Digital Security

БЕЗОПАСНОСТЬ КАК ИСКУССТВО

Аудит безопасности информационных систем:

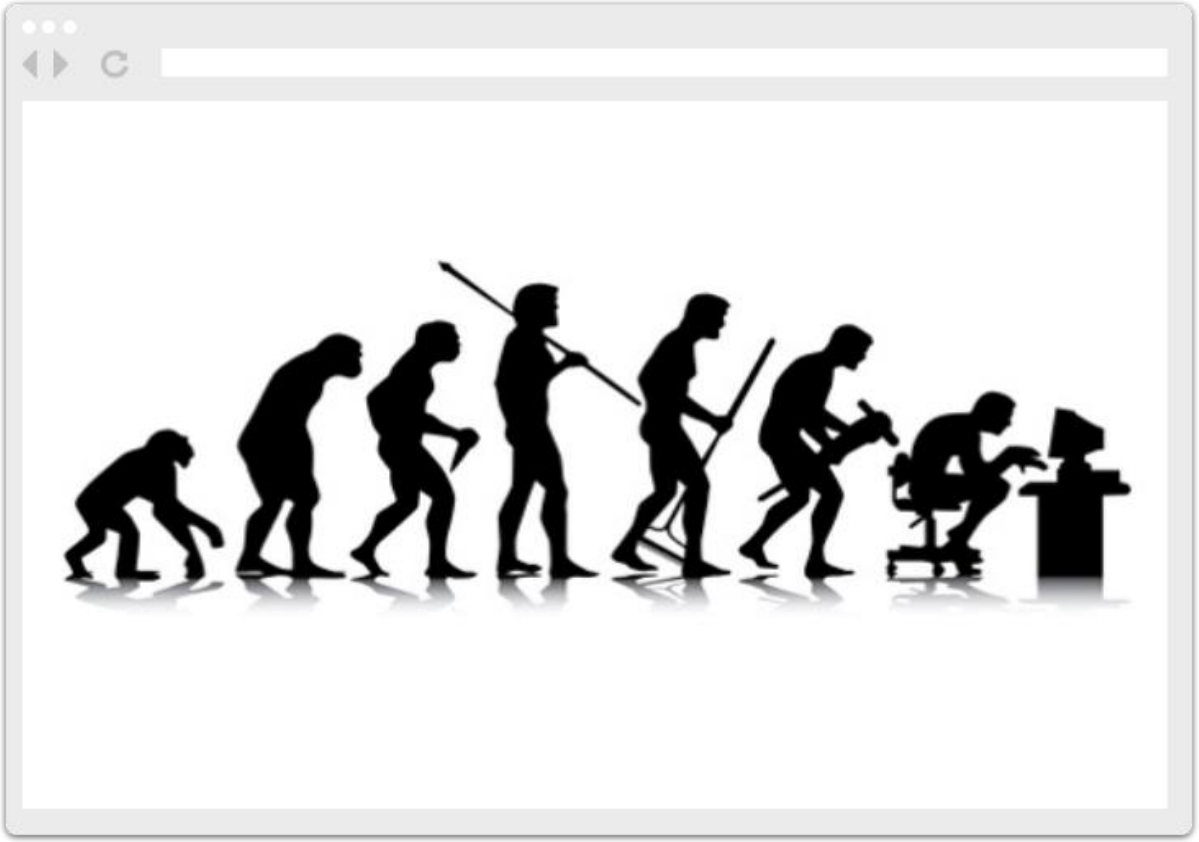
современные тенденции

Илья Медведовский

к. т. н.

