Технологический обзор

Кибербезопасность сетей предприятий электроэнергетики

Защита служебной сети

Моти Анави
Вице-президент по развитию бизнеса RAD

Аннотация

В данном документе рассматривается ряд проблем, которые возникают при решении вопроса безопасности сетей ICP на предприятиях электроэнергетики. Здесь описываются ограничения текущих решений и предлагаются новые технологии для устранения уязвимостей, присущих коммуникационным сетям.

Содержание

1 Введение

Сети предприятий электроэнергетики всегда значительно отличались от традиционных корпоративных сетей. Хотя определенная часть ресурсов сети предприятия электроэнергетики фактически используется для корпоративных и традиционных коммуникаций, большая часть ее инфраструктуры предназначена для обмена данными с промышленным оборудованием посредством различных протоколов SCADA.

Изначально сети предприятий электроэнергетики были разработаны так, чтобы выполнять единственную задачу: обеспечивать операторов информацией о состоянии электросети. Кибербезопасность не рассматривалась даже в качестве отдаленной перспективы. Фактически, в двадцатом столетии кибератаки были практически неизвестны в промышленной среде. Даже в процессе эволюционирования в современные интеллектуальные сети операторы по-прежнему обеспечивали минимальную защиту инфраструктуры служебной сети.

Наконец, в начале двадцать первого столетия появилось новое понимание потенциальных убытков, к которым могут привести кибератаки. Это, в свою очередь, привело к тому, что операторы стали уделять большее внимание безопасности сетей, имеющих критическое значение. Первым шагом стал набор требований NERC CIP, которые были приняты в 2008 году.
Тем не менее, кибербезопасность рассматривалась преимущественно в рамках ее традиционного ИТ-понимания, и поблемы обрабатывались в рамках такого понимания устранения угроз.

1.1 Традиционные средства защиты

Традиционно защита ИТ устройств основана на двух базовых элементах:

Первый элемент представляет собой “антивирус”, который является программным обеспечением определенного типа, работающим на вычислительной машине. Антивирусное ПО для анализа использует комбинацию "эвристических" моделей поведения вместе с другими моделями или сигнатурами и помогает обнаружить вредоносное ПО, запущенное на зараженной машине.

Вторым элементом является "межсетевой экран". Механизм защиты в ранних версиях межсетевых экранов основывался на настроенном заранее знании приложений, сетевых взаимосвязей между ними и механизма принудительной поддержки существующих взаимосвязей. В этом случае обмениваться данными могут только подтвержденные хосты и приложения. В более поздних версиях межсетевых экранов был добавлен механизм Deep Packet Inspection (DPI), который привел к появлению гибрида межсетевого экрана/антивируса, который может проверять харакетиристики данных, проходящих через межсетевой экран.

1.2 Новые пакетные технологии

Двадцатое столетие было также отмечено началом замены традиционных SONET/SDH/PDH сетей (которые использовались многие годы) сетями на основе новых пакетных технологий. Существует множество предпосылок такой замены, которые не относятся к теме данного документа. Тем не менее, следует упомянуть, что такой переход значительно повышает риск появления киберугроз для электросетей.

Поскольку традиционная технология SONET/SDH неуязвима для кибератак, она значительно менее восприимчива к такого рода угрозам, по сравнению с пакетной технологией, благодаря статической природе

SONET/SDH и отсутствию уровня сигнализации. Кроме того, статическая природа сети не позволяет злоумышленникам менять свое расположение по желанию.

С другой стороны, пакетные технологии по своей природе подвержены бесчисленному количеству угроз. Во-первых, они позволяют динамически проложить путь к любой точке сети посредством системы адресации. Сверх этого, некоторые пакетные протоколы и технологии имеют уровень сигнализации, который делает их особенно уязвимыми для кибератак.

1.3 Защита с помощью секретности

Производители промышленного оборудования всегда придерживались общего мнения, что системы остаются защищенными от кибератак до тех пор, пока их интерфейсы и коммуникационные структуры держатся в секрете от посторонних лиц. Они уверенно считали, что, не имея детализированных спецификаций, злоумышленники не смогут обмениваться данными с оборудованием (и вероятно, даже не станут пытаться это делать). Многие соглашались с тем, что такой подход сокрытия информации заблокирует все возможности для проведения кибератак на отдельные устройства или сети.

