К вопросу защищенности информационных систем

POSITIVE TECHNOLOGIES

ptsecurity.com

Немного статистики

POSITIVE TECHNOLOGIES

Защита периметра **не останавливает** проникновение

Атак могли быть предотвращены **стандартными решениями**

Инцидентов стали успешными **из-за серьезных ошибок в конфигурации**

Атак **не требовали** высокой квалификации нарушителей

Каждую вторую систему может взломать неквалифицированный хакер

Источник: Positive Research 2016

Сводки с полей кибер-войн

POSITIVE TECHNOLOGIES

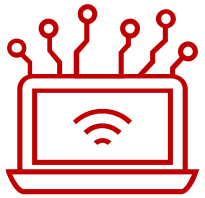
Космос, военные, телеком, государственные органы власти

- PlugX и NetTraveler–
  - 2016 год
  - вектор распространения: почта
  - способ: фишинг
  - url или exploit
  - цель: эксплуатация уязвимости в Microsoft Word
  - источник - Китай

Источники уязвимостей

POSITIVE TECHNOLOGIES

Слабые пароли

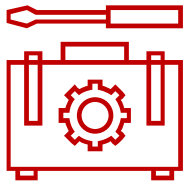


Небезопасные беспроводные сети

Уязвимости веб-приложений

Программное обеспечение

Социальная инженерия



Ошибки в настройках:

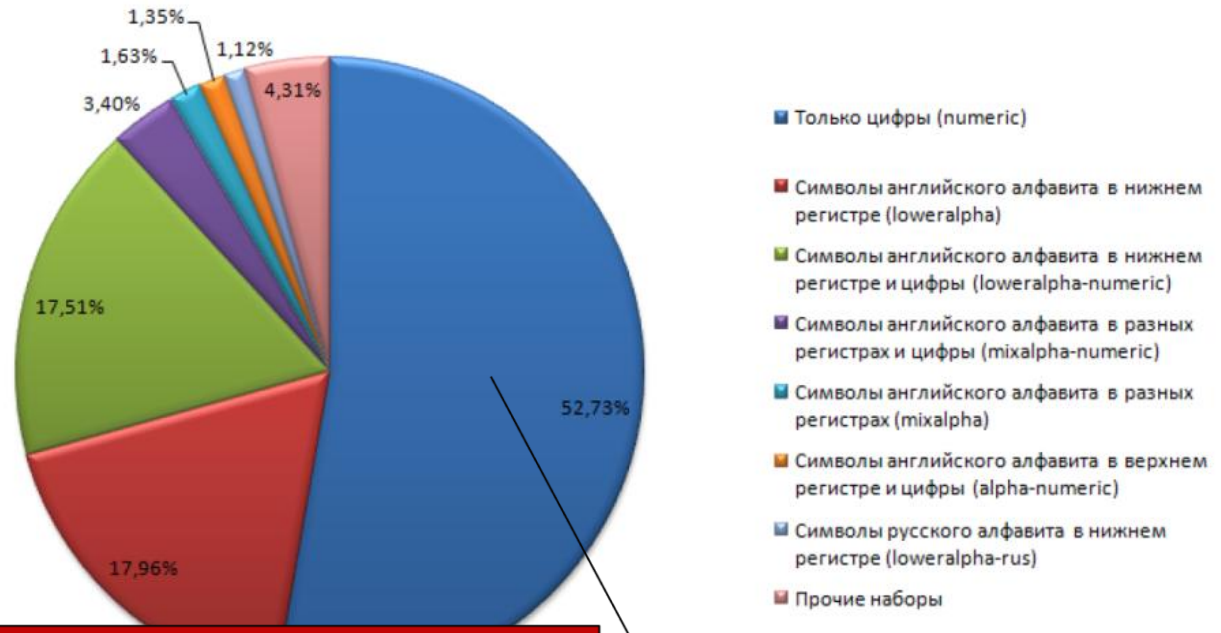
- сетевого оборудования
- систем защиты периметра
- веб-приложений
- баз данных

TOP 10

POSITIVE TECHNOLOGIES

Таблица 2. TOP 10 наиболее часто используемых паролей

Пароль	Позиция	Доля, %
1234567	1	3,36%
12345678	2	1,65%
123456	3	1,02%
Пустая строка	4	0,72%
12345	5	0,47%
7654321	6	0,31%



53% - использовали в пароле только цифры!

