Большие Данные в информационной безопасности

Наталья Касперская,
генеральный директор
ГК InfoWatch

«Большие данные в национальной экономике», 22 октября, Москва, ЦВК Экспоцентр

Что такое Большие Данные?

INFOWATCH

- Данные, которые слишком **велики** для ручного просмотра
- Позволяют **на всей совокупности** делать выводы, которые нельзя сделать по локальным сегментам
- Данные, в первую очередь, **о людях**
- Данные из **разнородных источников** (интернет-трафик, смартфон, гео-позиционирование, звонки, почта, видео, …)
- Данные **различной природы** (логи, ПДн, тексты, звук, изображения, координаты, поведение, семантика, …)
- Имеющие **временную компоненту** (ретроспективу)

Большие Данные уже собираются

- В маркетинге
- В рознице
- В интернет-рекламе
- В поисковых системах
- В социальных сетях
- В мобильных операторах
- В АНБ

…но не в ИБ предприятия!

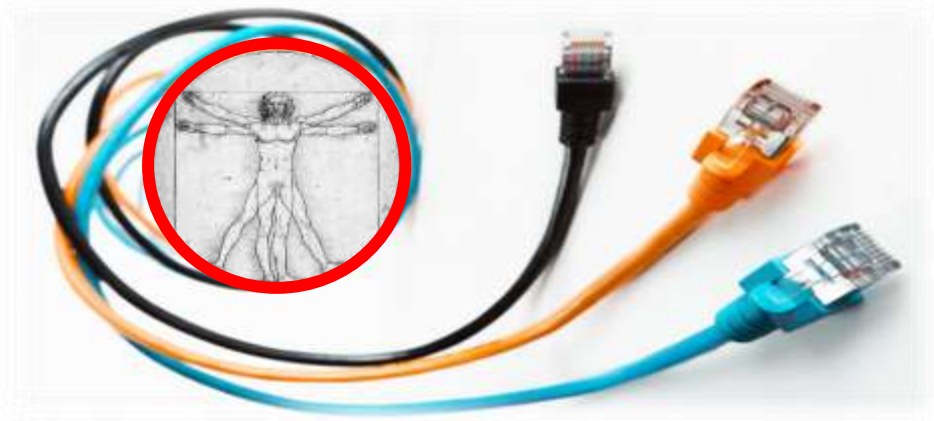
В корпоративной безопасности БД не анализируются

- Системы ИБ используются по отдельности, разрозненно
  - Контентные (DLP, Anti-Spam, Web-filter)
  - Инфраструктурные (Антивирус, Firewall, SIEM, IDS/IPS, НСД, Back-up, …)
  - Шифрование
- Большинство систем не накапливает ретроспективный анализ
- Человеческое поведение не является центром анализа, анализируются **технические явления**

Человек - центр рисков предприятия

Основные риски ИБ в корпорациях создают люди:

- Халатность, разгильдяйство
- Уходы, переманивание
- Хищения, растраты
- Утечки, инсайд
- Потеря клиентов
- Риски репутации
- Юридические риски



Данные внутри корпорации – более полны

- Почта, другие сообщения
- Походы в интернет
- Информация на компьютерах
- Кадровые данные
- Использование устройств

При этом ценность одного конкретного пользователя крайне высока (в отличие от соцсетей)

Будущее – за системами управления рисками

- **Анализ людей**, а не технических явлений
- Совместный анализ **всех источников и потоков данных** для раннего выявления и прогнозирования угроз
- Вычисление **различных видов рисков** (утечки, нелояльность, уязвимости систем, проблемы инфраструктуры и пр.)
- Обязательный **ретроспективный анализ**
- **Единые решающие правила** для вычисления итоговых рисков персонала и ИБ-систем

Проблемы разработки таких систем

- Качественный анализ возможен только с помощью алгоритмов искусственного интеллекта и машинного обучения
- Компании-разработчики ИБ не умеют разрабатывать системы ИИ, так как сосредоточены на технической защите
- Разработки таких систем требуют значительных ресурсов, а рынок пока еще мал
- Разработчики систем анализа Больших данных не занимаются ИБ (в частности, из-за узости рынка), а сосредоточены на электронной коммерции и рознице

Выводы

INFOWATCH

- Системы комплексного анализа рисков и угроз предприятия появятся в ближайшие 3-5 лет
- Они будут основаны на анализе Больших Данных о персонале и инфраструктуре предприятия
- Появление подобных систем позволит перейти от парадигмы реагирования на угрозы к парадигме детектирования и оценки роста рисков в критических точках
- «Технические» решения ИБ будут технологической подложкой для таких систем и поставщиками данных

INFOWATCH®
BECAUSE YOUR DATA
IS YOUR BUSINESS

Спасибо за внимание!

InfoWatch

www.infowatch.ru
+7 495 22 900 22

Наталья Касперская,
генеральный директор
ГК InfoWatch