2 Уязвимости индустриальных сетей

Как уже упоминалось вначале, основной отличительной чертой сети энергосистемы является использование протоколов управления (Industrial Control Protocol, общеизвестные как протоколы SCADA, системы диспетчерского управления и сбора данных) в дополнение к стандартным корпоративным коммуникациям. Хотя системы SCADA используются не только в энергетике, они примеяются в сети предприятий электроэнергетики для управления критически важным оборудованием. Потеря связи с таким оборудованием или любые даже незначительные сбои в системе связи могут быстро послужить причиной возникновения катастрофических ситуаций, сопровождающихся отключением электроэнергии на несколько дней, недель или даже месяцев. Поэтому безопасность коммуникационной сети имеет критическое значение.

Учитывая, как мало внимания было уделено обеспечению безопасности в сетях энергетиков на начальных этапах их разработки, тот факт, что в текущий момент эти сети содержат множество уязвимостей, не удивителен. В этом разделе мы рассмотрим уязвимости, присущие изначальным проектам сетей, а также современные средства защиты.

2.1 Уязвимости оборудования RTU и SCADA

При разработке промышленных устройств и протоколов вопрос их безопасности практически не учитывался. В лучшем варианте защита осуществлялась с помощью повышенной секретности. В настоящее время ни один из ведущих протоколов SCADA (DNP3 в Северной Америке и МЭК-101 в Европе) не имеет механизмов для выполнения аутентификации или проверки каких-либо команд, которые они получают. Эта уязвимость была продемонстрирована в рамках проекта Аврора в 2007 году в национальных лабораториях Айдахо, в котором группа хакеров должна была повредить учебную электростанцию. Хакеры успешно проникли на учебную электростанцию и запустили процесс самоуничтожения генератора. Появление вируса STUXNET в 2010 году стало очередным болезненным напоминанием об этой уязвимости. Вирус STUXNET отправлял ложные и вредоносные команды на Siemens PLC через множественные лазейки в защите консоли управления.

Фирменные свойства оборудования RTU и SCADA также создают проблемы. Из-за высокой чувствительности кода ПО промышленного оборудования операторам сетей предприятий энергетики часто запрещено вносить

какие-либо изменения, такие как обновление операционной системы или установка заплаток в системе безопасности. В результате существует множество брешей в системе безопасности, которые не покрываются существующими исправлениями или другим способом в RTU или промышленном оборудовании, которое работает на стандартных операционных системах.

Наконец, слабые стороны подхода, основанного только на секретности, обсуждались много раз, не только в упомянутых выше случаях, но также в более позднее время на демонстрациях конференции Black Hat, включая удаленное управление системами командования патрульной службой и дозаторами инсулина.

2.2 Уязвимости в сетях предприятий электроэнергетики

Одним из редко рассматриваемых вопросов анализа уязвимостей является используемая сетевая технология. Поскольку традиционные системы редко подвергались атакам, а более современные сети защищены лишь в небольшой степени, безопасность используемых сетевых технологий не изучалась должным образом в контексте сетей электроэнергетики.

Существуют две крупные уязвимости, которые связаны с используемой сетевой технологией:

- Атаки на уровне управления сети (control plane) – некоторые из сегодняшних пакетных сетей имеют уровень управления, созданный разработчиками протоколов для упрощения предоставления каналов связи. Пока этот аспект сети успешно используется для разработки схемы каналов в сети, он также открывает огромную уязвимость. Возможнось динамически задавать пункты назначения с помощью таких протоколов, как BGP и OSPF, открывает возможность для разрушения сети или вывода ее из строя. Путем простого распространения вредоносной информации злоумышленник может сделать так, что сеть будет отправлять трафик в никуда, создавая кольца из маршрутов или выполняя другие вредоносные действия. Фактически это позволяет вывести из строя всю сеть, используя один интерфейс. В протоколах, которые используют IP, MLPS и MPLPS-TP, отдельный незащищенный узел может послужить причиной выхода из строя всей сети. Именно это произошло в конце 2010 г в Китае., когда неверная информация о маршрутах от одного ISP привела к тому, что Интернет был недоступен.

