

# Проблема контроля сегментирования ОКИИ

Евгений Зайцев  
Начальник управления ИБ  
ПАО «Селигдар»

# Зачем?



1. Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ
2. Приказ ФСТЭК России от 25.12.2017 N 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»



1. Уменьшаем поверхность атаки
2. Облегчаем реагирование
3. Оптимизируетм СЗИ (как по производительности, так и по стоимости)
4. Упрощаем администрирование

# Немного статистики



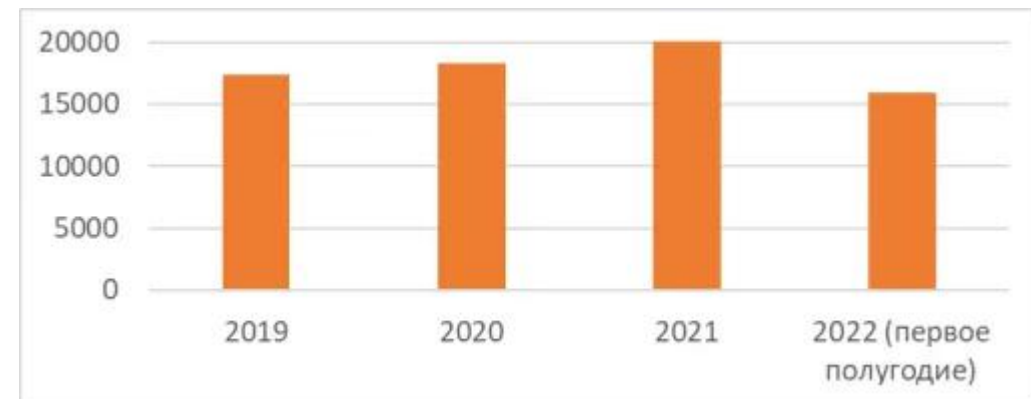
## Time to Known Exploitation (TTKE/days)



из блога Алексея Лукацкого (@alukatsk)



Статистика Group-IB



Статистика svedetails

# Что делать?



## 1. Первый этап

- 1.1 Инвентаризация - Вы не можете защитить то, о чем вы не знаете.
- 1.2 Категорирования пользователей и ресурсов
- 1.3 Разбиение информационной системы на сегменты
- 1.4. Обеспечение защиты и контроля периметров сегментов (ЗИС.4.1)  
сначала требования(политики), потом реализация(СЗИ)

## 2. Второй этап

- 2.1 Контроль внешнего периметра (инвентаризация + уязвимости)
- 2.2 Контроль внутреннего периметра (политик ИБ):  
п. 21+ контроль: доступа, покрытия и работоспособности СЗИ, журналирования и т.д.
- 2.3 Анализ
- 2.4 Внесение изменений
- 2.5 Вернуться в пункт 2.1



# В чем проблема обеспечить сегментацию?



## 1. Риски нарушения бизнес-процессов

### 2. Организационные проблемы:

1. Человеческий фактор (кадровый голод, инертность мышления, выгорание)
2. Правильная последовательность выстраивания защиты периметра
3. Организация повторяемости процесса
4. Естественные (неформализованные) процессы



### 3. Технические проблемы:

1. Археология (секреты в сетях)
2. Ложные срабатывания
3. Ограниченный выбор оборудования и ПО
4. Несовместимость оборудования и ПО
5. Стоимость



# Внешние проблемы

Программное  
обеспечение



Человеческий  
фактор



Автоматизированные системы



Киберхулиган/энтузиаст-одиночка



Киберкриминал/ организованные группировки



Кибернаёмники/ продвинутые группировки



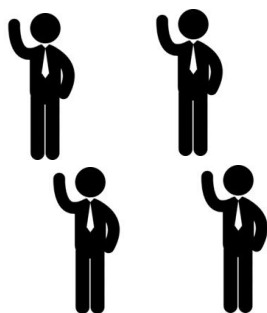
Кибервойска/ про государственные группировки

# Внутренние проблемы

Программное  
обеспечение



Человеческий  
фактор



Киберкриминал/  
организованные группировки



Кибернаёмники/  
продвинутые группировки



Кибервойска/  
про государственные  
группировки

# Чем опасны, как защититься?



Ошибки конфигурирования, использование ПО с актуальными опубликованными уязвимостями  
Любой недостаток инфраструктуры станет точкой входа. (RDP на периметре, незащищенный WEB-сервис)



