Информзащита
Системный интегратор

20 лет

PHD 2016
ЗАЩИТА АСУ ТП+ SOC

Даренский Дмитрий
Начальник отдела промышленных систем
ЗАО НИП «ИНФОРМЗАЩИТА»

Новый SOC и PHD`6

- Основные задачи:
  - Отработать взаимодействие различных подразделений при оказании единого сервиса
  - Отработать подключение SOC к инфраструктуре объекта
  - Отработать разворачивание СЗИ в условиях жестких временных рамок
  - Провести нагрузочное тестирование сервиса и СЗИ в условиях массированных атак
  - Получить PR-повод для продвижения нового сервиса

Информзащита
Системный интегратор
20 лет

Команда izo:SOC

- Основные задачи:
  - выявление инцидентов на инфраструктуре;
  - оповещение защитников о атаках;
  - поиск информации в ретроспективе по запросу Защитников;
  - сканирование инфраструктуры на определение новых хостов, сервисов и уязвимостей;
  - удаление нелегитимных сервисов и следов взлома.
- Состав:

  5 (4-ДИСБ; 1-СЦ)

Информзащита
Системный интегратор
20 лет

izo:SOC RedTeam

- Основные задачи:
  - Оценка уязвимостей;
  - актуализация возможных векторов атак по факту инцидента изменения инфраструктуры;
  - Расследование инцидентов проникновения;
  - Поиск уязвимостей в защищаемой инфраструктуре
  - Противодействие проведению атак.
- Состав:
  - 5 человек (ОАЗ)

Информзащита
Системный интегратор
20 лет

wizART

- Основные задачи;
  - Защита целевых систем
  - Выдача аналитики по возникающим инцидентам.
- Состав:
  - 10 человек (3-ОБСТ; 3-ОБПС; 3-ОПС; ДД ДП)
- Распределение ролей
  - ОБСТ/ОБПС – базовая техническая защита целевых систем
  - ОБПС/ОПС – аналитика возникающих специализированных атак уровня АСУТП. (ОБСТ-техническое сопровождение, ОПС-аналитика)

Информзащита
Системный интегратор
20 лет

Подготовка к PHD

Работа на стендах:

- Целевые системы: Почта, Интернет магазин, Доменная структура, АСУ ТП.
- Количество стендов: 7 итераций по усложнению
- Используемых виртуальных машин/серверов: 15 серверов, 2 АРМ.
- Используемых СЗИ: CheckPoint, Imperva, SilentDefense, TrendMicro, PaloAlto, Касперский, ArcSight/qRADAR

Информзащита
Системный интегратор
20 лет

Подготовка к PHD

- Работа с вендорами – IBM, Microsoft, CheckPoint, Imperva, PaloAlto, SecurityMatters
- Взаимодействие с производителем стенда IGrids
- Взаимодействие с РТ в части интеграции в инфраструктуру
- Подготовка образов виртуальных машин
- 1-7 мая – аудит инфраструктуры
- 7-15 мая – интеграция и настройка СЗИ и серверов в виртуальной инфраструктуре
- 16 мая – интеграция и настройка СЗИ на площадке

Информзащита
Системный интегратор
20 лет

Архитектура и состав объекта защиты

- Состав объекта защиты:
- Офис:
  - сегмент пользователей (50 АРМ и 20 серверов);
  - сегмент DMZ (28 серверов)
- АСУ ТП:
  - сегмент 10 Квольт (контроллер РТУ)
  - сегмент 500 Квольт (СКАДА WinCC 7.0)
  - сегмент ГЭС (СКАДА WinCC 7.0)
  - сегмент Центр управления (MicroSCADA)

