CASE STUDY

Электросети в безопасности: комплексная защита внешнего периметра сети компании АО «ЛОЭСК»

Акционерное общество «Ленинградская областная электросетевая компания» (АО «ЛОЭСК») было образовано 30 августа 2004 года на базе 15 муниципальных предприятий электрических сетей. Сегодня АО «ЛОЭСК» – крупнейшая электросетевая компания на территории Ленинградской области и одно из крупнейших предприятий коммунальной энергетики в Российской Федерации. 6 филиалов организации обеспечивают электроснабжением порядка 150 населенных пунктов региона с населением более 1 млн человек.

Комплексное решение

В 2016-2017 годах по миру прокатилась волна кибератак с использованием вирусов-вымогателей (шифровальщиков), жертвами которых стали сотни фирм из разных индустрий. Так, вредоносная программа WannaCry парализовала работу компьютеров более чем в 150 странах мира. Вирус-вымогатель шифровал информацию на устройствах и требовал за дешифровку выкуп. В России кибератаке подверглись «МегаФон», «ВымпелКом», компьютеры МВД. АО «ЛОЭСК» такая участь миновала, однако эта ситуация заставила обратить более пристальное внимание на информационную безопасность.

Решение, которое организация использовала в то время, уже не соответствовало ни масштабам бизнеса, ни требованиям к функциональности. Например, межсетевой экран и антиспам не были обеспечены антивирусной защитой, что значительно повышало риски заражения как отдельных рабочих станций, так и всей системы предприятия. Нужен был комплексный продукт, который включал бы в себя: межсетевой экран в отказоустойчивой конфигурации (для централизованного выхода в интернет); решение для защиты электронной почты с антиспам-фильтром, встроенным антивирусом и «песочницей»; возможность защиты рабочих станций; централизованное управление системами безопасности, мониторинг всей поверхности атаки и возможность формирования отчетов.

«Внедрение Fortinet Security Fabric позволило нам пересмотреть укоренившиеся подходы к решению вопросов безопасности, ускорить и оптимизировать ряд ключевых процессов. Таким образом удалось значительно усилить защиту внешнего периметра информационной сети компании».

– *Глеб Иванов, начальник сектора системного администрирования, АО «ЛОЭСК»*

По мнению специалистов АО «ЛОЭСК» мультивендорные решения с такой задачей справились бы с трудом. Они усложняют работу и требуют дополнительных расходов на обучение и содержание персонала. В то же время, интегрированная архитектура безопасности Fortinet Security Fabric наиболее полно соответствовала всем требованиям компании.

Сегодня для обеспечения защиты от угроз, предотвращения вторжений, фильтрации веб-сайтов (как зашифрованного, так и незашифрованного трафика) и контроля приложений АО «ЛОЭСК» использует межсетевой экран следующего поколения FortiGate (кластер) – он обеспечивает полное отслеживание приложений, пользователей и сетей. Сейчас решения Fortinet защищают более чем 900 пользователей внутри компании.

Незащищенное веб-приложение — распространенная уязвимость и одна из самых излюбленных у злоумышленников точек входа в систему.

Динамичное развитие АО «ЛОЭСК» также обусловило необходимость внедрения решения, позволяющего эффективно обеспечивать безопасность веб-приложений. Развертывание новых и обновление существующих функций, открытие новых Web API влечет за собой увеличение поверхности атаки и повышает степень уязвимости всей системы. Решение FortiWeb защищает от уязвимостей веб-приложений, ботов и подозрительных URL-адресов, а, благодаря механизму интеллектуального сканирования на базе машинного обучения, обеспечивается защита и от более изощренных угроз, например – таких как внедрение SQL-кода, межсайтовых сценариев, переполнения буфера, подделки маркеров, сомнительных источников и DoS-атак.

Корпоративная электронная почта – один из наиболее распространенных и успешных векторов атак киберпреступников. Согласно отчету Verizon 2019 Data Breach Investigations Report, 94% вредоносных программ было доставлено именно по E-mail. Для защиты столь важной и уязвимой части системы от распространенных и продвинутых угроз, специалисты АО «ЛОЭСК» внедрили решение FortiMail. А FortiClient, интегрирующий средства отслеживания, контроля и упреждения атак, позволяет снизить риски взлома и заражения конечных точек. Важным компонентом системы является «песочница» FortiSandbox, дополняющая всю структуру безопасности и позволяющая выполнять проверку угроз в отдельной безопасной среде.

