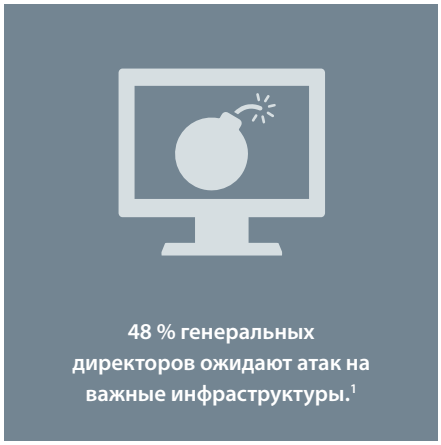
ТЕХНИЧЕСКИЙ ДОКУМЕНТ

Защита предприятий энергетического и коммунального сектора при помощи системы безопасности Fortinet Security Fabric

Аннотация

Предприятия энергетического и коммунального сектора должны позаботиться о внедрении стратегии эшелонированной защиты в сферах операционных технологий (OT) и информационных технологий (ИТ), где существуют серьезные уязвимости. Для этой цели идеально подходит система безопасности Fortinet Security Fabric, которая включает интегрированные автоматизированные функции защиты от угроз, предназначенные для противодействия рискам на предприятиях производства, передачи и распределения энергии и в корпоративных инфраструктурах, а также в сфере обслуживания клиентов.



48 % генеральных директоров ожидают атак на важные инфраструктуры.[1]

Сближение ИТ и OT повышает риски для эксплуатационных технологий

В процессе модернизации своих важнейших инфраструктур предприятия энергетического и коммунального сектора интегрируют сети ИТ и OT в целях повышения эффективности работы. Однако отказ от физического разделения — так называемого «воздушного зазора» — между средами ИТ и OT создает новые возможности для киберпреступников. По данным недавнего исследования, в настоящее время сфера энергетики и коммунальных услуг входит в число трех отраслей, чаще всего подвергающихся атакам в США[2]. Аналогичные тенденции наблюдаются в других регионах, к примеру, в Европе, Австралии и Японии, где зафиксирован значительный рост количества угроз, целью которых являются энергетические и коммунальные инфраструктуры.

В связи с модернизацией OT-сетей, управляющих важными инфраструктурами, эта опасность усугубляется. Отказ от так называемого «воздушного зазора», который в прошлом обеспечивал физическую изоляцию OT-систем от ИТ-сетей и общедоступного Интернета, привел к беспрецедентному росту риска не только вредоносных атак, но и нарушений безопасности с лучшими побуждениями, а также случайных утечек данных.

Основные проблемы кибербезопасности в сфере энергетики и коммунальных услуг

Кибератаки на энергетические и коммунальные системы чреваты негативными последствиями для физических и цифровых инфраструктур. Слабая защищенность электронных коммуникаций может привести к утечке конфиденциальных коммерческих данных и личных данных клиентов. В результате прерывания работы служб в связи с киберугрозами поставщик может понести финансовые убытки, еще более существенный ущерб может быть нанесен клиентам, зависящим от стабильной работы важной инфраструктуры. Диверсионные операции в сети угрожают травмами работникам объектов и даже местным жителям. Кроме того, компании, не сумевшие обеспечить защиту от подобных атак, рискуют своей репутацией. Они могут столкнуться с необходимостью уплатить штраф в связи с несоответствием многочисленным требованиям отраслевого законодательства.

Рис. 1: защита сферы энергетики и коммунальных услуг от вредоносных кибератак и внутренних угроз требует комплексного противодействия атакам по всем направлениям.

По мере внедрения новых форм энергетики степень распределенности инфраструктур растет. Это усложняет задачу обеспечения безопасности сетей предприятий энергетического и коммунального сектора. Отсутствие централизованных компонентов отслеживания и управления рисками в сети снижает эффективность работы в связи с необходимостью выполнения рабочих процессов безопасности и ведения отчетности о соответствии требованиям в ручном режиме. Из-за низкой эффективности замедляется выявление и реагирование на угрозы, создается избыточность, что повышает эксплуатационные расходы (OpEx).

