SecretTechnologies

DataMask

Универсальное решение по маскированию данных

Леонид Варламов

Заместитель генерального директора
по развитию продуктов собственной разработки

Алексей Корнюхин

Руководитель отдела
разработки маскирования данных

О компании Secret Technologies

SecretTechnologies

семейство продуктов **Secret Cloud**

безопасный файловый обмен с сотрудниками и партнерами
SCE сертифицирован ФСТЭК РФ по 4 уровню доверия

с 2016 года
на рынке ИБ

DataMask

обезличивание чувствительных данных

Trace Doc

создание уникальных копий документов

> 100 тысяч
пользователей продуктов

Screen Guard

защита экрана монитора от фотографирования

Printer Guard

контроль и экономия печати

7 продуктов
в Реестре отечественного ПО

Проблема утечек персональных данных

SecretTechnologies

«Ростелеком» сообщила о возможной утечке данных из инфраструктуры подрядчика

22/01/25

Как защититься от мошенников, 16 янв, 05:33 | 5 735 | Поделиться

Роскомнадзор выявил утечку 710 млн записей о россиянах за 2024 год

Сюжет
Как защититься от мошенников

Главная · Новости

Хакеры заявили о взломе «АльфаСтрахование-Жизнь»

Компьютерра
15 января 2025

На чтение: 1 минута Нравится:

Данные покупателей алкоголя в сети ВинЛаб выложили в свободный доступ

Екатерина Быстрова 08 июля 2024 - 09:02

Домашние пользователи | Утечки информации | Умышленные утечки информации | Кража данных

05 декабря 2024 · Технологии

«Почта России» начала проверку из-за сообщений об утечке данных пользователей

В открытом доступе опубликованы данные пользователей «Бургер Кинг»

Мария Нефёдова , 10.10.2024 Комментарии 12716

Как сообщили аналитики Data Leakage & Breach Intelligence (DLBI), в сети опубликованы данные клиентов сети быстрого питания «Бургер Кинг». В компании подтвердили утечку, но

Финансы, 06 ноя 2024, 12:41 | 108 215 | Поделиться

«Сбер» оценил долю утекших данных взрослых россиян в 90%

По оценкам «Сбера», в открытом доступе уже находятся около 3,5 млрд строк, содержащих персональные данные россиян. 2023 год стал пиком утечек данных, которые в основном допускают интернет-магазины и медицинские учреждения

Коммерсантъ

$ 94,04 € 98,01 ¥ 12,37 IMOEX 3208,70 Разговор Путина и Трампа Weekend №3–2025 Валютный п

Потребительский рынок
11.12.2024, 15:20

Ритейлер Metro проверяет возможную утечку данных

Российский ритейлер Metro проверяет вероятную утечку базы данных клиентов, произошедшую в апреле 2024 года, сообщила пресс-служба компании. Внешние источники могли получить личные сведения, в том числе фамилию, имя, электронный адрес и номер телефона клиента. Утечка не затронула пароли, кэш и платежные данные клиентов, уточнили в Metro.

Последствия утечек персональных данных

SecretTechnologies

Финансовые потери

- штрафы за нарушение законов о защите ПДн
- расходы на ликвидацию последствий утечки
- потенциальные судебные издержки
- снижение рыночной стоимости компании

Конкурентные риски

- утрата коммерческой тайны
- потеря рыночных позиций
- снижение инвестиционной привлекательности
- возможность использования данных конкурентами

Репутационный ущерб

- потеря доверия клиентов и партнёров
- негативная медиа-повестка
- сложности с привлечением новых клиентов

Операционные последствия

- простой бизнес-процессов
- падение производительности
- выделение ресурсов на устранение последствий
- необходимость обновления систем безопасности
- возможные изменения в ИТ-инфраструктуре