Пароли по умолчанию поменяли,
но сложные пароли придумать поленились!

Это все хорошо, но как мне соответствовать?

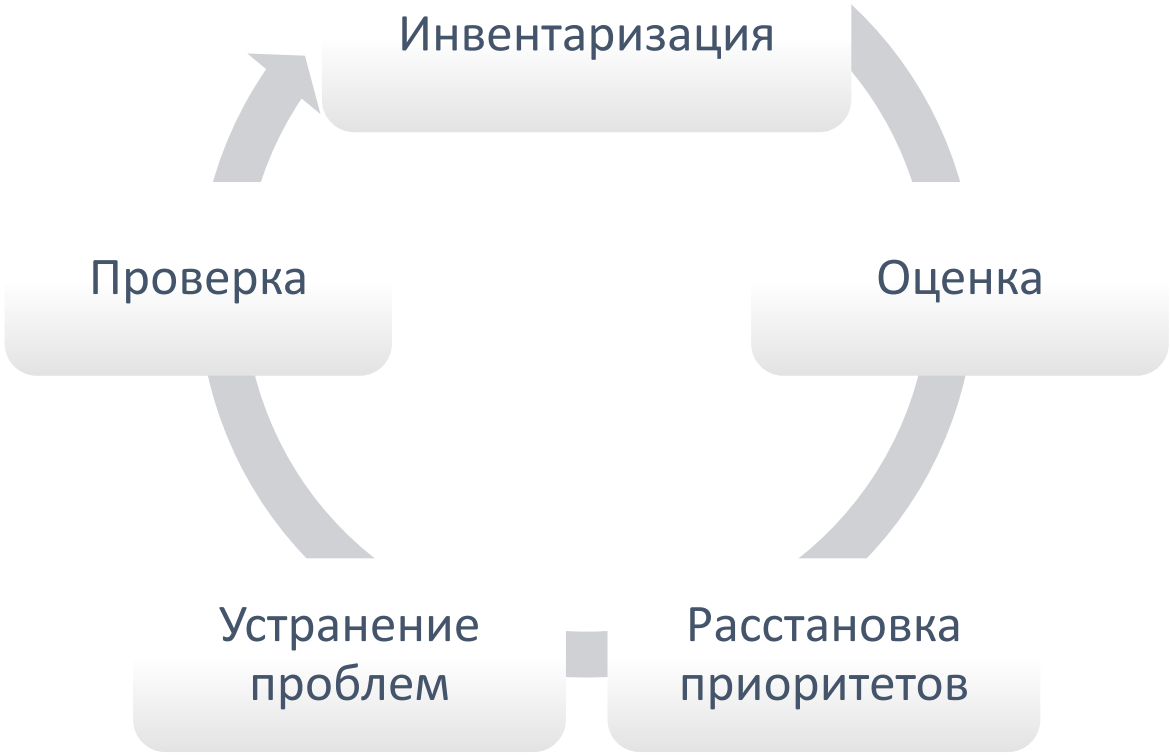
POSITIVE TECHNOLOGIES

№	МЕРЫ ЗАЩИТЫ	Классы защищенности ИС (Приказ 17)				Уровни защищенности ПДН (Приказ 21)				Класс защищенности АСУ(Приказ 31)		
		4	3	2	1	4	3	2	1	3	2	1
АНЗ 3.0	Разработка правил и процедур контроля защищенности	Отсутствует				Отсутствует				+	+	+
АНЗ 3.1	Выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей		+	+	+		+	+	+	+	+	+
АНЗ 3.2	Контроль установки обновлений ПО и средств защиты информации	+	+	+	+	+	+	+	+	+	+	+
АНЗ 3.3	Контроль работоспособности, параметров настройки и правильности функционирования ПО и средств защиты информации		+	+	+		+	+	+	+	+	+
АНЗ 3.4	Контроль состава технических средств, ПО и средств защиты информации		+	+	+		+	+	+	+	+	+
АНЗ 3.5	Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в информационной системе		+	+	+			+	+		+	+

Контроль уязвимостей – это процесс

POSITIVE TECHNOLOGIES

- ✓ Главное – повторять этот цикл регулярно