За последние 12 месяцев около 74 % OT-организаций пришлось столкнуться с вторжением вредоносных программ, которые причинили ущерб производительности, доходам, репутации бренда, интеллектуальной собственности и физической безопасности[3].

Примеры использования в сфере энергетики и коммунальных услуг

Корпоративная ИТ-инфраструктура

В корпоративную инфраструктуру предприятий энергетического и коммунального сектора входят сетевые ИТ-службы, имеющие критическое значение для работы распределенных станций и объектов. При поддержке корпоративных сетевых инфраструктур функционируют ключевые бизнес-приложения, в том числе предназначенные для планирования ресурсов предприятия (ERP), а также управления финансами и кадрами. Кроме того, в этих инфраструктурах хранятся конфиденциальные данные о предприятиях, операциях, поставщиках и клиентах. Некоторые данные поступают от датчиков и других устройств Интернета вещей (IoT), которые чрезвычайно уязвимы для кибератак.

Для защиты этих распределенных сетевых ресурсов от продвинутых угроз в системе безопасности Fortinet Security Fabric предусмотрен ряд межсетевых экранов следующего поколения (NGFW) FortiGate. Эти высокопроизводительные межсетевые экраны NGFW поддерживают развертывание в корпоративных центрах обработки данных, на периферии корпоративной глобальной сети (WAN), а также в полевых расположениях. Кроме того, компания может развернуть виртуальные версии межсетевых экранов FortiGate NGFW в любом общедоступном или частном облаке. Все межсетевые экраны FortiGate NGFW поддерживают проверку трафика (в том числе зашифрованных пакетов) на скорости, близкой к скорости сети, и защиту приложений и интерфейсов от множества известных угроз и угроз «нулевого дня». Также они обеспечивают безопасную реализацию ключевых функций сети, к примеру, работу программно-определяемых глобальных сетей (SD-WAN).

Коммутаторы безопасного доступа FortiSwitch служат для защиты точек доступа Wi-Fi FortiAP. Эти точки доступа не только обеспечивают подключение к Интернету или корпоративной сети, но и выступают в качестве первой линии защиты от вторжений. Межсетевые экраны FortiGate NGFW поддерживают настройку нескольких идентификаторов беспроводных сетей (SSID) для предоставления разных сервисов или прав доступа разным группам пользователей: сотрудникам, клиентам и подрядчикам. При входе пользователей в сеть с помощью точек доступа FortiAP автоматически применяются соответствующие политики межсетевых экранов и механизмы проверки подлинности. Кроме того, функции сбора данных о безопасности и управления событиями FortiSIEM обеспечивают автоматизированное реагирование и устранение нарушений до их возникновения. FortiSandbox с помощью технологии выявления продвинутых угроз противостоит ранее неизвестным угрозам и предотвращает утечку данных.

Благодаря средству централизованного управления и автоматизации рабочих процессов FortiManager даже малочисленные группы специалистов по безопасности, занятые в предприятиях энергетического и коммунального сектора, могут эффективно управлять всеми развертываниями межсетевых экранов FortiGate NGFW. Для создания отчетов по запросу заинтересованных лиц и проведения аудита соответствия требованиям целесообразно использовать средство централизованной регистрации и составления отчетов FortiAnalyzer, с помощью которого можно оперативно создать отчет и вернуться к управлению сетями и безопасностью.

Средство облачной защиты от несанкционированного доступа (CASB) FortiCASB, межсетевой экран веб-приложений (WAF) FortiWeb и средство защиты облачной нагрузки (CWP) FortiCWP объединяют многочисленные облака и обеспечивают централизованное управление политиками, что повышает эффективность работы с облачными инфраструктурами и службами. Решение FortiCASB отслеживает все действия и конфигурации инфраструктуры «программное обеспечение как услуга» (SaaS), FortiCWP выполняет мониторинг действий и конфигураций ряда облачных ресурсов, в том числе реализует функции составления отчетов об инцидентах и соответствии требованиям. Решение FortiWeb обеспечивает защиту важных веб-приложений от кибератак, использующих известные и неизвестные уязвимости.