Влияние на персонал

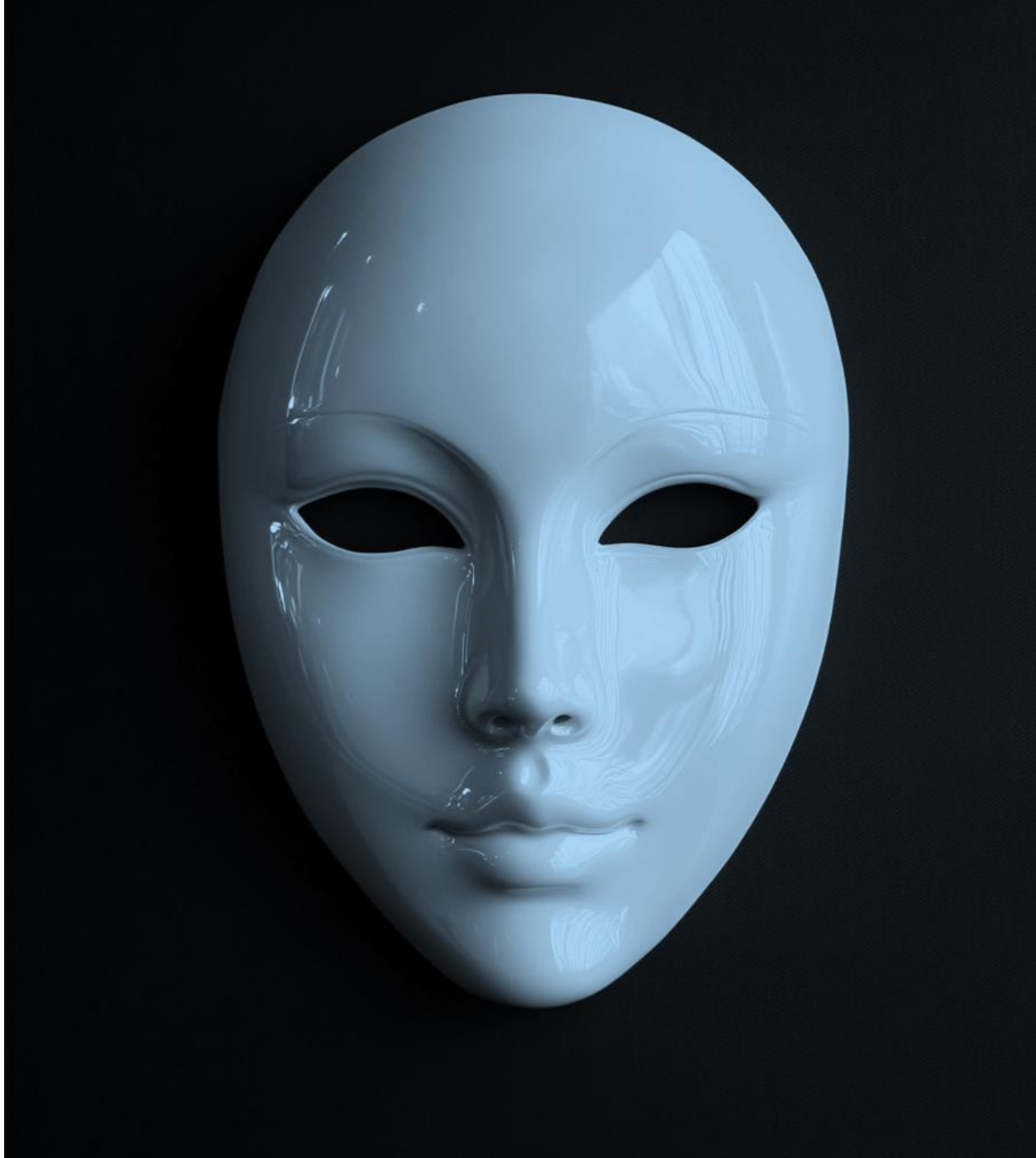
- падение морального духа сотрудников
- снижение лояльности сотрудников

Штрафы за утечку персональных данных

SecretTechnologies

Нарушение (КоАП РФ)	Было (152-ФЗ)	Будет с 30.05.2025 (420-ФЗ)
Сокрытие от госорганов факта утечки ПДн		1-3 млн. руб.
Утечка до 10 000 ФИО	100-300 тыс. руб.	3-5 млн. руб.
Утечка до 100 тыс. ФИО	100-300 тыс. руб.	5-10 млн. руб.
Утечка более 100 тыс. ФИО	100-300 тыс. руб.	10-15 млн. руб.
Повторная утечка ПДн	100-300 тыс. руб.	1-3% от выручки за предыдущий год (не менее 20 и до 500 млн. руб.)
Утечка специальных ПДн	100-300 тыс. руб.	15-20 млн. руб.
Утечка биометрических ПДн	100-300 тыс. руб.	15-20 млн. руб.
Повторная утечка специальных или биометрических ПДн	100-300 тыс. руб.	1-3% от выручки за предыдущий год (не менее 25 и до 500 млн. руб.)

Эти проблемы решают профессиональные системы маскирования данных



Что такое маскирование данных?

SecretTechnologies

Маскирование данных – это процесс скрытия исходной информации путём преобразования данных в формат, который сохраняет полезность для определённых процессов или тестирований, но делает эти данные бесполезными для злоумышленников.