- ✓ Иначе ваша система будет безопасной только «на бумаге»



MaxPatrol – комплексное решение

POSITIVE TECHNOLOGIES

+Все в одном: средство автоматизированного анализа защищенности и контроля соответствия

+Поиск уязвимостей и ошибок конфигурации компонентов ИС

+Контроль соответствий фактических настроек ИС установленным требованиям

+Более 120 встроенных, сгруппированных стандартов и возможность создания собственных

+Ежедневно обновляемая база знаний

Режим Pentest

POSITIVE TECHNOLOGIES

Режим «PenTest»

- Не требует учетной записи от сканируемого узла
- Определяет уязвимости:
  - путем анализа сообщений (баннеров)
  - путем выполнения эксплойтов
  - эвристическими методами
  - Анализирует веб-приложения
- Перебирает пароли

Режим «Audit»

- Использует только определенные протоколы удаленного доступа
- Анализирует ПО как на стороне сервера, так и на стороне клиента
- Идентифицирует установленное аппаратное и программное обеспечение
- Проверяет, установлены ли обновления безопасности
- Анализирует конфигурации

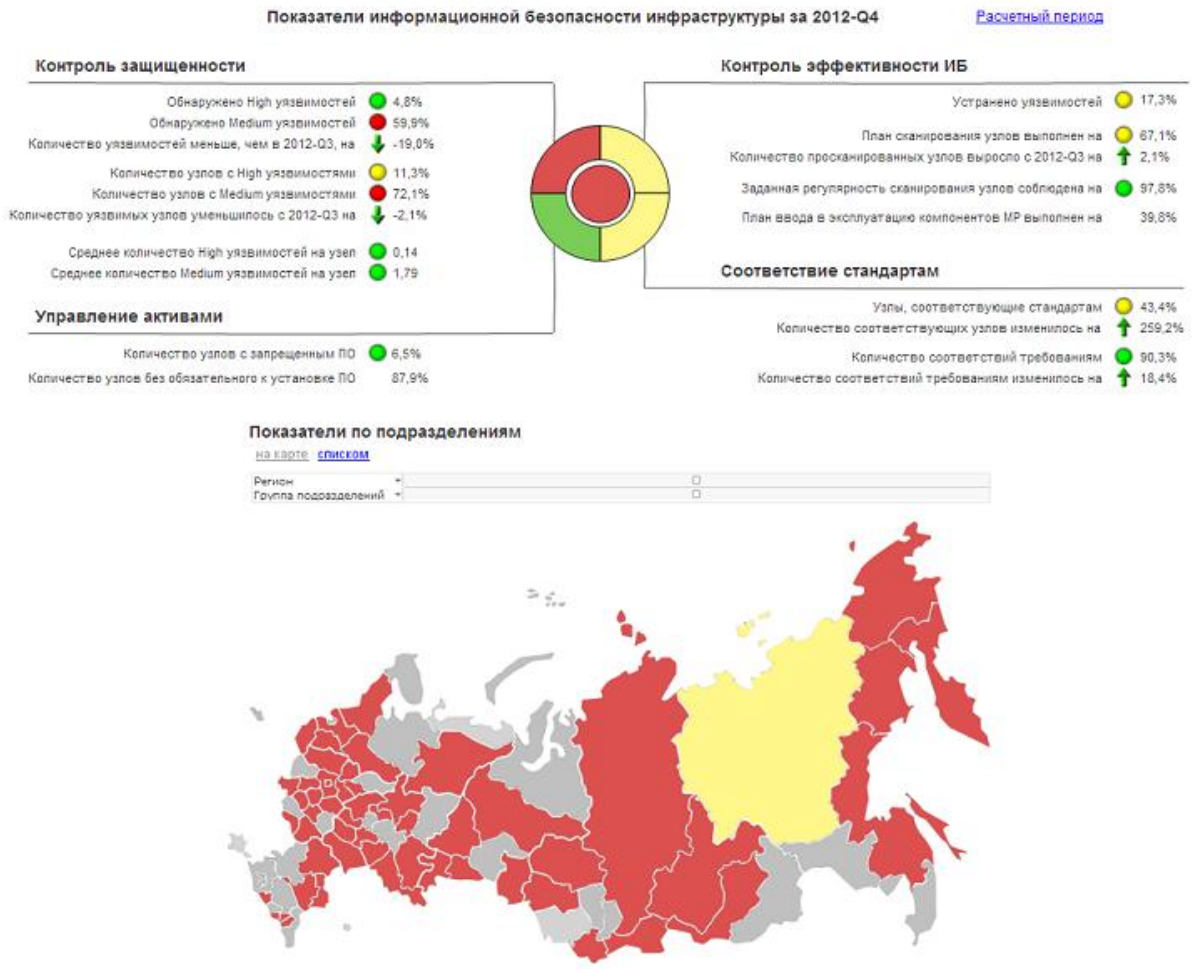
Режим «Compliance»