Отсутствие процесса анализа защищенности, настроенных и обновляемых базовых средств защиты  
-100% шанс быть взломанным



Обход базовых СЗИ  
Продвинутое ВПО (проверки среды, стеганография, многоуровневая обфускация)  
Целевой фишинг  
Взлом удалённых пользователей  
Взлом домашних ПК



Невозможность детектирования без налаженных процессов анализа защищенности и мониторинга событий безопасности



Использование 0-day на этапе проникновения и перемещения в инфраструктуре  
Использование легитимных сервисов для закрепления и перемещения  
Применение техник обхода средств защиты на хостах - запуск mimikatz в обход АВПО, использование С&С в TOR-сетях, powershell компоненты



Скрытое присутствие, не детектируемое базовым мониторингом



# Требования к женихам сканерам небольшие

## Внешний периметр

Black/Gray box  
L3-L7 проверки:



1. Контроль портов периметра на соответствие whitelist
2. Проверка ПО по базе уязвимостей и эксплойтов (MITRE, БДУ ФСТЭК, NIST + ExploitDB)
3. Проверка на OWASP-TOP-10 веб-уязвимости (XSS, SQLi, т.д)
4. Поддержка возможностей HTML5, AJAX, Angular, React
5. Подбор слабых паролей
6. Сканирование веб-порталов с аутентификацией
7. Поиск уязвимостей в CMS и версиях JS-библиотек
8. Тестирование API на основе swagger-описания
9. Обнаружение административных интерфейсов (PHPMyadmin, PGAdmin, Kubernetes, и д.р.)

Помимо этого:

1. Высокая скорость (полный скан не реже 1 раза в сутки)
2. Низкий процент ложных срабатываний
3. Экспертное сопровождение (SaaS, PaaS)
4. Автоматическое обнаружение доменов и сетей
5. Генерация PoC
6. Интеграция с IRP (SYSLOG или REST API)

# Это не всё!

## Внутренний периметр

White box:



1. Инвентаризация узлов и ПО (whitelist)
2. Агентный и безагентный способ сканирования
3. Проверка ПО по базе уязвимостей и эксплойтов (MITRE, БДУ ФСТЭК, NIST + ExploitDB)
4. Поддержка определения уязвимостей в эксплуатируемом ПО и оборудовании (Microsoft, OpenSource, сетевое оборудование, IoT и т.д.)
5. Подбор слабых паролей на стороне сервера
6. Определение ошибок конфигурации
7. Возможность детектировать изменения в конфигурации узлов
8. Проверки на соответствие стандартам (Compliance)

Помимо этого:

1. Поддержка многодоменной, многозвенной архитектуры
2. Высокая скорость (полный скан не реже 1 раза в неделю)
3. Низкий процент ложных срабатываний
4. Интеграция с LDAP, DHCP, CMDB
5. Интеграция с IRP (SYSLOG или REST API)

# Что делать?

## Шаг 1, найти экспертов!

---

Собственная экспертиза:

- Долго
- Очень дорого
- Риск потери экспертизы
- Низкая эффективность



Внешняя экспертиза:

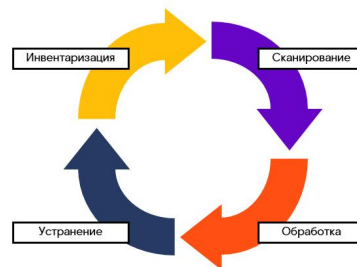
- Быстро
- Дорого
- Проблема контроля

## Шаг 2, выстраивайте процессы

---

Собственная экспертиза:

- Долго
- Дорого
- Работает



Внешняя экспертиза:

- Быстро
- Очень дорого
- Зачастую бесполезно

# В заключение

- Цените своих экспертов, либо ищите аусорсеров
- Дружите с ИТ
- Донесите до руководства, что уязвимости будут всегда, Ваша задача не допустить эксплуатации уязвимостей
- Донесите до ИТ, что уязвимости это не их косяк, а скорость устранения - это их KPI

# Спасибо за внимание!

Евгений Зайцев

Начальник управления ИБ

ПАО «Селигдар»

telegram: @ezaitsev