Цели маскирования данных

- защита персональных данных и другой конфиденциальной информации
- соблюдение регуляторных требований
- предотвращение утечек данных как изнутри, так и снаружи организации

Как работает маскирование данных

- профилирование данных: автоматическое определение чувствительной информации в базе данных
- обезличивание: замена реальных данных на фиктивные с сохранением структуры и логических связей
- предотвращение восстановления: маскированные данные невозможно преобразовать обратно в исходные

Методы маскирования данных

- по словарю: учет пола, лица, формулировок в документах
- посимвольная замена: замена каждого символа на другой
- на основе контрольных знаков: использование алгоритмов для номеров (ИНН, ОГРН)
- замена на константу: все чувствительные данные заменяются одинаковым значением

Как выглядят замаскированные данные?

SecretTechnologies

	Исходные данные		Замаскированные данные	
name	Андрей Воронин	→	Никита Пушкин	замена по словарю
e-mail	voronin@corp.ru	→	pyshkin@corp.ru	e-mail по фамилии
credit_card	4111-6420-7553-1464	→	4111-4325-2277-8300	учёт алгоритма Луна
inn	771866142018	→	771887294237	сохранение региона
date_of_birth	1984-04-04	→	1979-05-12	диапазон 40-50 лет

Зачем нужны системы маскирования?

SecretTechnologies

Надежность и безопасность

- проверенные алгоритмы маскирования
- соответствие стандартам и нормативам

Универсальность применения

- поддержка различных типов баз данных и форматов
- возможность настройки под специфические требования

Простота использования

- предустановленные шаблоны и политики маскирования
- возможность быстрого развертывания

Эффективность работы

- быстрая обработка больших объемов данных
- автоматизация процессов маскирования

Экономический эффект

- снижение затрат на разработку и поддержку собственных решений
- уменьшение рисков финансовых потерь от утечек данных

Сохранение целостности данных

- поддержание целостности
- сохранение статистических свойств данных

DATA MASK

Отечественное решение по маскированию чувствительных данных

Когда нужен DataMask?

SecretTechnologies

Соблюдение требований регуляторов

- при работе с персональными данными клиентов маскирование помогает выполнять законодательные нормы по защите информации

Разработка и тестирование

- в тестовых средах небезопасно использовать реальные данные, при этом важно сохранить их структуру для минимизации ошибок при разработке ИТ-продукта
- маскирование данных позволяет сохранить логику представления данных в базе без риска раскрытия конфиденциальной информации

Предотвращение утечек

- при получении злоумышленником доступа к базам данных маскирование не позволит извлечь реальную информацию из них

Аутсорсинг

- когда данные передаются внешним подрядчикам, маскирование необходимо для обеспечения конфиденциальности информации при её обработке третьими лицами

Аналитика данных

- при масштабном анализе данных важно обеспечить анонимность, сохраняя при этом статистическую ценность информации

Почему DataMask?

SecretTechnologies

Реалистичность

- обезличивание данных с сохранением смысла и структуры информации в зависимости от типа данных
- индивидуальный ключ маскирования для каждого заказчика, обеспечивающий уникальность алгоритмов маскирования
- автоматическое определение типов данных, в том числе с помощью ИИ
- поддержка большого количества СУБД: Postgres, Oracle, MS SQL, Maria DB, и др.

Целостность

Необратимость

- настройка и адаптация решения под конкретные потребности клиента, включая правила маскирования, алгоритмы обработки и интеграцию с существующими системами
- визуальный конструктор процессов маскирования *[in dev…]*
- мы не храним маскируемые данные

Однородность

Политика лицензирования DataMask

Корпоративное решение (12 месяцев или бессрочно)

- **модуль «Базовый сервер** (неотказоустойчивое исполнение)
- или **модуль «Корпоративный сервер»** (отказоустойчивое исполнение)
- **модуль «Профилирование»** – автоматическое определение типа данных (от 5 потоков* до ∞)
- **модуль «Маскирование»** – маскирование данных после профилирования (от 5 потоков* до ∞)
- **стоимость внедрения** – рассчитывается индивидуально

Решение для СМБ/разовых задач (12 месяцев)

- **модуль «All-In-One»** – серверная лицензия и маскирование (1 поток*)
- **стоимость внедрения** – рассчитывается индивидуально

**1 поток – скорость профилирования или маскирования данных, ~80 ГБ/сутки*

Тестирование DataMask*

Встреча в формате ВКС

- демонстрация ключевых возможностей решения
- обсуждение ваших потребностей и задач
- ответы на вопросы в реальном времени

Пилотный проект

- адаптация под ваши политики безопасности
- учёт особенностей ваших баз данных
- практическое тестирование в вашей инфраструктуре

**Для организации встречи и обсуждения пилотного проекта обратитесь к вашему менеджеру в компании Softline*