- Более 70 встроенных стандартов
- Автоматическое определение соответствия применимым стандартам
- Поддержка высокоуровневых стандартов и требований регуляторов
- СТО БР ИББС, PCI DSS
- ISO 27001/27002
- Доработка стандартов в соответствии с требованиями заказчика

Следующий уровень зрелости – портал аналитической отчетности

POSITIVE TECHNOLOGIES

- Анализ данных MaxPatrol
- Интегральные показатели ИБ
- Выявление негативных и позитивных тенденций
- Контроль работоспособности и использования MaxPatrol
- Представление в наглядной форме информации о реальном уровне ИБ в компании



История успеха

POSITIVE TECHNOLOGIES

Кто – ЦИТ Тюменской области

Направление деятельности – сопровождение государственных интернет-ресурсов и ИС

- Задача: оценка защищенности инфраструктуры правительства Тюменской области и выстраивание процесса управления ИБ
- Решение: система контроля защищенности и соответствия стандартам MaxPatrol 8
- Результат: выстроен стабильный процесс управление ИБ и автоматизирован контроль соответствия требованиям регуляторов

ЦЕНТР ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ТЮМЕНСКОЙ ОБЛАСТИ КОНТРОЛИРУЕТ ЗАЩИЩЕННОСТЬ IT-ИНФРАСТРУКТУРЫ ПРАВИТЕЛЬСТВА С ПОМОЩЬЮ MAXPATROL 8

«Обеспечение высокого уровня безопасности государственных ресурсов и информационных систем является одной из ключевых задач Центра информационных технологий. Сотрудничество с Positive Technologies позволило нам объективно оценить текущую защищенность IT-инфраструктуры, выстроить стабильный процесс управления уязвимостями, а также обеспечить уровень безопасности, полностью соответствующий как мировым стандартам, так и требованиям российских регуляторов».

Александр Забокрицкий
Начальник отдела информационной безопасности ЦИТ Тюменской области


Спасибо!
POSITIVE TECHNOLOGIES
ptsecurity.ru