Генеральный директор Digital Security

А что у нас? Исторический экскурс



Пентест по внешнему периметру

с 2003 по настоящее время

Внутренний пентест ИС

с 2003 по 2010, с последующим спадом

Пентест веб-приложений

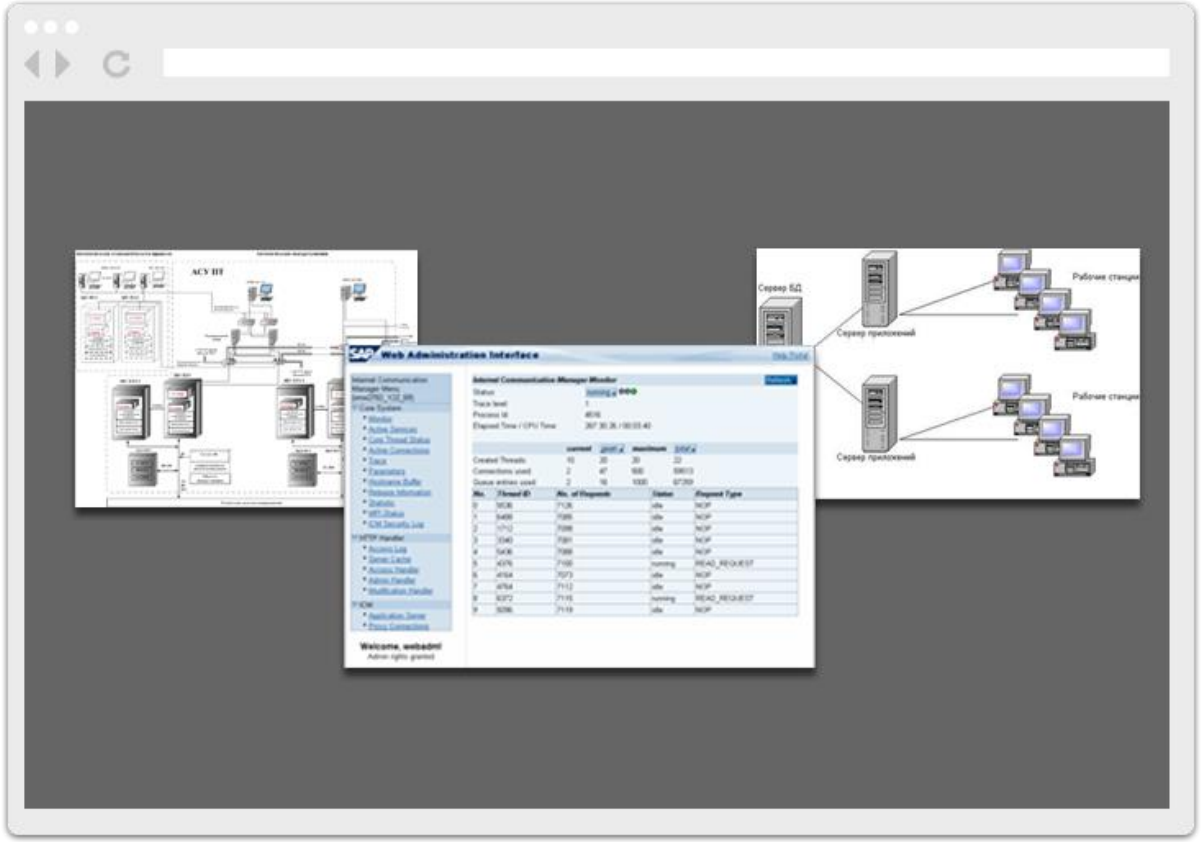
начиная приблизительно с 2009

А что у нас? Перспективы и тенденции

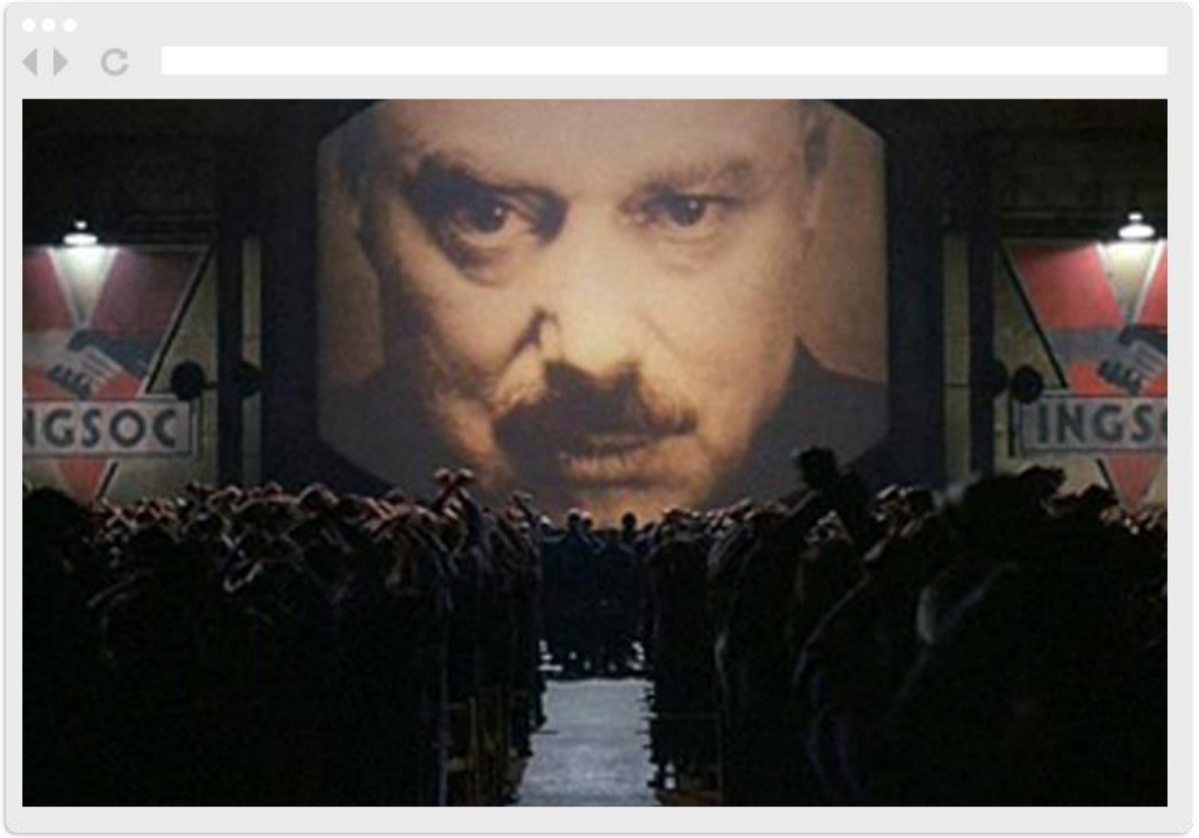
Пентест бизнес-приложений

начиная приблизительно с 2014

- ERP
- АСУ ТП
- АБС



А что у них? Перспективы и тенденции



Объем мирового рынка ИБ-консалтинга

Топ-5 западных консультантов (большая четверка + IBM):
около 9 млрд. долл
за 2014 год *(Гартнер)*

Остальные 14 ведущих игроков:
еще 2 млрд долл.

Проникновение в ИС

Через уязвимости средств защиты *(вспоминая 2015)*

по данным Пентагона в более чем 30% пентестов их успех был обусловлен уязвимостями систем защит;

уязвимости антивирусов, FireEye, Fortinet (начало 2016) и т.д.

Проникновение в ИС

Через уязвимости сетевого оборудования
(вспоминая 2015)

обнаружение злонамеренной прошивки в маршрутизаторах Циско у более чем 100 клиентов

бекдор в Juniper

Уязвимости облачных технологий

Разделение доступа между хостами внутри облака ещё не отработанная вещь *(нет DMZ, фильтрации по портам)*

