Цифровая безопасность бизнеса

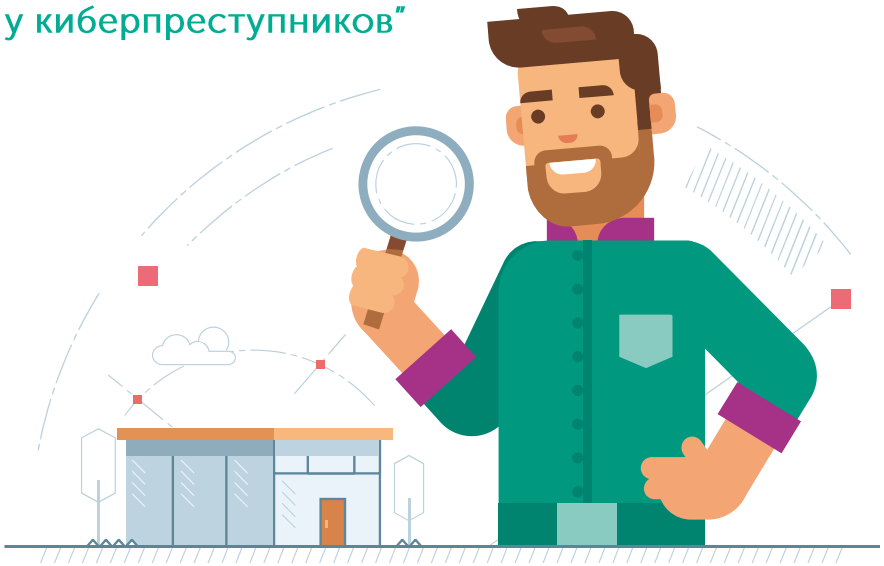
Тимур Бигулов
руководитель отдела продаж
клиентам малого и среднего бизнеса

kaspersky

Опасное заблуждение

СМБ-компании считают:

“Мы слишком малы,
чтобы вызывать интерес
у киберпреступников”



Реальная статистика:

50% успешных атак на СМБ проведены организованными киберпреступными группировками*

58% жертв попадают в категорию «малый бизнес»*

60% атакованных СМБ-компаний теряют бизнес в течение шести месяцев**

*2018 Data Breach Investigations Report. Verizon

**The Need for Greater Focus on the Cybersecurity Challenges Facing Small and Midsize Businesses

Трудности IT-администрирования в СМБ-секторе

Высокая нагрузка

Для **66%** компаний главная трудность – необходимость управления смешанной IT-средой

Ограниченный бюджет и ресурсы

50% СМБ-компаний считают безопасность рядовой IT-задачей, для решения которой не нужен выделенный IT-специалист

Удаленные сотрудники создают дополнительные риски безопасности

40% компаний в секторе СМБ разрешают своим сотрудникам работать вне офиса

50% сотрудников используют для работы личные устройства, в том числе мобильные

64% небольших компаний хранят конфиденциальную информацию клиентов на мобильных устройствах сотрудников

Контроль и защита рабочих мест

Защита

- Защита от почтовых, файловых и веб-угроз блокирует известное, неизвестное и сложное вредоносное ПО
- Защита от шифровальщиков и эксплойтов выявляет уязвимые приложения
- Восстановление системы позволяет отменить вредоносные действия шифровальщиков
- Сетевой экран блокирует неавторизованные сетевые соединения
- Анализ уязвимостей с рекомендациями по установке исправлений

Контроль и управление

- Веб-Контроль
- Контроль устройств
- Управление установкой исправлений
- Управление шифрованием

Безопасность мобильных устройств

- Мобильный антивирус
- Менеджер паролей
- Веб-Контроль и Контроль функций
- Анти-Вор


2003 ГОД
KASPERSKY lab


СЕГОДНЯ

Безопасность и контроль мобильных устройств сотрудников

Мобильный антивирус и защита от веб-угроз

- Защита в режиме реального времени от вирусов, вредоносных приложений и других угроз
- Блокирование фишинга и вредоносных веб-сайтов