Благодаря удобному средству управления доступом к сети FortiNAC сотрудники отделов безопасности могут отслеживать устройства в сети и назначать соответствующие права доступа для пользовательских устройств. Кроме того, решение FortiAuthenticator обеспечивает управление удостоверениями пользователей, а FortiToken — двухфакторную проверку подлинности. В связи с необходимостью регулярного выполнения корреляции событий безопасности корпоративной сети с физической активностью на объектах в состав системы Fortinet Security Fabric также входят сетевые видеоустройства обеспечения безопасности FortiCamera и FortiRecorder, которые служат для наблюдения за входами и периметром корпоративных объектов.

Безопасность производства

Целью кибератак на предприятия, производящие электроэнергию, является прерывание работы служб, которое чревато как физическим, так и экономическим ущербом. Подобно своим коллегам в офисах организаций, администраторы сетей таких предприятий могут воспользоваться решениями, входящими в состав системы безопасности Fortinet Security Fabric. Однако существуют и специфические для этой сферы факторы, к числу которых относятся преобладание OT-технологий, т. е. большое количество уязвимых устройств без собственных средств управления, и необходимость обеспечивать защиту важных инфраструктур от изощренных угроз. Также на предприятиях по производству электроэнергии или поблизости от них работает немалое количество подрядчиков и других посторонних лиц.

В связи с этими факторами к системе безопасности предъявляются особые требования, которым в полной мере соответствует решение Fortinet Security Fabric:

Обеспечение безопасных подключений между различными устройствами ИТ и ОТ. Межсетевые экраны FortiGate NGFW обеспечивают внутреннюю сегментацию сети ОТ на основе намерений, а также поддерживают отслеживание приложений и протоколов в этой сети. Решение Secure SD-WAN, которое активируется при помощи FortiGate, представляет собой высокопроизводительное средство защиты сетевых подключений с приоритетом важного трафика. Защиту остальной части сетевой инфраструктуры обеспечивают коммутаторы безопасного доступа FortiSwitch и точки доступа FortiAP.

Управление доступом к сети, не создающее неудобств для авторизованных пользователей. Для этого необходимо продуманное сочетание технологий проверки подлинности и авторизации. Система безопасности Fortinet Security Fabric обеспечивает интеграцию лучших в своем классе средств управления удостоверениями пользователей (FortiAuthenticator), двухфакторной проверки подлинности (FortiToken) и управления доступом к сети (FortiNAC). Последнее решение играет особенно важную роль в процессе аудита устройств ОТ, по результатам которого принимаются решения о модернизации или замене уязвимого оборудования.

На предприятиях одной крупной компании в США ежедневно фиксируется более миллиона попыток нарушения безопасности систем[4].

Отслеживание местоположения и действий пользователей на территории предприятия. С помощью средства анализа присутствия по Wi-Fi FortiPresence специалисты по безопасности электростанций могут отслеживать смартфоны и другие мобильные устройства в сети, а также их перемещения. Сетевые видеоустройства обеспечения безопасности FortiCamera и FortiRecorder включают технологии распознавания лиц, которые предотвращают проникновение сотрудников, подрядчиков и поставщиков в запретные зоны.

Оперативное и адекватное реагирование на события безопасности в сети предприятия. Решение FortiSIEM обеспечивает автоматизированное реагирование и устранение нарушений, что повышает эффективность их обнаружения. Оно работает в связке со средством выявления продвинутых угроз FortiSandbox, которое служит для противодействия неизвестным угрозам. Автоматизированная технология маскировки FortiDeceptor скрытно выявляет и устраняет внутренние и внешние угрозы. FortiManager предоставляет возможность управления с помощью одного окна, FortiAnalyzer обеспечивает эффективную защиту от нарушений благодаря функции автоматизированного ведения отчетности.