  Проблему усугубляет тот факт, что сети предприятий электроэнергетики обычно содержат достаточно большое количество физически незащищенных мест. Злоумышленник может легко проникнуть на автоматическую подстанцию, ввести вредоносную информацию в сеть и полностью деактивировать ее.

- Атаки на уровне передачи данных (data plane) – атаки Denial of Service (DoS) представляют собой классический пример атак при передаче данных. Как правило, DoS атаки бомбардируют цель множеством фальшивых запросов на соединение, что приводит к истощению ресурсов принимающей стороны настолько, что она с трудом обрабатывает действительные запросы. Иногда все ресурсы истощаются и система становится полностью недоступной. DoS атаки являются достаточно простыми в исполнении, они нацелены на самую чувствительную часть сети – способность к установке соединения. Для предприятия электроэнергетики потеря связи с RTU или оборудованием релейной защиты может очень быстро привести к потере контроля над электросетью и отключению электроэнергии на значительной территории. Поэтому DoS атаки особенно опасны для внутренних служебных сетей.

  DoS атаки не являются единственным серьезным типом атак на уровне передачи данных. Другие атаки включают перехват сетевых ресурсов и нападения на станции управления.

Сочетание этих двух плоскостей атак представляет значительную уязвимость, которая неизбежно

присутствует в сети. Уязвимость зависит от архитектуры и реализации сети и может быть исправлена или сведена к минимуму в результате пересмотра сетевой архитектуры.

3 Подходы к защите от угроз кибербезопасности

Для устранения уязвимостей операционных сетей применяются несколько тактик. Как упоминалось во введении, современные подходы к обеспечению безопасности различаются, однако существует тенденция, когда основное внимание уделяется IT природе сети.

3.1 Защита периметра

Первый набор защитных средств нацелен на запрет любых контактов сети с узлами, лежащими за ее пределами. К средствам защиты периметра сети относятся:

- Межсетевые экраны – разработаны для управления обменом информацией. Они позволяют создавать соединение только между заданными объектами и могут разрешить или отклонить запросы на соединение, а также проверить имя пользователя и пароль удаленных пользователей. Тем не менее, их эффективность ограничена, поскольку после того, как они разрешают установить соединение, они не владеют информацией о том, какие данные передаются. Таким образом, вредоносный код или ложные данные потенциально могут попасть в сеть.
- Однонаправленные межсетевые экраны – эти устройства разработаны таким образом, чтобы обеспечить "физическое" отделение служебной сети от пользователя, отслеживая запросы на соединение. Они позволяют информации двигаться только в одном направлении – из служебной сети наружу – и минимизировать уязвимость критически важных компонентов, сокращая вероятность управления ими извне.
- Зашифрованные VPN сети – это средство обычно используется в сочетании с межсетевыми экранами. Оно позволяет выполнить безопасный обмен данными между различными элементами периметра безопасности ESP(Electronic Security Perimeter). В сущности, они служат для защиты от атак "человек посередине", нацеленных на получение доступа к управляющей информации.

Большинство мер по обеспечению безопасности вытекают из концепции защиты периметра сети. Ограничения таких мер обычно связаны с тем, что физически внедриться в сеть предприятия энергетики довольно просто. Если другие сети (например, операторские) размещают свое оборудование в хорошо защищенных помещениях, таких как узлы и центральные офисы, коммуникационное оборудование предприятий электроэнергетики расположено в безлюдных, плохо защищенных местах. Сюда достаточно просто проникнуть физически и обойти всю защиту периметра сети. Поэтому критически важно свести к минимуму возможность проникновения в сеть. Именно здесь требуется применять дополнительные меры защиты.

