Решения для бизнеса

KASPERSKY lab

Kaspersky®
Fraud Prevention

Kaspersky Fraud Prevention

для здравоохранения

Цифровая трансформация в сфере здравоохранения набирает обороты. Kaspersky Fraud Prevention призван помочь организациям, предоставляющим медицинские услуги, добиться идеального баланса между защитой персональных данных и ожиданиями клиентов.

www.kaspersky.ru/enterprise-security/fraud-prevention

#truecybersecurity

Взгляд на индустрию

Для медицинских организаций цифровая трансформация означает возможность сфокусироваться на работе с пациентами, не тратя ценные ресурсы на бумажную волокиту. Однако технологический прогресс, хотя и дает огромные преимущества, сопряжен с дополнительным риском кражи ценных данных. Ниже перечислены некоторые потенциальные угрозы, актуальные для медицинских организаций.

Факты и статистика

В 2017 году медицинские учреждения становились жертвами примерно 2000 кибератак на ежедневной основе - в двое чаще, чем организации в других отраслях.

Данные пациентов стоят в разы больше, чем данные кредитных карт.

В данный момент на продажу в сети выставлены медицинские данные около 140 млн. пациентов.

Мировые затраты на кибербезопасность в сфере здравоохранения увеличиваются на 4.1% ежегодно и должны превысить 56 млрд. долларов в общей сумме к 2021 году.

Мировый рынок мобильных приложений, используемых в сфере здравоохранения, оценивается примерно в 30 млрд. долларов и должен достичь около 100 млрд. долларов к 2023 году.

Изменение пароля или блокировка кредитной карты могут помочь защитить от злоумышленников финансовую информацию, однако добытые ими медицинские сведения своей ценности уже не потеряют. Сейчас учетные записи пользователей хранят медицинскую информацию, номер медицинской страховки, контактные данные, номера социального страхования (США), а также сведения о медицинских счетах и их оплате.

Добытые нелегальным путем медицинские данные предоставляют мошенникам неограниченные возможности: это и незаконное получение медицинских услуг, и продажа информации, а также использование страховых полисов, приобретение лекарств, отпускаемых по рецепту, и др.

Для поставщиков медицинских услуг обеспечение IT-безопасности не входит в список первоочередных задач – их главной целью является спасение жизней, а все остальные вопросы считаются второстепенными. Тем не менее, учитывая растущее использование врачами и другим медицинским персоналом мобильных технологий для доступа к данным пациентов, крайне важно защитить эту информацию от все более изощренных кибератак.

Пациенты, использующие мобильные медицинские приложения, сталкиваются с такими же рисками. Они также нуждаются в усиленной защите в этой быстро развивающейся области.

В последнее время постоянно появляются сообщения об инцидентах, связанных с компрометацией медицинских данных. В первом квартале 2018 года только в США в результате 110 таких инцидентов было скомпрометировано около 1,13 млн медицинских карт. В июле 2018 года в Сингапуре хакеры взломали государственную базу данных системы здравоохранения, получив почти на целую неделю доступ к данным приблизительно 1,5 млн пациентов (включая премьер-министра страны). А в Великобритании Информационный центр Национальной службы здравоохранения NHS Digital пострадал от утечки данных, в результате которой была нарушена конфиденциальность 150 тыс. пациентов.

На поставщиков медицинских услуг возложена непростая задача по предотвращению нарушений, защите пациентов от вмешательства в их данные и обеспечению безопасности подключенных устройств. Учитывая жизненную важность этих данных и устройств, профилактика в данном случае имеет решающее значение. В то же время повышение уровня безопасности не должно вести к снижению удобства для пользователей.

Предотвращение мошенничества в сфере здравоохранения

Мошеннические учетные записи

- Обнаружение аккаунтов, использующихся для злоупотребления возможностями сервиса
- Распознавание новых устройств или тех, которые используются для различных учетных записей

Кража учетной записи

- Выявление кражи учетной записи, как на этапе логина, так и на протяжении всей сессии
- Обнаружение подозрительной активности в режиме реального времени
- Возможность предотвращения потенциальных потерь

Kaspersky Fraud Prevention

Благодаря обширному экспертному опыту «Лаборатории Касперского» в сфере кибербезопасности и высочайшему качеству предоставляемой защиты Kaspersky Fraud Prevention помогает поставщикам цифровых услуг добиться оптимального баланса между уровнем безопасности и удобством для клиентов. Гибкое управление инцидентами и возможности цифровой криминалистики позволяют значительно снизить операционные расходы крупных компаний.

Kaspersky Advanced Authentication

- Приоритизация легитимных пользователей
- Аутентификация на основе рисков
- Анализ биометрии, поведения и данных окружения в режиме реального времени
- Легитимные пользователи получают доступ к своим аккаунтам без дополнительной верификации, что позволяет сократить расходы на второй фактор аутентификации

Kaspersky Automated Fraud Analytics

- Мониторинг всех данных и активности во время сессии с использованием передовых технологий машинного обучения
- Выявление мошеннических учетных записей, отмывания денег и кражи учетных записей пользователей
- Выстраивание и сопоставление взаимосвязей между пользователями, сессиями, устройствами и организациями по всему миру

Группа исследования и анализа мошеннических инцидентов

Обширный экспертный опыт аналитиков «Лаборатории Касперского», передовые технологии и глобальная база знаний об угрозах помогут вам развивать свой бизнес, не беспокоясь о проблемах с безопасностью и удобством использования ваших сервисов.

Защита от мошенничества для вас - быстрый и удобный сервис для ваших клиентов

Реальное машинное обучение

Экспертиза и расследование мошенничества

Снижение операционных издержек

Automated Fraud Analytics

- Мониторинг всех данных и активности во время пользовательской сессии
- Выявление мошеннических учетных записей, кражи аккаунтов пользователей и случаев отмывания денежных средств
- Выстраивание и сопоставление взаимосвязей между пользователями, сессиями, устройствами и организациями по всему миру

Advanced Authentication

- Аутентификация на основе рисков (RBA)
- Непрерывный анализ биометрических, поведенческих показателей и данных окружения в режиме реального времени
- Сокращение расходов на второй фактор аутентификации

Чтобы заказать демо-версию, отправьте заявку на kfp@kaspersky.com

Kaspersky Lab
Enterprise Cybersecurity:
www.kaspersky.com/enterprise
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com**

#ИстиннаяБезопасность
#HuMachine

www.kaspersky.com/fraudprevention
www.kaspersky.ru/enterprise-security/fraud-prevention