IIoT – Industrial Internet of Threats?

IIoT: Промышленный Интернет Угроз?

Андрей Духвалов
Руководитель департамента Перспективных Технологий
Andrey.Doukhvalov@Kaspersky.com

7 июня 2016, Санкт Петербург, IoT Summit

Internet of Things: начало новой эры

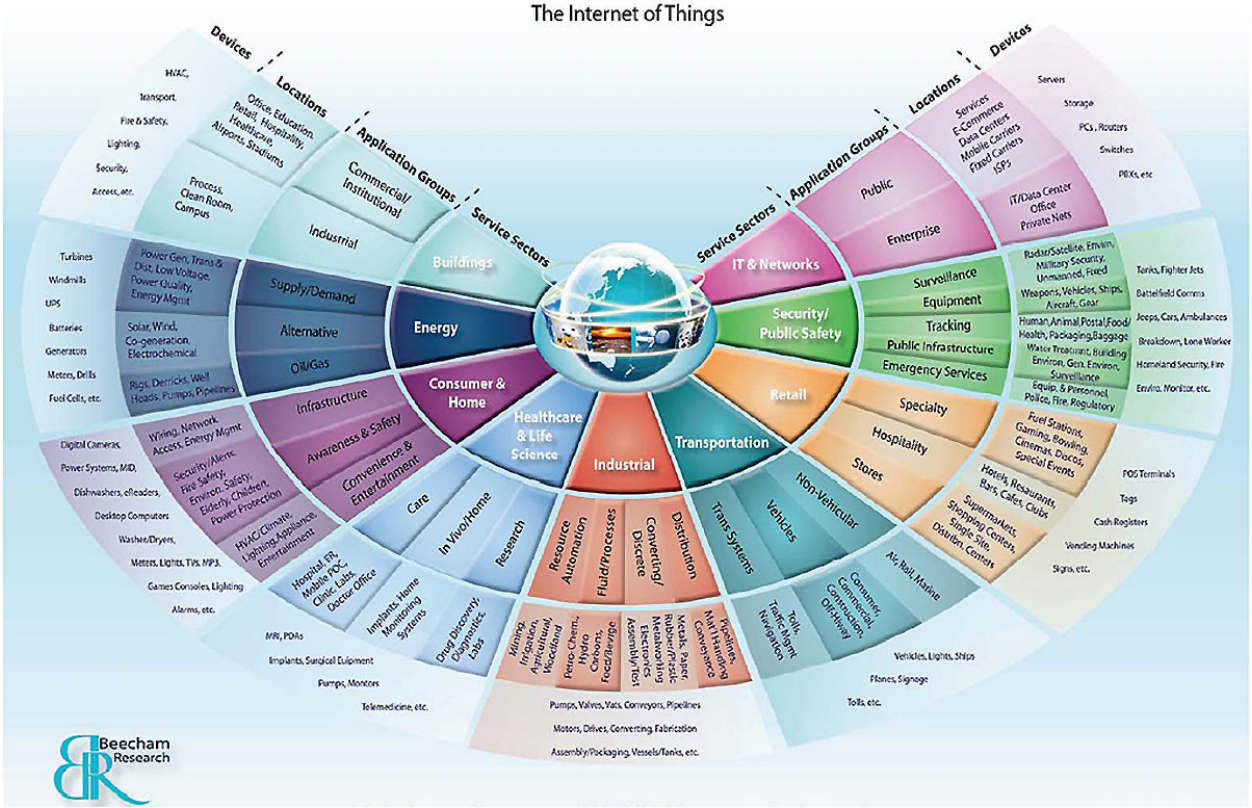
Кевин Эштон – помощник брэнд-менеджера Proctor & Gamble

В 1999 году предложил термин Internet of Things

В XX веке компьютеры были мозгом без чувств — они знали только то, что мы могли сказать им. Это было огромным ограничением: в мире во много миллиардов раз больше информации, чем люди могу ввести с клавиатуры или сканировать с помощью бар-кодов. В XXI веке, в рамках парадигмы «Internet of Things», компьютеры смогут чувствовать вещи самостоятельно

IoT: концепция вычислительной сети физических объектов (*«вещей»*), оснащённых встроенными технологиями для взаимодействия друг с другом или с внешней средой (*Gartner IT glossary, 2012)*

Internet of Things:



Internet of Things: умные города

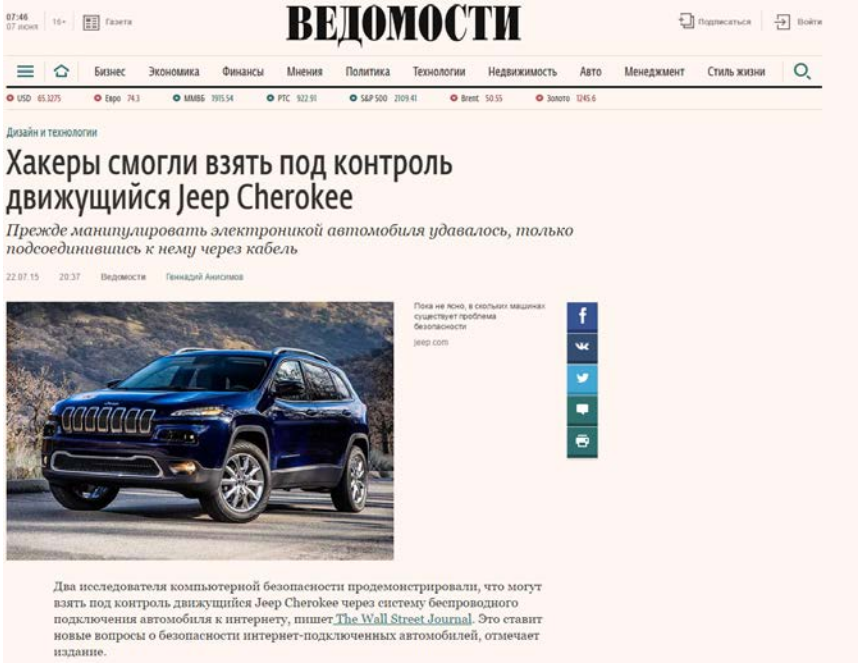
Frost & Sullivan

Internet of Things: инциденты

https://securelist.ru/blog/issledovaniya/28312/hospitals-are-under-attack-in-2016-2/

http://www.scmagazine.com/ransomware-holds-data-hostage-in-two-german-hospitals/article/479835/

Internet of Things: инциденты



ВЕДОМОСТИ

Дизайн и технологии

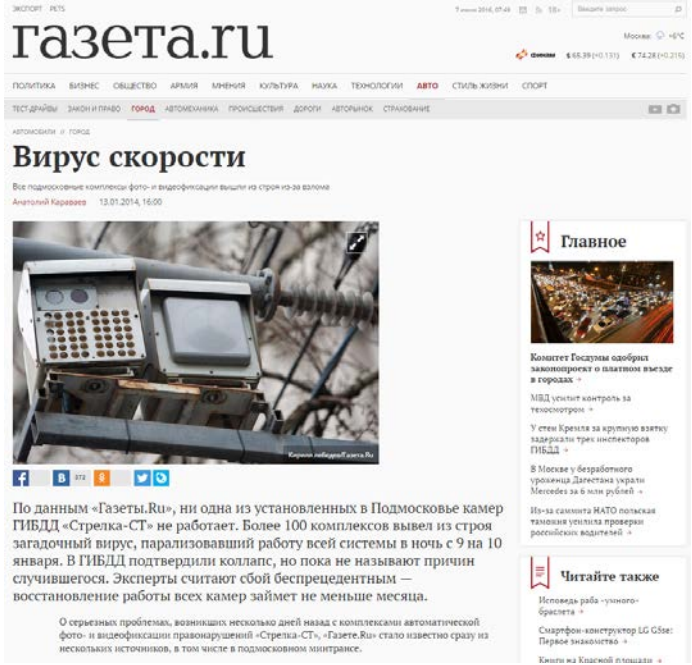
Хакеры смогли взять под контроль движущийся Jeep Cherokee

Прежде манипулировать электроникой автомобиля удавалось, только подсоединившись к нему через кабель

22.07.15 20:37 Ведомости Геннадий Аносмов

Два исследователя компьютерной безопасности продемонстрировали, что могут взять под контроль движущийся Jeep Cherokee через систему беспроводного подключения автомобиля к интернету, пишет The Wall Street Journal. Это ставит новые вопросы о безопасности интернет-подключенных автомобилей, отмечает издание.

https://www.vedomosti.ru/auto/articles/2015/07/22/601762-hakeri-smogli-vzyat-pod-kontrol-dvizhuschiisya-jeep-cherokee



газета.ru

Вирус скорости

Все подмосковные комплексы фото- и видеофиксации вышли из строя из-за взлома

Анатолий Караваев 13.01.2014, 16:00

По данным «Газеты.Ru», ни одна из установленных в Подмосковье камер ГИБДД «Стрелка-СТ» не работает. Более 100 комплексов вывел из строя загадочный вирус, парализовавший работу всей системы в ночь с 9 на 10 января. В ГИБДД подтвердили коллапс, но пока не называют причин случившегося. Эксперты считают сбой беспрецедентным — восстановление работы всех камер займет не меньше месяца.

О серьезных проблемах, возникших несколько дней назад с комплексами автоматической фото- и видеофиксации правонарушений «Стрелка-СТ», «Газете.Ru» стало известно сразу из нескольких источников, в том числе в подмосковном минтрансе.