3.2 Защита сети

Используемая архитектура и протоколы связи также содержат множество потенциальных уязвимостей для сети предприятия энергеики. Не смотря на то, что зачастую этот аспект не учитывается, выбранная сетевая технология может значительным образом повлиять на стабильность и восприимчивать сети к кибератакам. Как указано в предыдущей главе, существует несколько способов обойти систему безопасности сети, к которым относятся атаки на уровнях управления и передачи данных. Соответственно, существуют методы сведения к минимуму или подавления этих угроз таким образом, который позволяет повысить безопасность и отказоустойчивость сети, не оказывая влияние на ее производительность.

3.3 Противодействие атакам на уровень управления

Одним из наиболее опасных типов атак является атака на уровне управления, когда атакующий повреждает управление сетью. В результате сеть становится полностью недоступной. Такой тип атаки вызывает особое беспокойство, поскольку получение доступа по крайней мере к одному узлу потенциально может привести к выводу из строя всей сети. В сущности, вся сеть защищена ровно в той степени, насколько защищен наиболее слабый канал. Получается, что безопасность сети электроэнергетического предприятия зависит от доступа на наименее защищенную подстанцию.

Сети, которые включают уровень управления или протокол сигнализации, очень чувствительны к атакам такого типа. К ним относятся сети типа MPLS и IP. Уязвимости на уровне управления были продемонстрированы множество раз, как организациями стандартизации (см. IETF RFC 4272, 5920 и 6941), так и на хакерских конференциях. Фактически, техника вывода из строя сети MPLS через уровень управления была продемонстрирована в реальном времени на конференции Black Hat в 2011 году.

Поскольку подавление атак возможно только до определенной степени, угроза опасности остается до тех пор, пока существует плоскость управления. Сети, основанные на технологии без уровня управления, всегда будут более надежными. К ним относятся сети SONET/SDH и Carrier Ethernet. Средств для проведения атаки на уровень сигнализации сетей SONET/SDH или Carrier Ethernet не существует. Обе технологии требуют наличия управляющей станции для функционирования сети. Как только обеспечивается безопасность управляющей станции, атаки на плоскость управления становятся невозможными.

3.4 Противодействие атакам на уровень передачи данных

Атаки на уровне передачи данных также являются потенциальным источником угроз. Хотя такие атаки имеют тенденцию быть более узконаправленными (например, DoS атаки направляются на определенный хост), потенциальные потери связи между станцией HMI и RTU могут помешать управлению сетью. Также, как и в случае атак, направленных на уровень управления, атаки на уровне передачи данных могут быть подавлены в результате изменений схемы сети.

В сценариях, где соединения связи заданы жестко (как в случае SONET/SDH или Carrier Ethernet), атакующему гораздо сложнее изучить сетевые элементы без установки с ними прямого соединения. Такая жесткость плоскости передачи данных открывает минимальное количество частей каждого хоста в сети, а также закрывает остальные части, которые могут быть более уязвимыми. В тех случаях, где существует маршрутизируемая сеть (такая как MPLS и IP), злоумышленник может в первую очередь собрать информацию путем перехвата и шпионажа в сети с незащищенного узла, после чего использовать ложные адреса для подготовки атаки.

Другим способом повышения безопасности и защиты от нелегального проникновения или намеренного искажения информации является использование протоколов аутентификации источника. Наиболее важным из них является 802.1X на основе Ethernet, который проверяет каждое добавленное устройство в централизованно управляемой базе данных. Он использует шифрование для того, чтобы проверить подлинность нового устройства и удостовериться, что оно не маскируется под существующее сетевое устройство. Это гарантирует, что все подключенные к сети устройства действительно являются настоящими аутентифицированными сетевыми устройствами, а не устройствами, добавленными хакерами.

3.5 Внутренняя защита приложений (защита от вредоносного ПО)

Одними из наиболее сложных для обнаружения атак являются атаки изнутри, которые производятся с элементов, расположенных в сети. Внутренние атаки представляют угрозу с различных точек зрения.

Во-первых, крайне сложно принять решение относительно того, является ли определенная команда действительной или вредоносной. Некоторые команды (например, команда на вывод из эксплуатации старого блока RTU) могут корректно использоваться в тех случаях, когда их отправляет авторизованный персонал, однако могут нанести вред, если они были отправленны другими лицами без надлежащих полномочий.

