Информационная безопасность в бизнесе: зачем компаниям платформы для корпоративных коммуникаций?

Андрей Кузнецов, исполнительный директор и сооснователь платформы корпоративных коммуникаций dialog

Статистика по корпоративным киберпреступлениям в мире

I полугодие 2018 года по данным компании InfoWatch

2,39 млрд — Общее число зарегистрированных утечек информации в I полугодии 2018 года

- 64,5% внутренние нарушения
- 35,5% внешние атаки

Распределение по отраслям*

- Высокотехнологичные компании — 25,6%
- Муниципальные учреждения — 20,2%
- Госорганы, силовые структуры — 12,9%

Виновники утечек

- Сотрудники — 50,6%
- Внешние злоумышленники — 43,7%
- Бывшие сотрудники — 2,8%

Источники: www.infowatch.ru/report2018_half

* По объему скомпрометированных данных

dialog

Самые опасные мобильные приложения - мессенджеры

Случаи утечек данных из мессенджеров

TOP-3 самых опасных мобильных приложений для корпоративных клиентов: рейтинг аналитической компании **Appthority**.

WhatsApp

Facebook

Telegram

2018 Массовые фишинговые атаки в **WhatsApp** и **Facebook**.

2017 Через **Facebook Messenger** хакеры получили информацию о расположении военных частей в секторе Газа и другим данным посредством распространения вредоносного ПО через сообщения интимного характера.

2016 Иранские хакеры использовали уязвимость **Telegram** и скомпрометировали телефонные номера **более 15 млн** пользователей.

Источники:
Appthority Q2 2018 Enterprise Mobile Security Pulse Report
https://www.infowatch.ru/analytics/digest/19554

Риски использования публичных мессенджеров: человеческий фактор

Социальная инженерия

Мошеннические методики с целью получения конфиденциальной информации

Случайный фактор

Неосмотрительность сотрудников, утеря оборудования

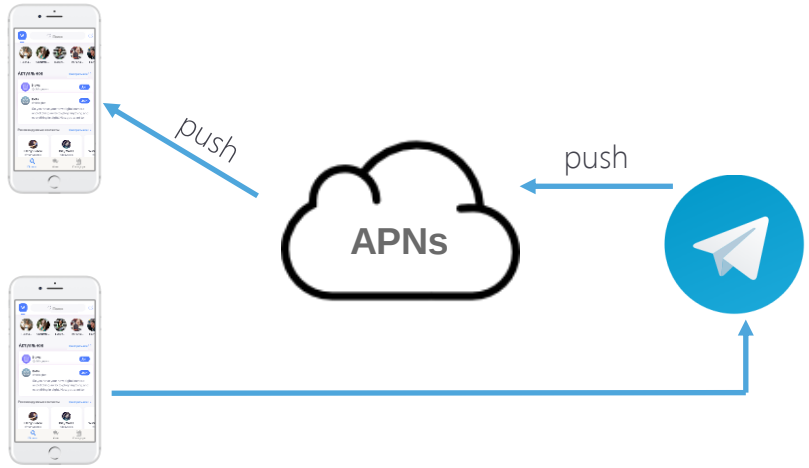
Бывшие сотрудники

Информация, которая остается на устройствах сотрудников, уже не работающих в компании

Риски использования публичных мессенджеров: технический фактор

1. Уязвимость протокола SS7
2. Вирусы
3. Атаки «Man in the Middle»
4. Утечка информации через push-уведомления

При использовании публичных мессенджеров всегда есть третья сторона



Утечки корпоративных данных с облачных сервисов

Проблема доверия администрации и сотрудникам облачных провайдеров

Уязвимости инфраструктур облачных сервисов

CLOUD Act

закон в США, предоставляющий спецслужбам США и других стран прямой доступ к пользовательским данным популярных сервисов

Отсутствие конфиденциальности коммерческих данных на **Facebook, WhatsApp, Gmail**