Менеджер паролей

- Защита устройства паролем
- Поддержка Face ID и Touch ID

Ограничение активности, не связанной с работой

- Контроль программ для Android
- Контроль функций

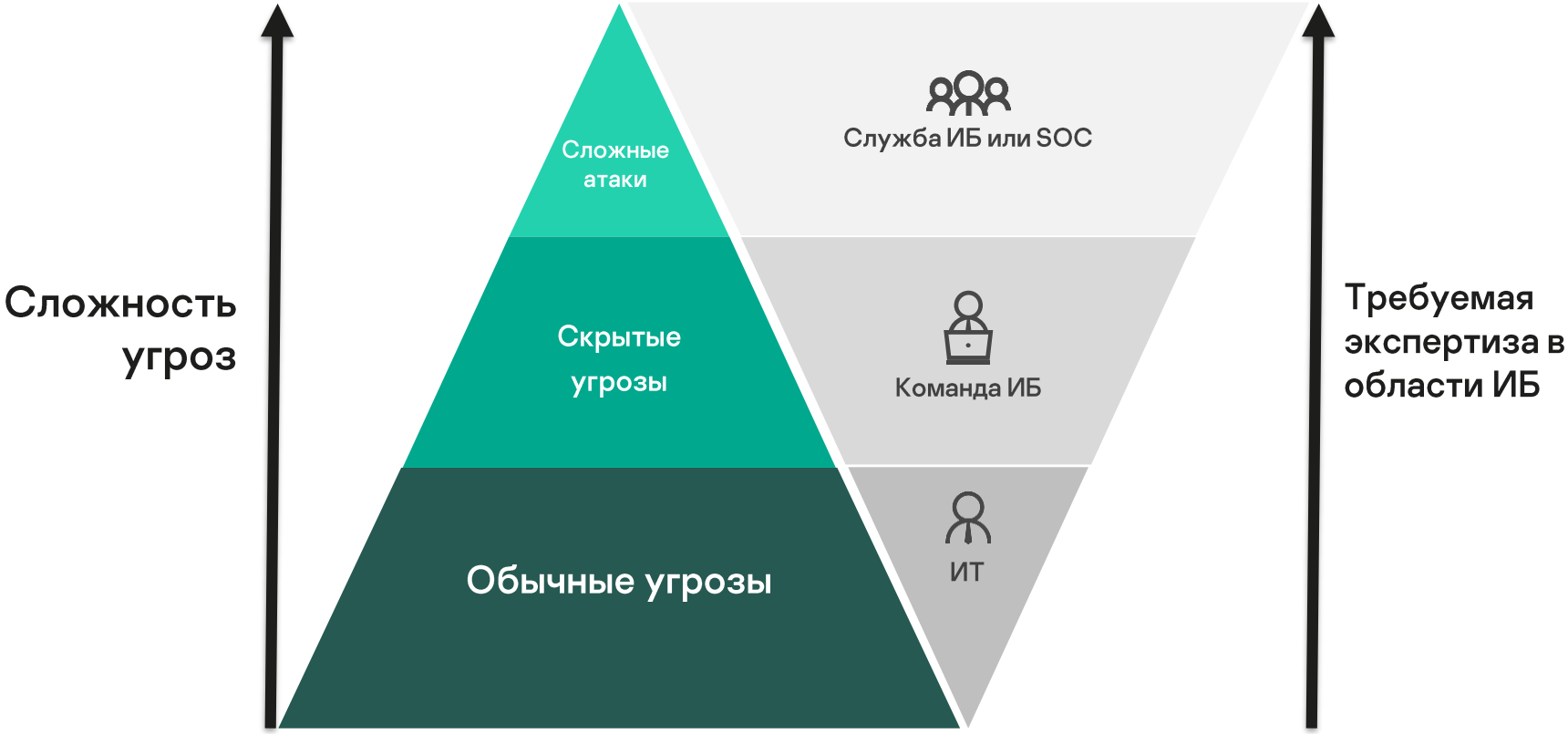
Анти-Вор позволяет удаленно

- Найти на карте/блокировать устройство
- Включить сирену
- Стереть данные

Контроль устройств iOS

- Веб-Контроль
- Настройки proxy
- Ограничение функций (до 40 функций)

Виды угроз и уровень экспертизы



Обычные угрозы

«Классические» вирусы и вредоносное ПО

Широко распространены

70-90% всего вредоносного ПО

Легко предотвратить

Для защиты достаточно сократить поверхность атаки

Надежное обнаружение

С помощью антивирусных и проактивных технологий EPP

Скрытые угрозы

Вредоносное ПО, программы-вымогатели, шпионское ПО и др.

Высокая «заразность»

У злоумышленников есть проверенный набор инструментов для организации атак

Неуловимость

Для доступа к системам и закрепления используются легитимные инструменты и другие способы маскировки

Разрушительность

У скрытых угроз больше времени на то, чтобы нанести максимальный ущерб

Высокая загрузка ИБ-специалистов

Отчетность

Политики

Сотрудники

Оценка соответствия требованиям

Реагирование на инциденты

Настройка

Инновации

Администрирование

Защита от скрытых угроз на всех этапах атаки

Проникновение

Заражение системы через переход по фишинговой ссылке

Установка

Установка злоумышленниками вредоносных компонентов, связи с сервером управления и изучение среды

Закрепление

Закрепление вредоносного ПО в системе с целью перемещения по сети

Повышение киберграмотности сотрудников

Уменьшение поверхности атаки

Автоматическое предотвращение угроз

Расширенные механизмы обнаружения, включая поведенческий анализ на основе машинного обучения и песочницу

Автоматизированный активный поиск угроз с помощью IoA

Анализ первопричин и поиск IoC

Автоматическое, удаленное реагирование и реагирование по инструкциям

Лучшие отраслевые стандарты

Рекомендации ‘Cyber Security: Small Business Guide’ от Национального центра компьютерной безопасности (Великобритания)

- Установите и активируйте антивирус
- Включите сетевой экран
- Включите защиту паролем
- Регулярно обновляйте приложения
- Регулярно обновляйте ОС и ПО на устройствах
- Регулярно устанавливайте патчи и исправления
- Контролируйте использование USB-носителей
- Ограничивайте загрузку сторонних приложений
- Установите приложения для отслеживания устройств (такие как Find my iPhone)

Спасибо!

Давайте поговорим!

kaspersky