История успеха

АО «Объединенная энергетическая компания»

ОБЪЕДИНЕННАЯ ЭНЕРГЕТИЧЕСКАЯ КОМПАНИЯ

«Объединенная энергетическая компания» усилила контроль безопасности инфраструктуры с помощью PT Network Attack Discovery

АО «Объединенная энергетическая компания» — одна из крупнейших электросетевых компаний Москвы. Занимается развитием, эксплуатацией и реконструкцией принадлежащих городу электрических сетей.

АО «ОЭК» старается сделать так, чтобы ночью в столице было почти так же светло, как и днем. С 1 января 2015 года ОЭК отвечает за работу 503 551 опоры наружного освещения, 659 775 светильников, 1 882 объектов архитектурно-художественной подсветки, праздничной иллюминации и часового хозяйства, расположенных на территории Москвы.

Задача

Positive Technologies провела исследование о целенаправленных атаках на российские компании. Согласно полученным результатам, в III квартале 2021 года 75% реализованных атак были целевыми. Топливно-энергетические организации атаки не обошли стороной. Со сложными киберугрозами уже сталкивались 33% представителей ТЭК.

Принимая во внимание существующие риски, департамент информационной безопасности ОЭК поэтапно выстраивает эшелонированную защиту инфраструктуры. В компании уже были внедрены средства периметровой защиты. Далее было решено усилить контроль безопасности внутренней сети, чтобы выявлять на ранних стадиях даже сложные целевые атаки. Для поставленных задач потребовалось решение, которое покажет, что происходит внутри сети, и не будет требовать долгой настройки. Таким решением стала система анализа трафика (NTA, network traffic analysis).

Задача хакеров — оставаться незаметными в компании максимально долго. Для этого они затирают следы своего присутствия на сетевых устройствах и серверах, но скрыть следы в трафике невозможно. Системы класса NTA выявляют активность злоумышленников и на самых ранних этапах проникновения в сеть, и во время попыток закрепиться и развить атаку внутри сети.

Решение

Весной 2021 года в центральном офисе ОЭК проходило пилотное тестирование системы глубокого анализа сетевого трафика компании Positive Technologies — PT NAD. Специалисты Positive Technologies провели экспертный мониторинг сети с помощью PT NAD, подготовили рекомендации по устранению потенциальных угроз и продемонстрировали возможности системы в реальной инфраструктуре. По итогам тестирования было принято решение о внедрении PT NAD в центральном офисе компании и на удаленных площадках в Москве.

Профиль организации

Название: «Объединенная энергетическая компания»

Отрасль: электроэнергетика

Объем обрабатываемого трафика: 1 Гбит/сек

Задача: выявление целевых атак на ранних этапах, расследование инцидентов, контроль появления новых устройств в сети

Решение: PT Network Attack Discovery (PT NAD) — система глубокого анализа сетевого трафика для выявления атак на периметре и внутри сети

Партнер проекта:
Softline — глобальный провайдер IT-решений и сервисов, который помогает осуществить цифровую трансформацию и предоставляет услуги по информационной безопасности заказчикам из более чем 50 стран и почти 100 городов по всему миру, являясь ведущим международным поставщиком решений для цифровой трансформации, облачных сервисов, информационной безопасности и сопутствующих решений и услуг.

PT NAD обнаруживает действия злоумышленников на разных этапах атаки от разведки до воздействия. Узнайте, какие техники по MITRE ATT&CK выявляет PT NAD и как именно он это делает: mitre.ptsecurity.com/ru-RU/techniques

«PT Network Attack Discovery (PT NAD) — полезный инструмент для мониторинга безопасности сети. После внедрения продукта мы почти **моментально увидели первые результаты, которые помогли нам снизить риски безопасности** и улучшить защищенность инфраструктуры».

Антон Мельник, начальник управления ИБ АО «Объединенная энергетическая компания»

КЛЮЧЕВЫЕ ПРЕИМУЩЕСТВА

- Показывает, что происходит в сети, с первых минут его установки
- Видит активность злоумышленников как на периметре, так и внутри сети
- Выявляет атаки и их последствия даже в шифрованном трафике
- Определяет техники и тактики из матрицы MITRE ATT&CK

PT NAD ВЫЯВЛЯЕТ:

- Перемещение злоумышленника внутри сети
- Угрозы в зашифрованном трафике
- Применение хакерского инструментария
- Активность вредоносного ПО
- Признаки атак, не обнаруженных ранее
- Эксплуатацию уязвимостей в сети
- Признаки сокрытия активности от средств защиты
- Автоматически сгенерированные домены
- Нарушения регламента ИБ

Компания Softline победила в конкурсе на реализацию проекта. Специалисты Softline выделили сегмент для мониторинга и настроили зеркалирование трафика из коммутаторов в PT NAD. Подключение к SPAN-портам коммутаторов позволяет избежать каких-либо воздействий на работу корпоративной инфраструктуры, так как в систему поступает только копия реального трафика. Таким образом, PT NAD выявляет угрозы в трафике в режиме, близком к реальному времени.

Чтобы команда ИБ в ОЭК могла по максимуму использовать возможности PT NAD, специалисты Softline провели тренинг по продукту.

Результат

Благодаря PT NAD специалисты ОЭК отслеживают, что происходит в сети компании и какие узлы в ней есть, получают сведения, которые помогают оперативно устранить нарушения, потенциально интересные злоумышленникам. Например, с помощью PT NAD специалисты ИБ помимо выявления атакующих техник смогут наглядно контролировать сетевую активность при взаимодействии клентских хостов с серверным сегментом, выявлять нарушения регламентов ИБ и ошибки сетевого конфигурирования, а также передачу данных по устаревшим и незащищенным протоколам. Выявление угроз в режиме, близком к реальному времени, позволяет своевременно реализовывать мероприятия по предотвращению нарушений ИБ.

Во время недельного тестирования на проникновение служба ИБ использовала PT NAD как средство мониторинга действий атакующих на всех этапах атаки: от разведки до сбора данных и попыток управления и контроля сети. Также сотрудникам службы ИБ удалось вывести IT-ресурсы из тени. С помощью PT NAD они обнаружили несколько «теневых» приложений (shadow IT), установка которых не была одобрена IT-отделом.

В планах ОЭК интеграция PT NAD с «песочницей» — решением для анализа файлов из трафика на наличие в них новых видов вредоносного ПО.

ptsecurity.com
pt@ptsecurity.com
facebook.com/PositiveTechnologies
facebook.com/PHDays

PT-NAD_uneco_SS_A4.RUS.0002.03.JAN.19.2022