Выход за пределы VM

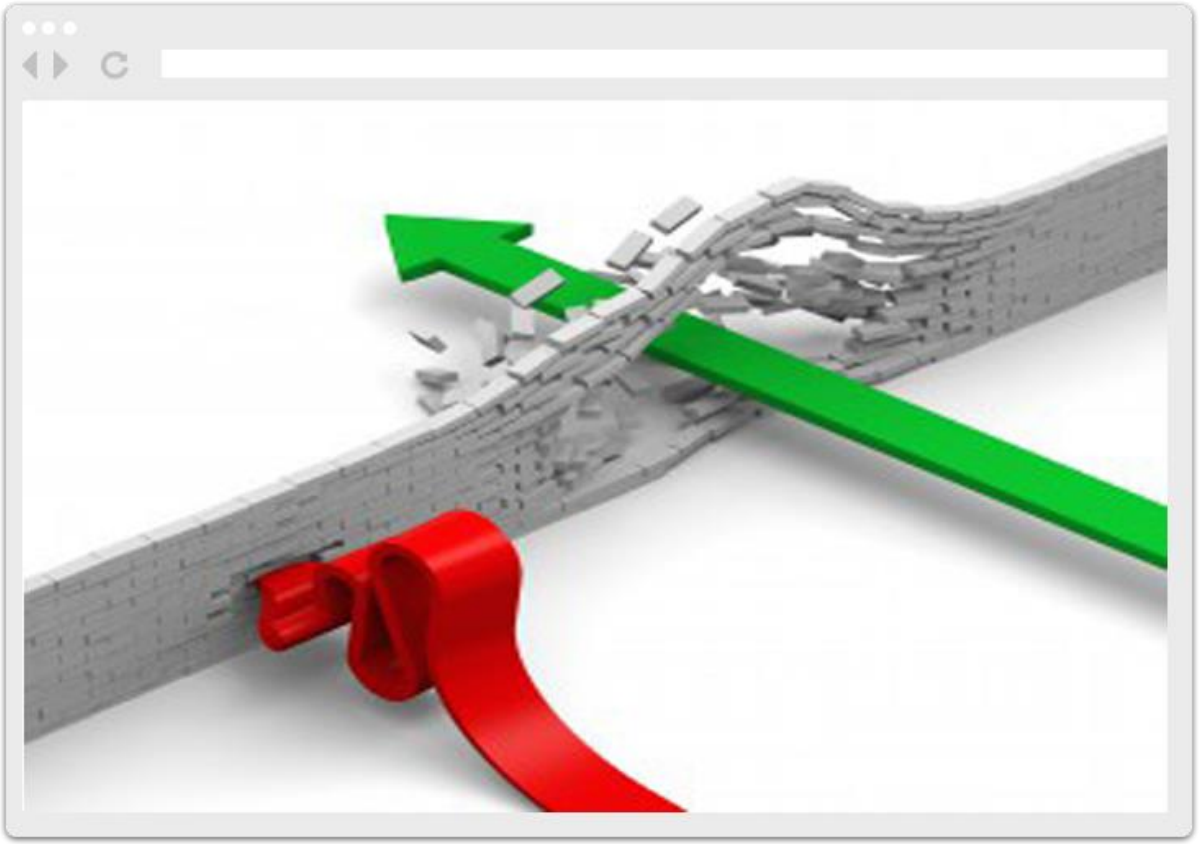
Целевые пентесты

С четко указанной целью атаки:

внешний периметр
> SAP > MES > SCADA;

АБС;

внешний периметр
> IoT (медицинское оборудование).



Проникновение в госсистемы

Цель - манипуляции данными о гражданине:

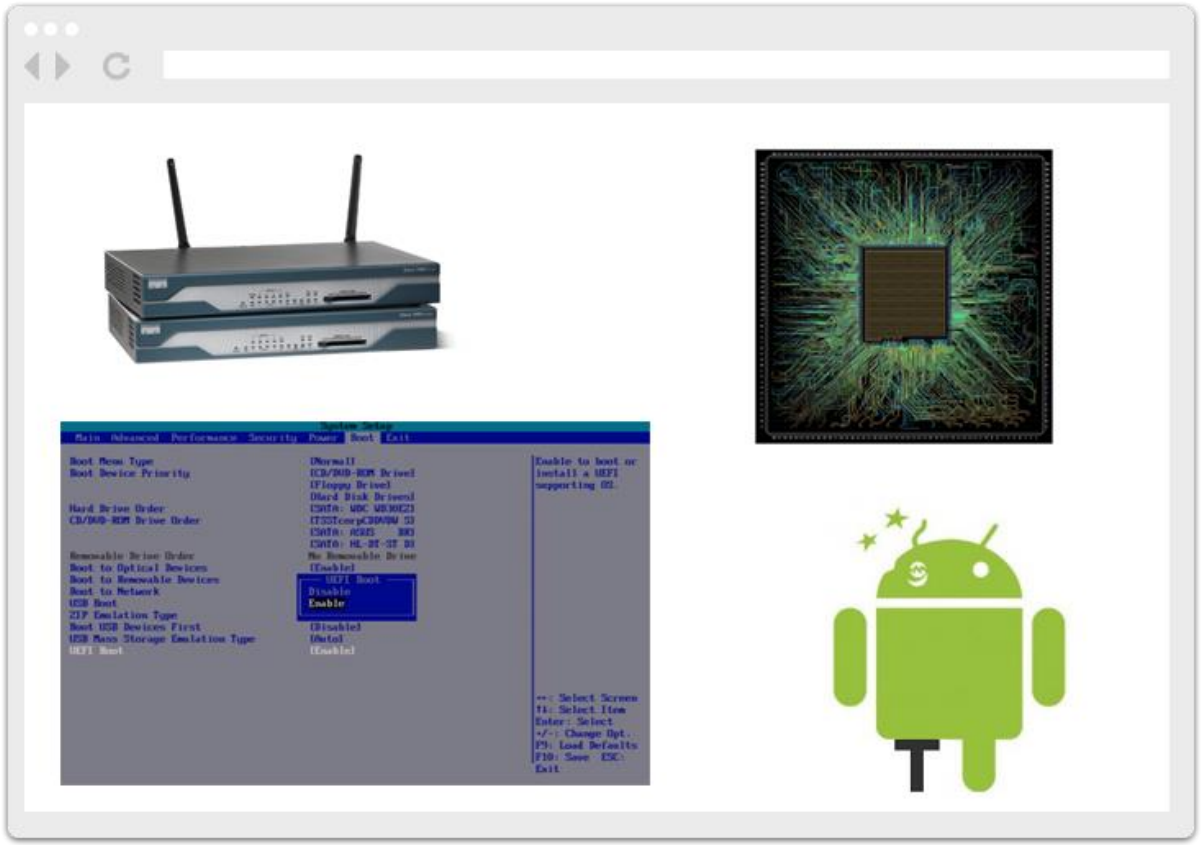
"убийство" произвольного гражданина *или*

"рождение" нового

приписка высшего "образования"

Атаки на уровне железа

- Роутеры
- Процессоры
- биос (uefi)
- драйверы мобильных устройств*



** например, недавняя атака на Андроид с последующем RCE*

Спасибо за внимание!
Вопросы?

Digital Security в Москве: (495) 223-07-86
Digital Security в Санкт-Петербурге: (812) 703-15-47

www.dsec.ru
info@dsec.ru