

АНАЛИЗ ЗАЩИЩЁННОСТИ ИТ-ИНФРАСТРУКТУРЫ: ПОДХОД INFOWATCH ARMA

Равиль Зулькарнаев

Руководитель отдела защиты
информации, InfoWatch ARMA



Диагностика на возможность реализации проникновения

→ Отвечает на вопрос: как будет действовать злоумышленник, чтобы получить несанкционированный доступ к промышленной сети или компонентам устройств АСУ ТП?

Поиск уязвимостей

→ Отвечает на вопрос: Какие уязвимости технологических сетей предприятия и АСУ ТП можно эксплуатировать?

Зачем?

→ Приказ ФСТЭК России № 239 от 25 декабря 2017 (п 11.1, 12.6)

Хотите подобрать решение под задачи вашей компании?

Получите консультацию наших экспертов. Напишите нам: anna@team.infowatch.com

72%

можно использовать удалённо

47%

затрагивают уровни 1 и 2 модели Purdue (PLC, SCADA, DMZ)

76%

не требуют аутентификации для эксплуатации

Рост рисков с развитием цифровизации

- 449 уязвимостей в АСУ ТП (II пол. 2020)
- Более 70% — критические (CVSS)

[Отчёт Claroty](#)

-
- 49% — рост уязвимостей в АСУ ТП
 - 22% — скачок атак на промышленность (II кв. к I кв. 2020)
 - 25% всех атак в мире — на производство (1–8.2020)

[Отчёт IBM](#)

Методы

→ «Чёрный ящик»

Когда уязвимости и векторы атак ищутся через имитацию хакерской атаки, а об инфраструктуре не известно ничего

→ «Серый ящик»

Есть санкционированный доступ к инфраструктуре, и проверяется, как злоумышленник может получить доступ к конфиденциальной информации

→ «Белый ящик»

Все данные об инфраструктуре известны, и можно найти максимальное количество уязвимостей

С чего начать?

Анализ доступных из сети интернет-адресов с использованием сервисов типа Shodan



Почему это важно

Классический подход

- 1 Разведка и сбор данных об инфраструктуре
- 2 Определение активов
- 3 Определение уязвимостей и угроз
- 4 Проверка возможности эксплуатации уязвимости
- 5 Типовые политики и настройки оборудования

Типовые политики

→ Наличие / отсутствие:

- Подключения к интернету
- Подключения съёмных носителей
- Парольной политики
- Политики обновления
- Политики антивирусной защиты

1

Сформированные процессы
по их выполнению

2

Нужны средства автоматизации

И это всё?

- Fuzzing
- **Анализ защищённости оборудования:**
 - Исследование компонентов устройства
 - Исследование сетевого взаимодействия
 - Исследование исходного кода программ

Какие риски?

1 Nmap

2 Кирпич

Что встречаем чаще всего и почему?

- 1 Пароли ТОП-100
- 2 Устаревшие версии ПО и ОС
- 3 Не настроенное корректно оборудование АСУ ТП и СЗИ
- 4 Человеческий фактор

**НЕТ ВОЗМОЖНОСТИ
САМОСТОЯТЕЛЬНО
ПРОВЕСТИ АНАЛИЗ
ЗАЩИЩЁННОСТИ?**

**ЭКСПЕРТЫ INFOWATCH
ARMA ПОМОГУТ**

Получите консультацию наших
экспертов. Напишите нам:
anna@team.infowatch.com

