Актуальные угрозы ИБ: Как им противостоять в современном мире

Финогенов Дмитрий Владимирович

ptsecurity.ru

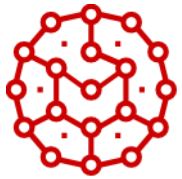
POSITIVE TECHNOLOGIES

Индустрия компьютерной преступности

POSITIVE TECHNOLOGIES

- аналитик находит уязвимости
- программист пишет вредоносное ПО
- сканер определяет места функционирования уязвимого ПО

- преступник вербует инсайдера
- хакер внедряет вредоносное ПО



- группировки разворачивают бот-сети
- сдают их в аренду или продают

- наркоман забирает деньги из банкомата
- сборщики собирают деньги
- страховщик страхует от потери наличных денег

Состояние защищенности

POSITIVE TECHNOLOGIES

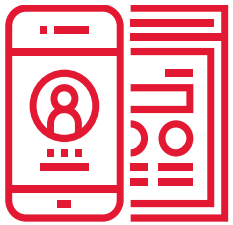
Более 60% корпоративных систем ломаются легко

70% владельцев узнают о взломе своих сетей из СМИ

Среднее время присутствия вредоноса в сети – 3 года!

Тенденции и ожидания

Web-приложения



Мобильная связь ОКС-7

Автоматизированные системы управления (АСУ ТП)

Атаки на веб-приложения

POSITIVE TECHNOLOGIES

- **Практически все web-приложения уязвимы**
- **60% всех атак идут через web**
- **Лидируют простые атаки:** SQLi, Path Traversal, XSS, выполнение команд ОС
- **Высокая автоматизация**, особенно на сайты промышленных компаний (98%)

ЦЕЛИ:
- проникнуть во внутреннюю сеть компании через взлом сайта
- похитить персональные данные клиентов
- получить доступ к финансовым инструментам
- заразить клиентов сайта
- дефейс сайта

Инциденты из-за уязвимостей в вебе

POSITIVE TECHNOLOGIES

Стоимость акций кредитного бюро Equifax Inc., входящего в тройку крупнейших в США, упала на 17% после того, как компания сообщила о масштабном нарушении кибербе[illegible]и получить доступ к персона[illegible]А - 143 млн человек.

Talk Talk оштрафован на £400 тысяч за плохую защиту данных клиентов

17:09 05.10.2016 (обновлено: 17:10 05.10.2016) 0 184 0 1

© Fotolia / Tomasz Zajda

Бизнес Экономика Финансы Мнения Политика Технологии Недвижимос

USD 57.8025 Евро 68.8175 ММВБ 2055.53 РТС 1118.24 S&P 500 2496.48 Brent 54.92

18 ЛЕТ «ВЕДОМОСТЯМ». ВСЕ МАТЕРИАЛЫ ДОСТУПНЫ ДАЖЕ БЕЗ ПОДПИСКИ* Осталось 12 д

Статья опубликована в № 3668 от 05.09.2014 под заголовком: JPMorgan обнаружил дыру в Россию

JPMorgan обнаружил дыру в Россию

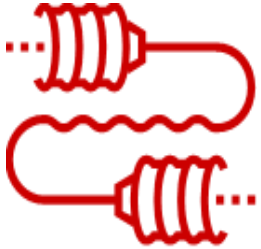
05 сентября 2014 00:00 | Александр Силонов / Ведомости

Внутреннее расследование, проведенное JPMorgan Chase в связи с хакерской атакой на этот банк, позволило следователям сделать вывод, что украденные хакерами данные переправлялись в Россию. Для атаки хакеры использовали международную сеть компьютеров.

Телеком: основные угрозы

POSITIVE TECHNOLOGIES

- прослушивание
- отслеживание геолокации
- подделка SMS
- внедрение в аппарат



- перебои в функционировании
- нарушения маршрутизации

ВСЕ исследованные сети мобильных операторов подвержены угрозам!

В ходе тестов на практике проведено:

80%

атак, направленных на сбои в работе

77%

атак с целью вызвать утечку информации

67%

мошеннических атак

Инциденты с телеком-операторами

POSITIVE TECHNOLOGIES

The Register®
Biting the hand that feeds IT

DATA CENTRE | SOFTWARE | SECURITY | TRANSFORMATION | DEVOPS | BUSINESS | PERSONAL TECH

Security

48

After years of warnings, mobile network hackers exploit SS7 flaws to drain bank accounts

O2 confirms online thefts using stolen 2FA SMS codes

By Iain Thomson in San Francisco 3 May 2017 at 20:02 SHARE ▼

SecurityLab.ru
by Positive Technologies

RaaS-сервис Shifr позволяет любому вымогательское ПО

Новости | Уязвимости | Статьи | Софт | Блоги | Форум | PHDays

...вная / Новости

...04 / 6 Августа, 2012

...Южной Корее скомпрометированы персональные данные почти 9 млн ...ользователей местного провайдера сотовой связи