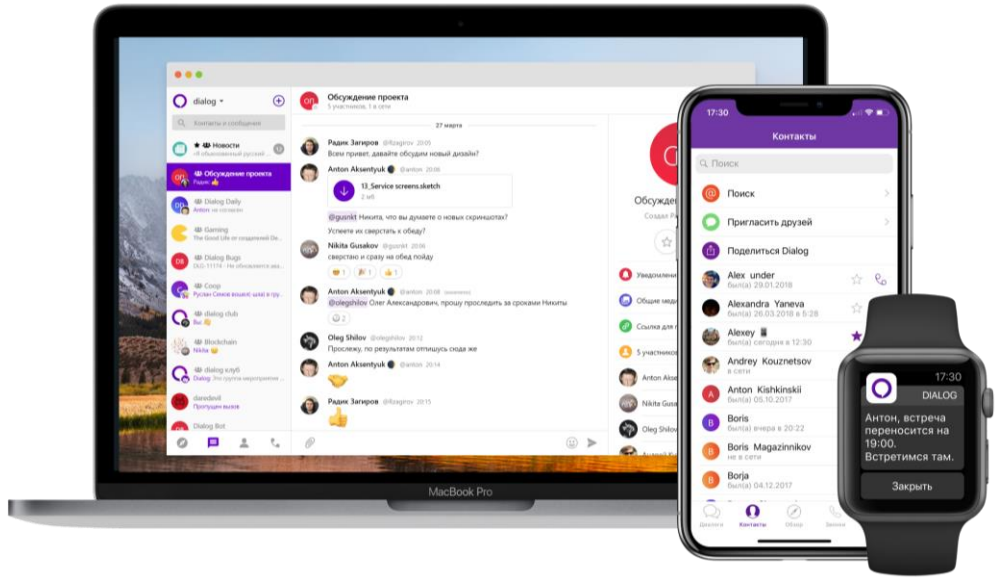
dialog

Простая и безопасная платформа для корпоративных коммуникаций

Российское решение
для совместной работы
и оптимизации бизнес-процессов

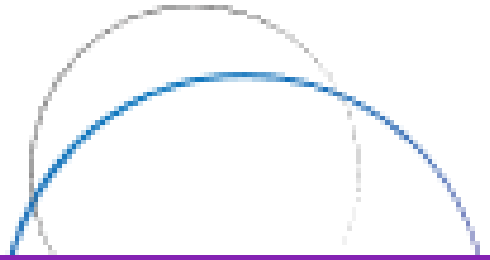
Высокая скорость и удобство
использования на компьютере или смартфоне

Работает на всех платформах –
Android, iOS, macOS, Windows, Linux, Sailfish.



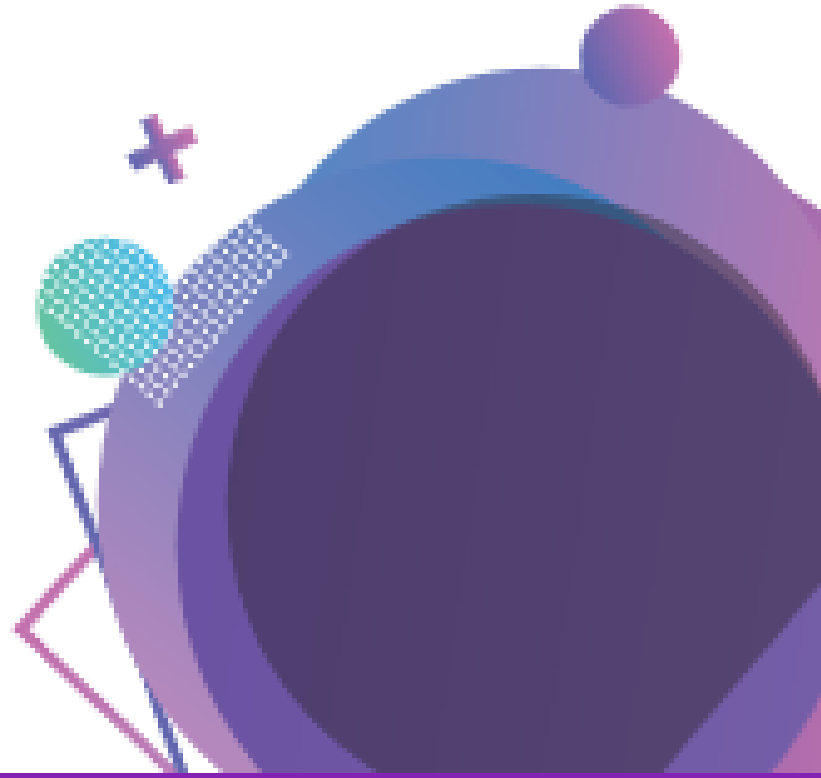
Гарантия безопасности данных

Риски	Средства защиты
Перехват данных	Шифрование трафика и push-уведомлений
Инсайдеры	Интеграция с DLP, SIEM, контроль создания скриншотов
Утеря/кража устройств	Крипто-Контейнеры
Ошибки сотрудников	Отдельная зона для корпоративного общения и Интеграция с DLP
Вирусы	Интеграция с антивирусным ПО
Ошибки в ПО, уязвимости	Регулярный аудит Bi.Zone



Зачем компаниям платформы для корпоративных коммуникаций

- Привычный интерфейс и функционал массового мессенджера с высоким уровнем безопасности
- Централизованный контроль доступа
- Контроль раскрытия информации третьим сторонам
- Интеграция с системами безопасности
- Исключение внешних угроз в виде человеческого фактора и социальной инженерии
- Автоматизация бизнес-процессов
- Сокращение расходов на связь за счет интеграции с телефонией



Наши контакты

Сайт dlg.im
E-mail sales@dlg.im

Приходите на стенд №15