Во-вторых, поскольку атаки проводятся по различным направлениям, для обеспечения безопасности всей сети требуется система, которая присутствует во всех элементах и плоскостях, а также отслеживает все возможные направления атаки. Некоторые утилиты используют межсетевой экран для подавления риска того, что один узел будет контролировать другой, а также для сдерживания киберугроз на месте их возникновения. Тем не менее, это может привести к более обширной, чем хотелось бы, блокировке или отключению сети. Чем крупнее подстанция, вовлеченная в этот процесс, тем выше риск поражения сети.

Наконец, стандартному межсетевому экрану тяжело контролировать команды. Хотя стандартные межсетевые экраны с активной функцией DPI способны проверять полезную нагрузку программного обеспечения с целью определить, присутствует ли там выделенная ранее сигнатура, и отмечать потенциальные совпадения, они не имеют возможности оценить, является ли определенная команда истинной или вредоносной.

Все эти ограничения представляют, казалось бы, непреодолимые сложности, когда речь идет о внутренних угрозах. При этом, в соответствии с NERC CIP ожидается, что электроэнергетические предприятия будут решать такие проблемы. В частности, согласно NERC CIP ожидается, что электроэнергетические компании должны обнаруживать и блокировать ситуации, когда некое оборуование, RTU или консоль управления, захвачено вредоносным ПО, и смогут остановить выполнение вредоносных действий.

Для того, чтобы сеть смогла справиться со всеми ограничениями, которые появляются в результате существования внутренних угроз, требуется учесть несколько факторов. Распределенный характер возможных атак приводит к тому, что централизованное или переходное решение не подходит для решения таких проблем. Кроме того, решения должны "понимать" ICS протокол и интеллектуально распознавать команды, чтобы определить, является ли определенная команда действительной или вредоносной.

Следовательно, идеальное решение представляет собой распределенный межсетевой экран с проверкой команд ICS. Решение такого типа может присутствовать во всех элементах, поскольку оно интегрировано в структуру сети (являясь частью сетевого коммутирующего оборудования). При этом, способность межсетевого экрана с поддержкой ICS определять достоверность различных команд систем SCADA используется для того, чтобы обнаружить внутренние атаки или угрозы, возникающие в результате попадания вредоносного ПО в сеть.

Два основных элемента идеального решения - присутствие во всех частях сети и распознавание приложений - вытакают из характеристик атак. Распределенный характер сетей предприятий электроэнергетики, а также тот факт, что большинство элементов сети могут быть не защищены должным образом, заставляет предпочесть распределенный подход централизованному. Единственным способом внедрения такого решения без того, чтобы весь трафик не перенаправлялся в центр, вызывая перегрузку, является распределенное

использование интеллектуального анализа команд.

Здесь в связи со сложностью обнаружения вредоносных атак возникает требование распознавания трафика приложений. Вредоносные программы обычно размещаются на действующих управляющих станциях и проверяемых хостах. Изменениям подвергается только содержание управляющих сообщений. Чтобы обнаружить такой тип искажения информации, такие сообщения должен проверить внешний элемент, свободный от атаки. Для этого требуется производить интеллектуальный анализ и проверку каждой команды, что приводит к необходимости использования средств распознавания приложений.

4 Многоуровневая сетевая защита систем управления производственным процессом (ICS)

Как упоминалось выше, служебные сети электроэнергетических предприятий сталкиваются с огромным количеством потенциальных киберугроз. Такие угрозы охватывают несколько векторов атак, а каждая уязвимость имеет свою собственную стратегию защиты. Таким образом, сеть может быть реально защищена только при условии применения множества средств защиты на различных уровнях. Если коротко, только таким способом можно защитить систему от каждого вектора атак и покрыть все уязвимости, которые появляются в случае использование отдельной защитной стратегии.

Применение защитных средств на различных уровнях называется глубокой защитой (Defense-In-Depth). Стратегия глубокой защиты направлена не на построение непроницаемой единой стены, но на построение различных уровней защиты. Такие защитные средства используют сочетание различных тактик для того, чтобы обнаружить и заблокировать атаку.
В служебных сетях предприятий электроэнергетики такой подход должен применяться на всех уровнях и векторах потенциальных атак.

