Информационная безопасность как облачный сервис

Александр Герасимов

Конференция
«Информационная безопасность бизнеса и госструктур»

Киберугрозы: Crime as a service

- От «стрельбы по площадям» к четко нацеленным атакам по заранее выявленным уязвимостям
- Эффективная маскировка: от явно выраженной угрозы к неявной
- Использование принципов облачного сервиса при организации кибератак:
  - Автоматически исполняемый «сервис»
  - Распределенные ресурсы, подключаемые и высвобождаемые по мере надобности
  - Оплата по факту использования = дешево и доступно!
  - Новое - интеллектуальность: автоматически (само) совершенствующийся сервис!

EUROPOL / Exploring tomorrow's organized crime / 2015

Что умеем защищать сейчас

- ✓ Физические ПК
- ✓ Физические сервера и СХД
- ✓ Физические локальные сети
- ✓ Внутри-корпоративные приложения

Тратим на это более

1 млрд. долл. ежегодно

И то с трудом…

Точечные продукты

Высокая сложность, меньшая эффективность

Ручные и статические механизмы

Медленный отклик, ручное управление, низкая результативность

Слабая прозрачность

Многовекторные и продвинутые угрозы остаются незамеченными

Наличие обходных каналов

Мобильные устройства, Wi-Fi, флешки, ActiveSync, CD/DVD и т.п.

75% CISO считают свои средства защиты «очень» или «всесторонне» эффективными

Что вообще не имеет адекватной защиты

- Умные абонентские устройства
- Глобальные IP-сети
- Публичные онлайн и облачные сервисы

Пользователь не в состоянии противостоять современным кибератакам

Уязвимость сервиса – в «доставке» через публичную IP-сеть

Что будем защищать

- Мобильные абонентские устройства, включая модульные, вне DMZ (внутри виртуальной DMZ)
- IoT устройства вне DMZ (внутри виртуальной DMZ): сенсоры и физические объекты в целом
- Внешние сервисы, в значительной степени определяющие функциональность устройств

Требования к ИБ в «мире IoS»

- Тотальность:

  Аппаратная и территориальная независимость, минимизация требований к защищаемым устройствам, возможность обращения сервиса ИБ к самым разнообразным устройствам

- Измеримый и управляемый уровень безопасности

- Автоматическое исполнение в режиме реального времени

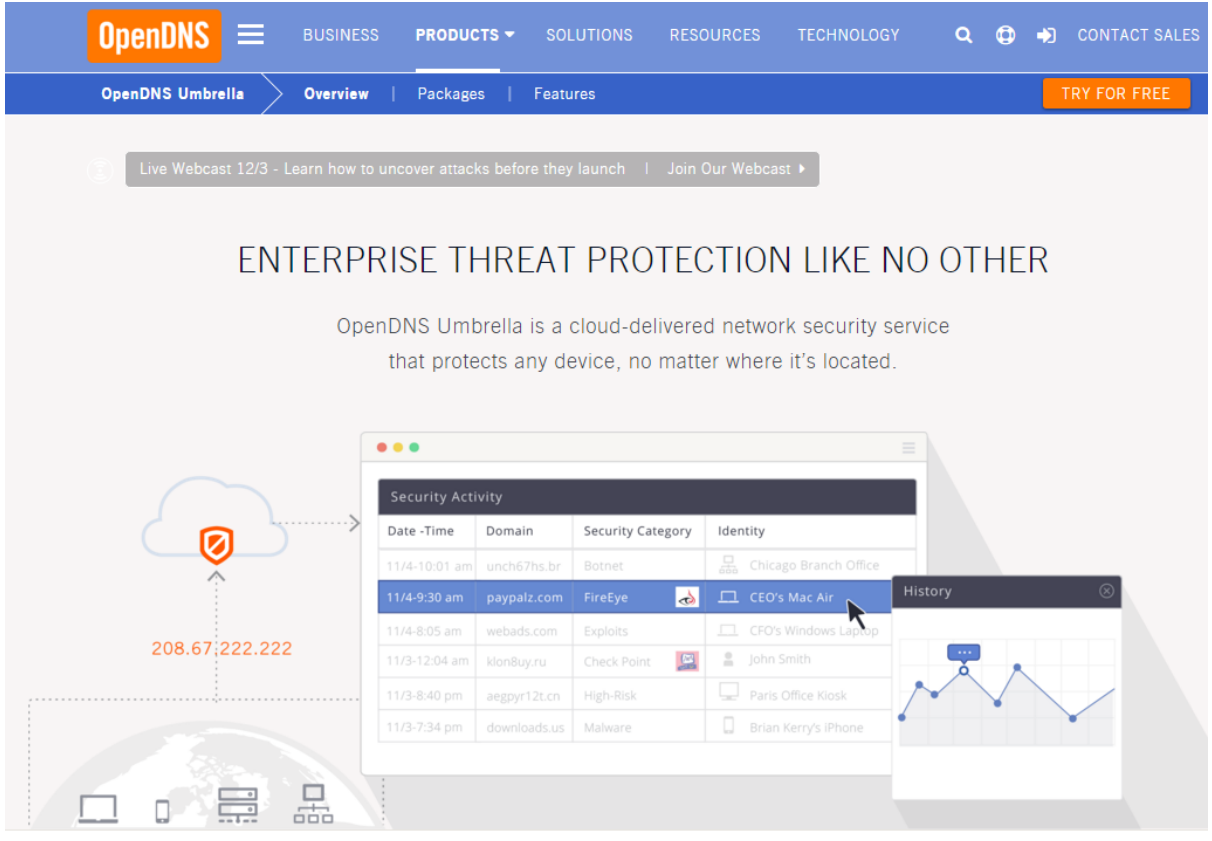
  Сбор и анализ разнообразных данных с целью формирования облика «естественного фона» и отслеживания отклонений от нее как угроз, с последующим анализом адекватности оценок и предпринятых действий

- Возможность автоматического взаимодействия с другими сервисами ИБ

Информационная безопасность как сервис

- Облачная модель (самообслуживание, выделение и высвобождение ресурсов по требованию, автоматическое исполнение)
- Основная задача – не информирование, а предотвращение нежелательных событий
- Многокомпонентность (сервис формируется из набора базовых по отношению к нему сервисов)
- Мощная аналитическая компонента реального времени
- Интеллектуальные (самообучающиеся) алгоритмы
- Прямая монетизация

Информационная безопасность как сервис: пример



Спасибо за внимание!
Вопросы?

Александр Герасимов