Теги: Южная Корея, мобильная связь, утечка, данные

Полиция арестовала двух хакеров, продававших личные данные абонентов мобильной связи компании Korea Telecom, а также инструмент, при помощи которого им удалось эти данные

SecurityLab.ru
by Positive Technologies

В Забайкалье арестованы хакеры, у... миллионов рублей

Новости | Уязвимости | Статьи | Софт | Блоги | Форум | PHDays

...авная / Новости

...28 / 24 Февраля, 2017

...Лондоне задержан хакер по подозрению в атаке на Deutsche Telekom

Теги: хакерская атака, арест, ботнет

Хакерская атака оставила более 1 млн клиентов Deutsche Telekom без доступа к интернету.

Сотрудники Национального агентства по борьбе с преступностью Великобритании (National Crime Agency) задержали в одном из аэропортов Лондона 29-летнего британца, подозреваемого в масштабной кибератаке на крупнейшую телекоммуникационную компанию Deutsche ...elekom в конце ноября 2016 года.

...апомним, в результате атаки более 1 млн пользователей проводной связи Deutsche ...elekom испытали проблемы с доступом к Сети в связи с выходом из строя ...аршрутизаторов. Как полагают эксперты, злоумышленники использовали новый образец ...редоносного ПО Mirai, созданный специально для атак на уязвимые маршрутизаторы ...роизводства компании Zyxel.

Полный Интернет автоматики, которую нужно защищать

POSITIVE TECHNOLOGIES

Количество компонентов АСУ ТП, доступных в сети Интернет, **увеличивается** с каждым годом

2016

В результате исследования было выявлено более **160 000** компонентов АСУ ТП, доступных в сети Интернет

АСУ ТП: уязвимости в цифрах

POSITIVE TECHNOLOGIES

Во всех АСУ ТП, исследованных в 2016 году, найдены уязвимости

47% высокая степень риска

14% исправлены в течение трех месяцев

1/3 доступных через Интернет систем управления не защищены

наиболее уязвимы системы автоматизации зданий и управления электроэнергией

Инциденты с АСУ ТП

POSITIVE TECHNOLOGIES

15:27
29 июня
16+
Газета

ВЕДОМОСТИ

Бизнес Экономика Финансы Мнения Политика Технологии Недвижимость Авто

USD 58.9975 Евро 67.32 ММВБ 1890.04 РТС 1009.17 S&P 500 2440.69 Brent 47.91 Золото 1248

Honda на сутки остановила один из заводов из-за кибератаки

21 июня 10:21 ТАСС

ISA Setting the Standard for Automation™

Phone: (9

MEMBERSHIP | TRAINING & CERTIFICATIONS | STANDARDS & PUBLICATIONS | CONFERENCES & EVENTS | PR

Home › ISA Publications › InTech Magazine › InTech articles › Special Section: Ukrainian pow

Ukrainian power grids cyberattack

A forensic analysis based on ISA/IEC 62443

SecurityLab.ru by Positive Technologies

The Shadow Brokers грозятся раскры
бывшего хакера из АНБ

Новости Уязвимости Статьи Софт Блоги Форум PHDays

лавная / Новости

1:07 / 17 Мая, 2017

Хакеры взломали табло железнодорожного вокзала в Вашингтоне

Теги: хакеры, взлом, США

В результате взлома на экране вместо расписания поездов появилась видеозапись интимного характера.

В результате взлома неизвестными хакерами информационного табло железнодорожного вокзала Юнион-Стейшн в Вашингтоне на экране вместо расписания поездов появилась видеозапись непристойного

ТАСС

ИН
АГЕ

Кубок конфеде

Промышленност

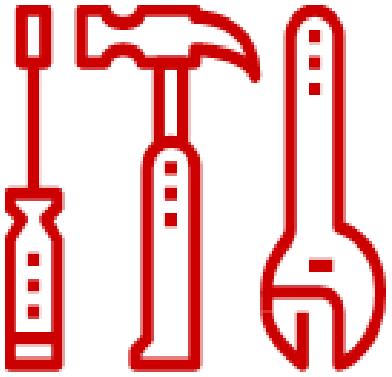
одержания

AFP: несколько заводов Renault во Франции остановлены из-за массированной кибератаки

