

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!

The future of serious and organised crime:

- A virtual and global criminal underground made up of individual criminal entrepreneurs
- Using a **crime-as-a-service business model** and trading in diversified commodities
- Relying on **digital infrastructures, virtual currencies and infiltration**
- Targeting changing pools of victims and clients such as **the elderly or legal business structures.**

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



«Облака» провайдеров
внешних сервисов

Прикладные сетевые
независимые сервисы

Требования к ИБ в «мире IoT»

- **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

The screenshot displays the OpenDNS Umbrella website. The top navigation bar includes the OpenDNS logo, a menu icon, and links for BUSINESS, PRODUCTS, SOLUTIONS, RESOURCES, TECHNOLOGY, a search icon, a shield icon, a plus icon, and CONTACT SALES. Below this, a secondary navigation bar features OpenDNS Umbrella, Overview, Packages, Features, and a TRY FOR FREE button. A banner for a Live Webcast is visible. The main heading reads 'ENTERPRISE THREAT PROTECTION LIKE NO OTHER'. Below this, a text block states: 'OpenDNS Umbrella is a cloud-delivered network security service that protects any device, no matter where it's located.' The central graphic illustrates the service's architecture, showing a cloud with a shield icon and the IP address 208.67.222.222. A 'Security Activity' window is overlaid, displaying a table of security events. A 'History' window with a line graph is also shown.

OpenDNS

BUSINESS PRODUCTS SOLUTIONS RESOURCES TECHNOLOGY

OpenDNS Umbrella Overview Packages Features TRY FOR FREE

Live Webcast 12/3 - Learn how to uncover attacks before they launch | Join Our Webcast

ENTERPRISE THREAT PROTECTION LIKE NO OTHER

OpenDNS Umbrella is a cloud-delivered network security service that protects any device, no matter where it's located.

208.67.222.222

Date -Time	Domain	Security Category	Identity
11/4-10:01 am	unch67hs.br	Botnet	Chicago Branch Office
11/4-9:30 am	paypalz.com	FireEye	CEO's Mac Air
11/4-8:05 am	webads.com	Exploits	CFO's Windows Laptop
11/3-12:04 am	kionBuy.ru	Check Point	John Smith
11/3-8:40 pm	aegpyr12t.cn	High-Risk	Paris Office Kiosk
11/3-7:34 pm	downloads.us	Malware	Brian Kerry's iPhone

History

Спасибо за внимание!
Вопросы?

Александр Герасимов