4.1 Стратегия глубокой защиты в ICS системах на предприятиях электроэнергетики

В сетях электроэнергетики применение стандартных межсетевых экранов и антивирусного ПО является не достаточным для того, обеспечить глубокую защиту. Такой подход нацелен только на один вектор защиты, он окажется бесполезным, если атакующий проникнет в сеть или воспользуется вредоносным ПО для отправки вредоносных команд. По этой причине применяется стратегия многоуровневой защиты по всем векторам атак, особенно в критически важной служебной сети или сети автоматизации.

В ICS сети каждый уровень глубокой защиты имеет свои преимущества и недостатки. Работая на каждом уровне, комбинированное решение успешно обеспечивает защиту от:

1. Удаленных атак, которые проводятся из другого местоположения. Защита достигается путем использования межсетевого экрана и межсайтового шифрования. Эти действия не позволяют хакерам получить доступ к внутренним сетям "логически".

2. Атаки "человек посередине". Защита достигается путем применения межсайтового шифрования, что предотвращает повреждение или фальсификацию данных.

3. Атаки на уровне управления сети. Защита достигается с помощью определенной архитектуры сети. Например, выбор инфраструктуры с высокой степенью защиты, такой как Carrier Ethernet или SONET/SDH вместо MPLS или MPLS-TP.

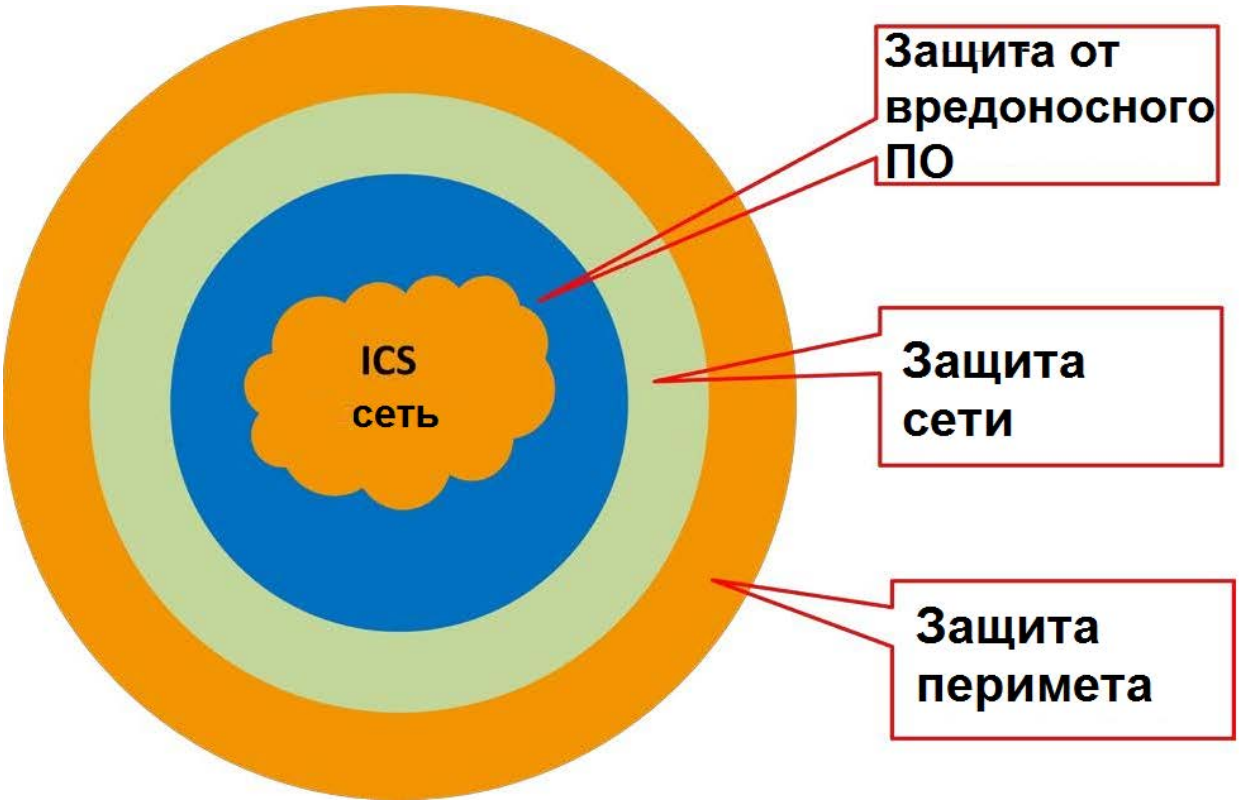
4. Атаки с маскировкой. Устраняются с помощью протоколов аутентификации источника, таких как IEEE802.1X, которые проверяют, что определенный хост не был заменен другой машиной, которая отправляет вредоносные данные.