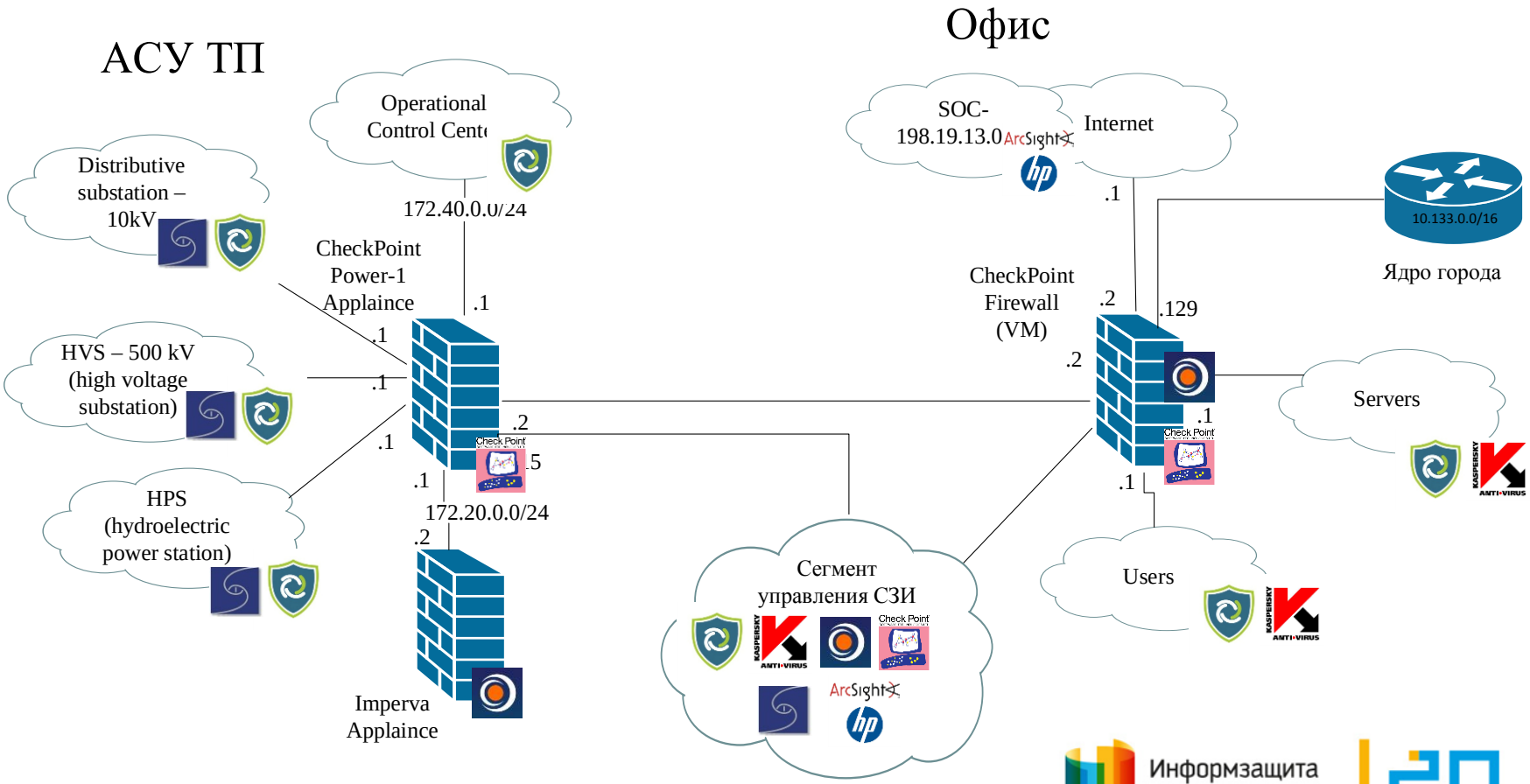
Архитектура СЗИ

Для обеспечения защиты целевых систем использовались следующие прицепы:

1. Любой сегмент должен быть защищен;
2. Защита должна быть многоуровневой;
3. Для сложных средств автоматизации необходимо использовать специализированные СЗИ.