Экономика и бизнес 13 мая, 13:38 UTC+3

Причины низкой защищенности

Ошибки при проектировании и реализации



- защита не предусмотрена
- низкое качество программного кода

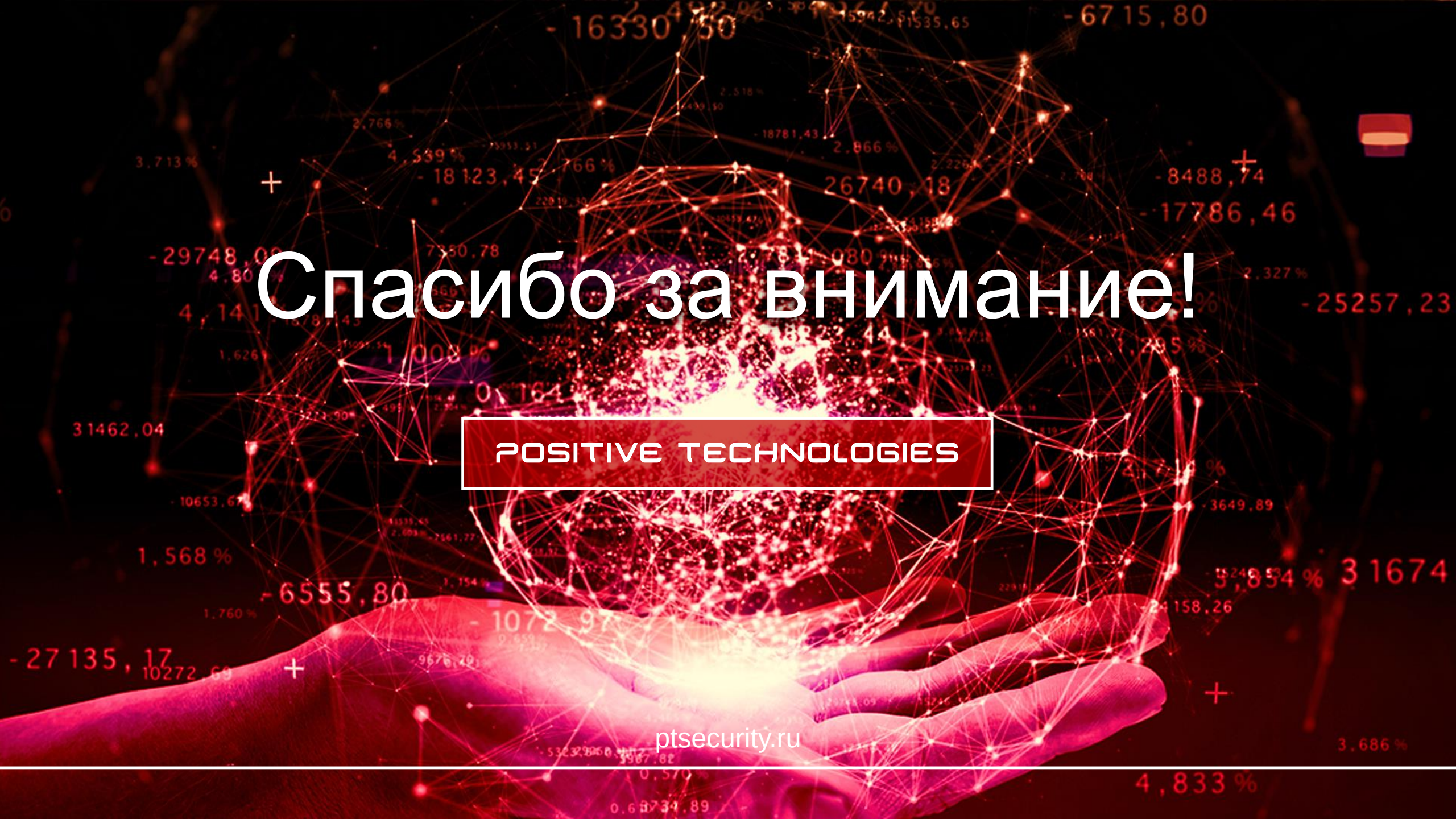
Человеческий фактор

- фишинг работает всегда
- низкая квалификация
- плохая координация
- недооценка рисков

Что делать

POSITIVE TECHNOLOGIES

1. **На государственном уровне** : ФЗ-187 от 26 июля 2017, ГосСОПКА, программа «Цифровая экономика»
2. **На региональном уровне** : Ведомственные и Корпоративные центры ГосСОПКА
3. **На уровне организации** – анализировать риски, ГосСОПКА, квалификация администраторов, информированность руководителей. Продукты класса WAF, SIEM и решения для безопасной разработки.
4. **На уровне общества** – создавать самоорганизующиеся организации, некоммерческие общества
5. **На личном уровне** – жить так, чтобы не было стыдно за публикации в Интернете; а также соблюдать «гигиену» и повышать осведомленность свою и близких


Спасибо за внимание!
POSITIVE TECHNOLOGIES
ptsecurity.ru