kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky
Fraud Prevention

Kaspersky Fraud Prevention для здравоохранения

Переход здравоохранительных учреждений на цифровую документацию предполагает, что врачи, не тратя время на написание бумаг, смогут больше внимания уделять пациентам. Однако технологический прогресс имеет и обратную сторону, и наряду с ростом возможностей и преимуществ увеличивается и риск кражи ценных данных. Рассмотрим основные проблемы кибербезопасности для медицинских организаций.

Немного фактов и статистики

Медицинские карты пациентов стоят намного дороже, чем похищенные данные банковских карт.

В мире в целом расходы на кибербезопасность в сфере здравоохранения ежегодно растут на **4,1%**. Ожидается, что к 2021 г. они превысят **65 млрд долларов**.[1]

Глобальный рынок мобильных медицинских приложений оценивается в **28,32 млрд долларов**, и предполагается, что к 2023 г. этот показатель должен достичь **102,35 млрд долларов**.[2]

Взгляд на индустрию

В то время как банковские данные становятся бесполезны после смены паролей или блокировки банковских карт, ценность медицинских данных остается прежней. В учётных записях пациентов теперь хранятся данные их медицинских карт, информация о страховке, контактная информация, номера полиса ОМС и платежные данные.

Краденые медицинские данные открывают перед мошенниками бесконечные возможности: махинации с медицинскими полисами, неправомочное пользование медицинскими услугами, продажа информации, приобретение лекарств, отпускаемых только по рецептам, и т.п. Обеспечение IT-безопасности не является приоритетом для медицинских учреждений, поскольку их главная задача – спасать жизни, а все остальное вторично. Однако сейчас, когда врачи и весь медицинский персонал всё активнее используют мобильные технологии для доступа к данным пациентов, особенно важно защитить информацию от киберпреступников, чьи методы становятся все изощреннее.

Пациентам, использующим мобильные медицинские приложения, угрожает та же опасность. В этой динамично развивающейся области в защите нуждаются обе стороны. Случаи нелегального доступа к медицинским данным происходят постоянно, и вряд ли в ближайшем будущем их станет меньше. В первом квартале 2018 г. только в США произошло 110 случаев утечки данных в сфере здравоохранения, в результате чего было скомпрометировано порядка 1,13 млн записей пациентов. В июле 2018 г. в Сингапуре хакеры взломали государственную медицинскую базу данных, получив меньше чем за неделю доступ к данным около 1,5 млн пациентов, включая премьер-министра.

На здравоохранительные учреждения возложены обязанности по предотвращению утечек данных, защите пациентов от искаженной информации и обеспечению безопасности подключенных устройств. Так как эти данные и устройства очень важны, предотвращение инцидентов должно быть приоритетной задачей. В то же время нельзя выстраивать безопасность за счёт удобства пользования устройствами и приложениями.

1 cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/
2 markets.businessinsider.com/news/stocks/28-32-billion-mobile-health-mhealth-app-market-2017-market-is-projected-to-reach-102-billion-by-2023-1011556625
3 healthitsecurity.com/news/1.13m-records-exposed-by-110-healthcare-data-breaches-in-q1-2018
4 healthcareitnews.com/news/hackers-breach-15-million-singapore-patient-records-including-prime-ministers

Предотвращение мошенничества в здравоохранении

Мошеннические учётные записи
Обнаружение аккаунтов, использующихся для злоупотребления возможностями сервиса
Распознавание новых устройств или тех, которые используются для различных учётных записей
Кража учётной записи
Выявление кражи учётной 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 учётных записей, отмывания денег и кражи учётных записей пользователей
- Выстраивание и сопоставление взаимосвязей между пользователями, сессиями, устройствами и организациями по всему миру

Команда 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. Kaspersky Fraud Prevention

Реальное машинное обучение

Экспертиза и расследование мошенничества

Сокращение операционных расходов

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
Threat Intelligence Portal: opentip.kaspersky.com

www.kaspersky.ru

Kaspersky Fraud Prevention

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

Подробнее на www.kfp.kaspersky.com/ru/

@KasperskyFP