Еще одной существенной составляющей структуры безопасности является возможность собирать, систематизировать и анализировать информацию со всей системы. FortiManager и FortiAnalyzer обеспечивают централизацию хранения и управления данными, автоматизируют рабочие процессы для более эффективного противодействия нарушениям.

Архитектура Fortinet Security Fabric позволяет осуществлять динамическое расширение и настройку функций безопасности по мере усложнения задач и внесения новых данных. При дальнейшем масштабировании необходимо лишь добавить дополнительные устройства и включить их в систему.

Общая информация

Клиент: АО «ЛОЭСК»

Отрасль: Энергетика

Страна: Россия

Бизнес результаты

- Обеспечение защиты внешнего сетевого периметра
- Обеспечение информационной безопасности важной инфраструктуры

Решение

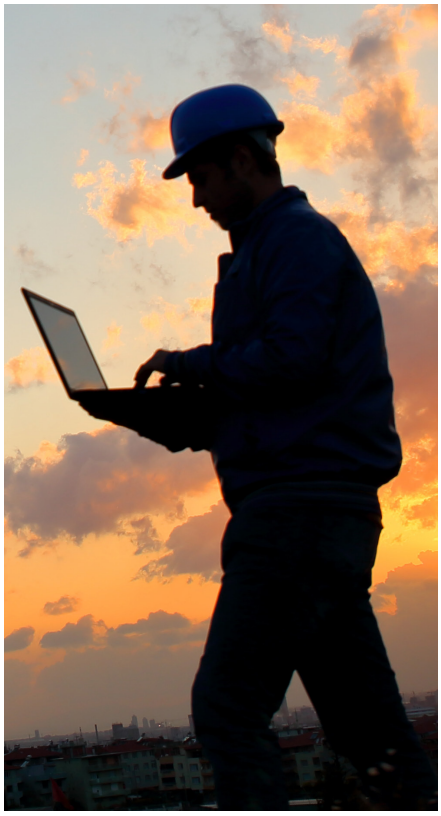
- FortiGate (кластер)
- FortiWeb
- FortiMail
- FortiSandbox
- FortiClient
- FortiAnalyzer
- FortiManager

Внедрение и новые возможности

Базовое внедрение архитектуры Fortinet Security Fabric заняло около 7 месяцев, но обучение персонала не прекращается – система постоянно обновляется, появляются новые функции, позволяющие все более эффективно решать задачи обеспечения безопасности. Специалисты АО «ЛОЭСК» отдельно отмечают высокий уровень поддержки – качественное сопровождение адаптации системы и обучение персонала, быстрое и эффективное решение возникавших проблем. Интегрированность Fortinet Security Fabric обеспечила высокий уровень эффективности защиты всех компонентов корпоративной сети без ущерба для ее производительности и способствовала оптимизации затрат компании на кибербезопасность. Интерфейс архитектуры интуитивно понятен – в зависимости от специализации сотрудники компании смогли достаточно оперативно овладеть всеми инструментами, необходимыми для работы.

Так, благодаря комплексному решению Fortinet, удалось повысить безопасность работы с подрядчиками. SSL VPN портал Fortinet позволяет управлять функциями и инструментами, которые доступны сторонним компаниям, обслуживающим и работающим в информационной системе организации. Таким образом, риск злоупотреблений (несанкционированных действий, утечек информации) со стороны подрядчиков минимизирован.

Компания АО «ЛОЭСК» подписала пятилетний контракт на поддержку решений Fortinet с перспективой дальнейшего расширения сотрудничества. В планах на будущее у компании – внедрение внутрисетевого сегментирования.



FORTINET

www.fortinet.com/ru

December 17, 2019 12:58 PM

565067-0-1-RU

fortinet:Shared:CREATIVE SERVICES:EMEA Creative Server:03_DOCUMENTS:05_CASE_STUDIES:CS_Loesk_JSC_A4_RU:cs_Loesk_JSC_A4_RU