Информзащита
Системный интегратор
20 лет

Архитектура СЗИ



Информзащита
Системный интегратор

20 лет

Как проходила игра

1. Игра без Защитников
2. Защита первого дня
3. Ночь
4. Защита второго дня

Информзащита
Системный интегратор
20 лет

Хронология часть 1

- 4 часа без защиты, результат: ученик 10 класса взломал АСУТП.
- 14:30 Включены системы защиты. Результат: Хакеры не смогли реализовать ни одну из атак и начали возмущаться о плохой подготовки CTF
- 16:30 По просьбе организаторов открыли доступ к офисной сети и к сегменту АСУТП по определенным портам, результата также не последовало;
- 18:30 По просьбе организаторов открыли полный доступ к сегменту АСУТП, результат: был взломан контроллер РТУ;

Информзащита
Системный интегратор
20 лет

Хронология часть 2

- 19:30 По просьбе организаторов открыли доступ в сегмент АСУТП 500 КВольт. и отключили защиту WEB порталов. Результат: начались взломы серверов. Инициализация нелегитимных сервисов
- 22:30 По просьбе организаторов был открыт доступ из офисной сети к сетям SCADA по всем портам, доступ от всех к сетям SCADA по ограниченным портам (портам для SCADA).

Информзащита
Системный интегратор
20 лет

Хронология часть 3

- Взлом 500 КВольт. (На наш взгляд это был самая красивая атака)
- **18 мая 2016**
- Большое количество всевозможных атак: результат взлом РТУ и ГЭС. Атаки на целевые системы выполнялись подбором управляющих команд.
- 13:00 Команда RedTeam начала противодействие выборочным атакам обеспечивали защиту от самых активных хостов.
- 15:00 Отключение всех хостовых средств защиты.

Информзащита
Системный интегратор
20 лет

Яркие моменты

- Ночью был взломан unix-хост в public-сегменте. От сока требовалось проанализировать ранние события, связанные с хостом, понять как его взломали.
- Мы выявили, что взлом был осуществлен через уязвимый сервис PostgreSQL и что злоумышленник закрепился на хосте, создав rsa-ключ для авторизации на ssh-сервере без пароля.
- PostgreSQL был пропатчен, rsa-ключ удален вместе с иными следами взлома.

Яркие моменты

- В 21:00 был определен новый хост в подсети АСУТП с которого выполнялось активное сканирование. Был вычислен его IP и MAC адрес, по MAC адресу был определен производитель и определен тип устройств – WiFi точка доступа. При внимательном осмотре стенда было найдено и отключено указанное устройство.

Информзащита
Системный интегратор
20 лет

Яркие моменты

- В 22:30 Был взлом ГЭС. Хакеры нашли в сети Citrix сервер с учетными записями по умолчанию. С помощью нее взломали внутренний сервер и закрепились во внутреннем сегменте. После чего получили АСУТП проект в котором находился пароль администратора благодаря которому и была взломана ГЭС.

Информзащита
Системный интегратор
20 лет

Используемые СЗИ и их оценка

- EndPoint (не оценивались, т.к. не было достаточно атак)
  - PaloAlto Traps
  - Kaspersky End Point
- Web сервера
  - Imperva (средняя оценка 4)
- Общая защита сети
  - CheckPoint (оценка 5 для защиты сети и 4 в части АСУТП)
- Защита АСУТП (мониторинг и анализ)
  - SilentDefense (оценка 3)

Информзащита
Системный интегратор
20 лет

Результаты

- Всем понравилось ;)
- Выявлены ньюансы взаимодействия СОК\ RedTeam\Защита
- Выявлены особенности функционирования СЗИ
- Получен опыт противодействия реальным атакам на АСУ ТП
- Накоплена база правил корреляции, образцы траффика
- Мы готовы предоставлять новый сервис SOC

Информзащита
Системный интегратор
20 лет

Информзащита
Системный интегратор

20 лет

СПАСИБО