Безопасность передачи

В состав передающей инфраструктуры предприятий входят высоковольтные линии, водопроводы, газовые и канализационные магистрали. Управление этой инфраструктурой осуществляется с подстанций, на которых не всегда находится персонал. Таким образом, злоумышленники могут физически вмешаться в работу подстанции. Кроме того, они могут использовать точки доступа Wi-Fi и подключения WAN к главному офису в качестве точек входа для атак на передающие сети и даже проникновения в корпоративную сеть.

Решения безопасности Fortinet для передающих сетей решают три важные задачи:

Обеспечение высокой доступности. Решение FortiGate поддерживает настройку активной-пассивной высокой доступности (HA) в целях оперативного переключения на другой ресурс в случае отказа сети или злонамеренного отключения межсетевого экрана NGFW. Решение FortiGate NGFW с включенной технологией Secure SD-WAN автоматически оптимизирует использование всех доступных каналов WAN. Параллельно выполняется проверка трафика, проходящего по всем каналам. Используются также коммутаторы безопасного доступа FortiSwitch, объединенные в общую сеть с точками доступа Wi-Fi FortiAP.

Своевременное реагирование на инциденты. В рамках программы управления инцидентами комплексное средство сбора данных безопасности и управления инцидентами FortiSIEM обеспечивает отслеживание, корреляцию, автоматизацию и устранение угроз. Решение FortiManager служит для централизованного управления всеми продуктами Fortinet, а FortiAnalyzer повышает эффективность защиты от нарушений благодаря мощным функциям автоматизации и управления журналами.

Централизованное наблюдение. Аналогично системам производителей электроэнергии решения FortiCamera и FortiRecorder в целях защиты инфраструктуры обеспечивают визуальное наблюдение за важными физическими расположениями. Кроме того, с помощью аналитического программного обеспечения FortiPresence администраторы подстанций могут выявлять случаи несанкционированного проникновения в здания или зоны путем отслеживания устройств, подключенных к сети Wi-Fi подстанции. Также FortiPresence анализирует закономерности появления в сети пользователей устройств по времени суток, частоте и расположению, что повышает эффективность мер безопасности предприятия.

Управление сетями третьих лиц и удаленных сотрудников. Наша система безопасности поддерживает функции проверки подлинности и управления пользователями (FortiAuthenticator), двухфакторной проверки подлинности (FortiToken) и управления доступом к сети (FortiNAC). Решение FortiClient включает технологии отслеживания и управления конечными устройствами, получающими доступ к расширяющейся сети.

Распределительные сети

Работу современных распределительных систем обеспечивают сложные структуры интеллектуальных измерительных устройств, водопроводов, канализационных магистралей и подстанций. К направлениям атак, связанным с распределительными сетями, относятся промышленные устройства Интернета вещей (IIoT), находящиеся практически во всех сооружениях зоны обслуживания, и сотни подстанций, на которых

сотрудники бывают лишь эпизодически. Все атаки на подключенные к сети устройства IoT предотвратить невозможно, однако важно обеспечить защиту остальных компонентов сети от заражения.

В то же время предприятия сталкиваются с проблемой недостаточной устойчивости и высокой совокупной стоимости владения (TCO) подключений WAN на подстанциях без персонала. Решение FortiGate Secure SD-WAN обеспечивает приоритетность важного бизнес-трафика и приложений. Функции интеллектуальной маршрутизации и восстановления линии поддерживают наивысший уровень производительности и возврат в состояние, предшествующее сбою. Интегрированные компоненты безопасности FortiGate Secure SD-WAN предоставляют защиту сетевой периферии.

