов событий

для расследования инцидентов в соответствии с требованиями отраслевых стандартов и регуляторов

ЧТО БЫЛО РЕАЛИЗОВАНО

MAKVES ТЕПЕРЬ ЧАСТЬ ГАРДА

1 ЭТАП. АУДИТ И РЕКОМЕНДАЦИИ

Риски, связанные с нарушением логического доступа

Обнаружены уволенные сотрудники с активным доступом к информационным ресурсам

750 сотрудников с паролем без срока действия

Более 1000 учетных записей сотрудников, **2 месяца** не заходивших в систему

Анализ файловых хранилищ 320 Тб данных

Категоризация: персональные данные, банковская тайна и другие категории конфиденциальной информации

Обнаружено **30% дубликатов** файлов
25% файлов **не использовались более 3-х лет**

Файлы, попадающую под категорию банковская тайна и персональные данные, в общем доступе

MAKVES
ТЕПЕРЬ ЧАСТЬ ГАРДА

ЧТО БЫЛО РЕАЛИЗОВАНО

1 ЭТАП. АУДИТ И РЕКОМЕНДАЦИИ

В кратчайшие сроки на основе нейросетей* были обработаны десятки тысяч документов.
Ручная категоризация файлов с изображениями при таком объёме данных – задача нереализуемая

- Водительские права
- Банковские карты
- Полис ОМС
- Документы об образовании
- СНИЛС (старого и нового образца)
- Пенсионное удостоверение
- Загранпаспорт
- Военный билет
- Офисные документы*
- Прочие изображения
- Паспорта РФ и СНГ

* определение печатей, штампов, подписей, ЭЦП, таблиц, графиков, реквизитов

ЧТО БЫЛО РЕАЛИЗОВАНО

2 ЭТАП

АДАПТАЦИЯ ВОЗМОЖНОСТЕЙ СИСТЕМЫ ПОД ЗАДАЧИ БАНКА

Настройка хранения и регистрации событий в соответствии с требованиями регуляторов

Настройка автоматических оповещений о критичных событиях и сценариев реагирования на инциденты

Контроль логического доступа к информационным системам в соответствии с должностными обязанностями

Контроль подключенных почтовых ящиков. Обнаружение нелегитимного доступа к почтовым ящикам

Контроль действий с документами, содержащими персональные данные и банковскую тайну: создание, удаление, изменение, копирование

Интеграция с существующими системами информационной безопасности: SIEM, DLP, Антивирусы

Мониторинг активности пользователей и событий. Регулярный анализ соответствия модели доступа политикам компании

РЕЗУЛЬТАТЫ

01 Оперативное выявление причин сбоев

02 Соответствие наличия доступа к информации у надлежащих учетных записей сотрудников

03 Автоматизация рутинных процессов, увеличение эффективности ИТ и ИБ отделов

04 Уменьшение поверхности потенциальной кибератаки

05 Поддержание доступности и целостности важных данных для поддержания непрерывности бизнес-процессов

06 Инструмент для расследования инцидентов

07 Уменьшилось количество инцидентов безопасности после внедрения

08 Предотвращение штрафов за нарушение ФЗ-152

Комплексное выполнение требований регуляторов

- ГОСТ Р 57580.1-2017,
- № 152-ФЗ,
- № 787-П, №716-П,
- PCI DSS, СТО БР ИББС
- Указ Президента РФ № 250 от 1 мая 2022 г.

MAKVES СЕГОДНЯ

MAKVES ТЕПЕРЬ ЧАСТЬ ГАРДА

В реестре Минцифры

Сертификат ФСТЭК

Часть группы компаний «Гарда»

Первые на российском рынке DCAP

Сертификаты совместимости с РедОС и Astra Linux

Узнайте больше в нашем телеграм-канале