Главное

Читайте также

http://www.gazeta.ru/auto/2014/01/13_a_5845877.shtml

Состояние информационной безопасности в мире промышленной автоматизации

Документированная статистика инцидентов в АСУ ТП

	2014		2015	
Всего инцидентов	**245**	100%	**295**	100%
Critical manufacturing	27	11%	97	33%
Energy	32	13%	46	16%
Water	6	2%	25	8%
Government facility	5	2%	18	6%
Transportation	5	2%	23	8%
Chemical	2	1%	7	2%
Nuclear	2	1%	7	2%

По данным US ICS-CERT.

KASPERSKY lab

цифровая подстанция

В октябре 2015 года Лаборатория Касперского в рамках своей конференции, посвященной информационной безопасности АСУ ТП провела соревнования среди команд, специализирующихся на поисках уязвимостей в информационных системах (CTF)

Стадии атаки:

- Перехват сетевого трафика
- Получение доступа к системе
- Отключение защитной автоматики (РЗА)
- Короткое замыкание на макете ЛЭП

Три из четырех команд-финалистов раелизовали аварийную ситуацию в первый день знакомства с объектом:

- Специалисты в области РЗА – за 3 часа
- Хакеры широкого профиля – за 5 часов

Industrial Internet of Things: начало новой эры

МЭФ 2015: Концепция Индустриального Интернета приведет к транформациии многих отраслей включая машиностроение, нефтяную и газовую промышленность, сельское хозяйство, добычу полезных ископаемых, транспорт и медицину. В общей сложности эти изменения затронут 2/3 мировой экономики.

Industrial Internet of Things: Unleashing the Potential of Connected Products and Services. Отчет Мирового Экономического Форума. Январь, 2015

Accenture: Потенциальный рост производства за счет внедрения IIoT оценивается в $12 триллионов увеличения ВВП к 2030

Эффективная промышленность за счет:

- Эффективное использование энергии
- Эффективные склады и сети поставки
- Аналитика состояния оборудования
- Предсказание мероприятий по обслуживанию
- Индивидуальное и мелко-серийное производство по стоимости продукции сравнимо с крупносерийным

Безопасность CPS: подход к снаряду

Два измерения безопасности систем

Safety (внутренняя безопасность) – свойство системы сохранять работоспособность, не наносить вред окружающей среде и людям при условии ее эксплуатации в соотвествии с предопределенными правилами и в заданных условиях.

Security (внешняя безопасность) – степень устойчивости к внешним угрозам или степень защиты от внешних угроз. Применимо к значимым и уязвимым системам. Безопасность предоставляет форму защиты когда создается какое-либо разделение между системой и угрозой.

Для CPS значимым является соблюдения обоих условий = safety + security

IoT: основные принципы

Концепция, рассматривающая организацию «умных» сетей как явление, способное перестроить экономические и общественные процессы, исключающее из части действий и операций необходимость участия человека (Кевин Эштон, 2009)

Аспекты, которые необходимо учитывать в целях безопасности

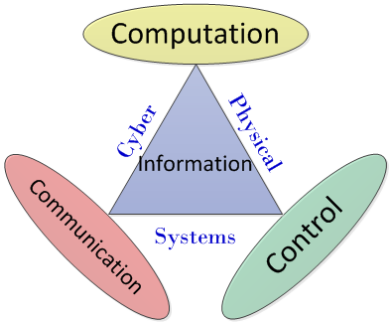
- «вещи»: однозначно идентифицируемые сущности (RFID, bar-code, GPS, etc)
- «вещи умные »: встроенные (информационные) технологии
- «вещи взаимодействующие»: сети и протоколы обмена информацией
- «вещи чувствующие»: датчики, информация об окружающей среде
- «большие данные»: вычислительные средства, способные обрабатывать большие объемы данных

кибер-физические системы (CPS): системы, способные реагировать и воздействовать на окружающую среду

Безопасность IIoT: подход к снаряду

Чем отличается кибер-безопасность CPS от IT systems

Cyber-Physical system (CPS)



Приоритеты целей

IT	CPS
Конфиденциальность	Доступность
Целостность	Целостность
Доступность	Конфиденциальность

Безопасность IIoT: подход к снаряду

Сейчас существует уникальная возможность разрабатывать устройства и системы «with security in mind». Необходимо учитывать опыт разработки систем АСУ ТП

Необходимо использовать экспертизу безопасности на ранних стадиях проектирования IIoT систем. Мы уже видели последствия, когда этого не происходит. Jason Porter, Vice President, Security Solutions, AT&T

Совершенно необходимо разрабатывать IoT устройства с учетом требований информационной безопасности. Для минимизации риска их компроментации очень важно изолировать критические устройства от избыточных коммуникаций

Chris Penrose, Senior Vice President, Internet of Things Solutions, AT&T

Спасибо
за
внимание

sIIoT: Secure Industrial Internet of Things!

sIIoT: Безопасный Промышленный Интернет Вещей!

Андрей Духвалов
Руководитель департамента Перспективных Технологий
Andrey.Doukhvalov@Kaspersky.com

7 июня 2016, Санкт Петербург, IoT Summit

KASPERSKY lab