Помимо решения Secure SD-WAN система безопасности Fortinet включает ряд других технологий. Межсетевые экраны FortiGate NGFW при поддержке средства управления доступом к сети (NAC) FortiNAC и коммутаторов безопасного доступа FortiSwitch обеспечивают эффективную сегментацию сети и сводят к минимуму риски, связанные с уязвимостями и вредоносными угрозами. На втором уровне защиты решения FortiSIEM, FortiManager и FortiAnalyzer реализуют функции отслеживания и оперативного реагирования. Третий уровень служит для физической защиты сетевых ресурсов, в особенности зданий и оборудования подстанций, при помощи средств наблюдения FortiCamera и FortiRecorder, а также модуля анализа присутствия FortiPresence. И наконец, средство проверки подлинности и управления пользователями FortiAuthenticator и технология двухфакторной проверки подлинности FortiToken предоставляют сторонним пользователям и удаленным сотрудникам безопасный доступ к сети.

Обеспечение удобства клиентов

Клиентов интересует удобный, оперативный и автоматизированный доступ к службам поставщиков электроэнергии и коммунальных услуг при помощи мобильных приложений, систем автоматической оплаты счетов и отображения показаний приборов учета в режиме реального времени. Для взаимодействия с клиентами и предоставления актуальной информации о сбоях систем или ситуациях, угрожающих физической безопасности, поставщики используют одни и те же электронные каналы. DDoS-атаки на веб-сайты предприятий энергетического и коммунального сектора, препятствующие своевременному получению клиентами точной информации, чреваты угрожающими жизни последствиями. Атаки с применением программ-вымогателей, которые блокируют доступ к данным и приложениям предприятия, могут привести к остановке работы.

Организации, на протяжении последних 12 месяцев ни разу не столкнувшиеся с вторжением, на 51 % чаще используют сегментацию сети для ограничения перемещений потенциального злоумышленника, чем организации, испытавшие 6 и более вторжений[5].

78 % OT-организаций имеют только фрагментарную централизованную видимость мер информационной безопасности OT-сред[6].

В целях минимизации этих рисков предприятия энергетического и коммунального сектора могут использовать комплексный пакет технологий защиты от угроз, доступный на базе межсетевых экранов FortiGate NGFW, межсетевых экранов веб-приложений FortiWeb и средства облачной защиты от несанкционированного доступа FortiCASB. После развертывания этих решений в корпоративном центре обработки данных и облаке их можно автоматически настраивать и применять согласованные политики безопасности при помощи центральной консоли FortiManager с поддержкой функций автоматизации и управления журналами FortiAnalyzer.

Конкурентные преимущества решений Fortinet для предприятий энергетического и коммунального сектора

Компания Fortinet предоставляет уникальные технологии, доказавшие свою эффективность в сфере энергетики и коммунальных услуг. К числу конкурентных преимуществ относятся следующие:

Широкий охват отслеживания

Решения Fortinet обеспечивают комплексное отслеживание и интеграцию компонентов безопасности ИТ- и OT-сред. Все межсетевые экраны FortiGate NGFW включают службу ICS, предназначенную для взаимодействия с уникальными протоколами связи OT-систем. Такой подход обеспечивает контекстную осведомленность обо всех событиях и компонентах сетевой среды, а также поддерживает проверку надежности и мониторинг внутреннего и внешнего трафика.

Управление из одного окна

Сети предприятий энергетического и коммунального сектора включают ряд конечных точек, в том числе ICS, устройства IIoT, такие как датчики и измерительные устройства, а также оборудование для наблюдения, к примеру, IP-камеры. Решения Fortinet консолидируют инфраструктуры сети и безопасности, объединяют средства защиты и обеспечивают возможность отслеживания и управления из одного окна.

Устройства повышенной прочности

Средства безопасности Fortinet работают в самых суровых условиях: они выдерживают экстремальные температуры и электрические помехи. Межсетевые экраны FortiGate NGFW и коммутаторы FortiSwitch повышенной прочности обеспечивают защиту важных инфраструктур в любых расположениях.