5. Перехват данных и шпионаж. Защита достигается путем использования сетевых технологий с жестким определением пути и универсальным адресным пространством – таких как Carrier Ethernet.

6. Вредоносные атаки с RTU, управляющих станций или HMI. Устраняются путем использования распределенных межсетевых экранов с распознаванием приложений. Такие межсетевые экраны могут углубленно проверяют трафик SCADA чтобы убедиться, что команды относятся к приложению управления или автоматизации – помимо проверки, что устройства являются элементами сети автоматизации.

4.2 Множественные уровни защиты

Должным образом разработанная ICS сеть окружена множеством защитных слоев, где каждый слой нацелен на защиту от определенного типа атаки. Когда один уровень защищает от одного типа атаки, следующий уровень покрывает его уязвимости. Лежащая в основе ICS сеть может быть полностью защищена только в том случае, когда все уровни работают одновременно. В противном случае, каждый отдельный уровень может быть атакован и выведен из строя относительно просто.



5 Заключение

ICS сети чрезвычайно уязвимы дляк кибератак. Они не только уязвимы для традиционных угроз, которые часто встречаются в корпоративных сетях, но также подвержены атакам, для которых не существует распространненых средств защиты. К ним относятся вредоносные атаки, нацеленные на уровень управления ICS. Незащищенная физическая часть служебной сети предприятия электроэнергетики – вместе с существующими необслуживаемыми подстанциями – также может подвергаться атакам на уязвимости сетевой технологии, лежащей в основе сети предприятия.

Все эти атаки могут быть подавлены и удержаны на начальных векторах с помощью стратегии глубокой защиты. Глубокая защита представляют собой широкий набор средств для защиты различных уязвимостей сети предприятия электроэнергетики. Ко множеству уровней относятся защитные средства периметра вместе с сетевой защитой и защитой от вредоносных программ.

Архитектура сети играет критическую роль в уровне уязвимости сети. Такие технологии, как Carrier Ethernet, которые по определению более безопасны, могут значительно снизить уязвимость. И наоборот, такие технологии, как MPLS, могут усилить уровень уязвимости сети и потенциально позволяют злоумышленникам завладеть сетью целиком, используя простую брешь в физической защите.

Защита от вредоносных программ должна входить в функции постоянно активного распределенного межсетевого экрана с распознаванием приложений, который способен блокировать внутренние атаки. Такой экран может защитить в ситуациях, когда злоумышленник не совершает атаку извне, а проникает сквозь периметр сети.

В конечном итоге, сетевая безопасность сети предприятий электроэнергетики должна серьезно рассматриваться на каждом этапе разработки архитектуры сети, а не только в качестве завершающей процедуры ее создания. Такое тщательное планирование может значительно улучшить отказоустойчивость сети и сократить затраты на обеспечение безопасности.

www.rad.com
www.rad.ru

Международный главный офис
RAD Data Communications Ltd

.
24 Raoul Wallenberg St.

Tel Aviv 6971923 Israel

Тел: 972-3-6458181

Факс: 972-3-6498250

E-mail: market@rad.com
www.rad.com

Региональныйофис в Росии
RAD Data Communications

Ул. Б.Тульская 10, строение 9 5 этаж, офис 9506

Москва, 115191, Россия

Тел.: 7-495-231-1239 |

E-mail: info_russia@rad.ru

www.rad.ru