Защита от внутренних угроз

Решение FortiInsight использует анализ поведения пользователей и организаций (UEBA) для защиты от внутренних угроз и утечек данных в результате злонамеренного или неосторожного поведения. Сегментация на основе намерений изолирует важные системы для защиты от внутрисетевых угроз, FortiDeceptor содействует выявлению и реагированию на угрозы со стороны вредоносных или скомпрометированных учетных записей.

89 % организаций сталкивались с нарушением безопасности своих систем ICS/SCADA[8].

Упреждающий анализ угроз

Для защиты важных инфраструктур необходимы данные об угрозах, специфичных для ICS. За 15 лет работы в сфере безопасности компания Fortinet накопила уникальный опыт и статистику. На основе этой статистики и данных о специфичных для OT угрозах, сбором которых занимается подразделение FortiGuard Labs, компания Fortinet составляет отчеты об угрозах безопасности OT. Первый отчет опубликован в этом году[7].

Опыт отраслевых специалистов

В команду Fortinet входят отраслевые специалисты с многолетним опытом в сфере защиты OT-систем. Этот богатый опыт используется в процессе разработки ведущих в свой области технологий безопасности OT-систем предприятий энергетического и коммунального сектора. Также к нему прибегают руководители отделов безопасности в сфере энергетики и коммунальных услуг.

Надежная экосистема партнеров

Компания Fortinet разрабатывает лучшие в своем классе решения по информационной безопасности, которые благодаря открытому исходному коду поддерживают интеграцию с решениями других поставщиков сетевых технологий и технологий безопасности. Компания Fortinet создала крупнейшую экосистему партнеров, специализирующихся на безопасности OT-систем, и занимается интеграцией сторонних решений при помощи набора открытых API-интерфейсов и встроенных API-интерфейсов, готовых к интеграции решений партнеров Fortinet с нашей системой безопасности.

Заключение

Атаки на важные инфраструктуры национальной значимости могут привести к катастрофическим последствиям, что привлекает спонсируемых государствами злоумышленников, киберпреступников, преследующих корыстные цели, и хакеров-любителей. Руководители отделов безопасности предприятий энергетического и коммунального сектора должны жестко пресекать подобные попытки при помощи стратегий эшелонированной защиты, предусматривающих применение комплексного пакета интегрированных и автоматизированных технологий безопасности.

В основу таких стратегий может лечь система безопасности Fortinet Security Fabric, которая объединяет разрозненные компоненты безопасности и обеспечивает управление политиками и рабочими процессами, а также обмен данными об угрозах. Таким образом, даже малочисленные группы ИТ-специалистов могут управлять полным диапазоном систем безопасности ИТ и OT. Для этого достаточно минимальной квалификации и более умеренных финансовых вложений по сравнению с развертыванием аналогичного количества специализированных средств безопасности и даже других платформенных решений.

[1] Кэтрин Мохаус (Catherine Morehouse), 48% of power and utility CEOs think cybersecurity attack is inevitable: KPMG, Utility Dive, 16 ноября 2018 г.

[2] Стив Ливингстон (Steve Livingston) и другие, Managing cyber risk in the electronic power sector: Emerging threats to supply chain and industrial control systems, Deloitte, 31 января 2019 г.

[3] Shortcomings of Traditional Security and Digital OT: Key Takeaways for Network Operations Analysts, Fortinet, 12 апреля 2019 г.

[4] Марк Джеймс (Mark James) и другие, Improving the Cybersecurity of the Electric Distribution Grid: Identifying Obstacles and Presenting Best Practices for Enhanced Grid Security, Institute for Energy and the Environment, Vermont Law School, апрель 2019 г.

[5] State of Operational Technology and Cybersecurity Report, Fortinet, 15 марта 2019 г.

[6] Там же.

[7] Там же.

[8] Серьезные риски кибербезопасности, которые угрожают системам SCADA/ICS, выявленные в ходе независимого исследования, Fortinet, 28 июня 2019 г.

FORTINET®

www.fortinet.com/ru

23 апреля, 2020 4:59 PM

123456-0-1-RU

wp-protecting-the-power-and-utilities-A4_RU