Особенности организации удаленного мониторинга и диагностики энергетического оборудования

Вячеслав Половинко, *руководитель направления собственных продуктов Департамента информационных систем АМТ-ГРУП*
Илья Зуевский, *руководитель проектов Департамента информационных систем АМТ-ГРУП*

Сегодня однонаправленные шлюзы — это распространенное средство защиты, которое широко используется во всем мире. Их применение является передовой практикой, которую рекомендуют к внедрению ведущие эксперты по информационной безопасности, регуляторы и экспертные организации. В этой статье мы рассмотрим примеры защиты сетевого периметра с применением устройств класса “диод”.

ИТ-инфраструктура современного предприятия уже давно предполагает значительную распределенность в пределах локальной вычислительной сети, а также выход за контролируемый периметр, и даже может пересекать физические границы страны, в том числе находиться в другой правовой юрисдикции.

На практике такая распределенность может выглядеть как:

- использование предприятием арендуемых аппаратных мощностей (VM) по принципу IaaS;
- использование стороннего ПО на принципах SaaS;
- использование различных сервисов государственных и регулирующих органов, новостных сервисов и сервисов аналитики, взаимодействие с контрагентами и службами технической поддержки оборудования и ПО;
- использование сторонних услуг SOC и NOC;
- развитие облачных и ресурсоемких систем Data Science и Machine Learning и т.п.

Любой из приведенных выше примеров показывает использование ресурсов, находящихся далеко за пределами периметра сети отдельного предприятия. Как следствие, практически каждая локальная сеть имеет сопряжение с сетью Интернет и сетями сторонних организаций. К сожалению, очень часто такие точки взаимодействия не имеют каких-либо дополнительных средств защиты, кроме стандартных межсетевых экранов.

Удаленные сервисы на предприятиях энергетики

Требования, предъявляемые к современному предприятию, предполагают определенную степень открытости и взаимодействия. Без этого невозможно построение современного конкурентоспособного и развивающегося бизнеса. В частности, особую важность приобретает взаимодействие с поставщиками (вендорами) промышленного оборудования. Не является здесь исключением и энергетический сектор. Например, компания GE еще в 2018 г. предложила[1] своим клиентам программные продукты по управлению эффективностью активов на базе разработанной облачной платформы. Решение в том числе позволяет проводить техническое обслуживание "по состоянию" и осуществлять удаленный мониторинг оборудования из глобального центра мониторинга и диагностики. Это только один из примеров наиболее тесного сопряжения сетевых ресурсов предприятия энергетики со сторонним поставщиком в целях организации мониторинга и поддержки.

Очень часто сервис, который предлагается производителем, носит удаленный характер взаимодействия. В первую очередь это связано с тем, что нередко для анализа ситуации или расследования какого-либо инцидента требуются специализированные решения вендора – его внутренние системы, профильные эксперты, сотрудники службы технической поддержки.

Другими примерами взаимодействия предприятия энергетики с внешними контрагентами в части обмена информацией могут быть:

- передача данных об ошибках в работе оборудования его производителю;
- вывод "картинки" в экспертный ситуационный центр;
- передача данных в специализированные организации, оказывающие услуги по устранению инцидентов безопасности;
- обмен данными с третьей и четвертой линиями технической поддержки производителей и поставщиков и т.п.

"Диоды" для защиты удаленного периметра

Новые технические и сервисные возможности, предполагающие расширение границ бизнеса и повышение его конкурентоспособности, одновременно расширяют контролируемый сетевой периметр и идут бок о бок с новыми вызовами в области информационной безопасности. Неконтролируемый и непрогнозируемый доступ к защищенному сегменту предприятия порождает угрозы из сопрягаемых сетей, которые могут приводить к катастрофическим последствиям. За последние несколько лет уже наблюда-

[1] *https://www.ge.com/news/press-releases/ge-представила-сервисные-решения-для-повышения-производительности-и-надежности*

лись примеры неконтролируемого распространения вирусов и скомпрометированного ПО из внешних сетевых сегментов, обладающих меньшим уровнем доверия. Такое распространение обычно происходит веерно и исключительно быстро.

Производители оборудования, ПО, АСУ ТП для предприятий энергетики и сами стараются предлагать самые различные инструменты для устранения этой проблемы (NGFW, специализированные маршрутизаторы промышленного трафика, средства защиты информации и т.п.).

В последнее время одним из применяемых на практике решений стало использование устройств класса "диод" (однонаправленный шлюз). На западных рынках применение таких устройств в промышленности и энергетике уже давно является стандартом и "настойчивой рекомендацией" регуляторов[2, 3, 4].

Особое внимание производителей, предприятий энергетики и представителей регуляторов к такому классу решений связано с тем, что на данный момент число доступных практических сценариев использования "диодов" значительно выросло. Важной особенностью всех этих сценариев является тот факт, что во всех случаях применения "диодов" обеспечивается гарантированная защита сетевого сегмента от какого-либо внешнего воздействия на физическом уровне. Несколько возможных сценариев их применения для предприятий энергетики в целях решения задач мониторинга представлены ниже.

Однонаправленные шлюзы могут применяться для репликации различных источников данных из технологической сети предприятия в некую стороннюю сеть, в том числе в сеть производителя оборудования. Репликация исторических данных, доставка файлов могут быть использованы в сценариях предоставления отчетности, обмена сырыми данными и файлами, обеспечивающими сопровождение процессов отладки и мониторинга. Внешние пользователи и приложения, например служба технической поддержки производителя оборудования, могут обращаться к ним без какой-либо угрозы для технологической сети и оборудования критической инфраструктуры предприятия.

Еще одним сценарием применения "диодов" является передача Syslog-трафика и трафика, циркулирующего в технологическом сегменте предприятия, на специализированные серверы/системы безопасности сторонней организации или в пределах одного предприятия.

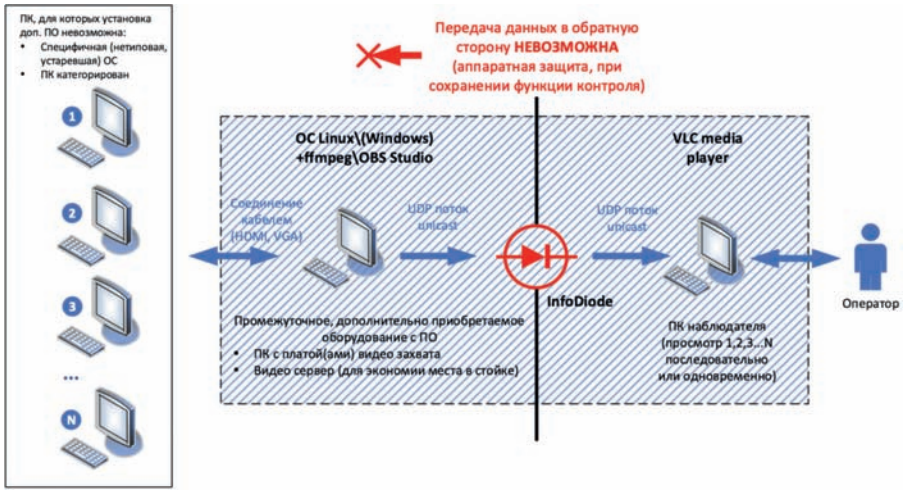

Схема передачи видеотрафика и снимков рабочего стола

Такая передача выполняется для фиксации событий в SIEM-системах, специализированных системах обнаружения вторжений и изменения сетевой топологии, функционирующих в рамках корпоративных SOC, NOC-центров. В тех случаях, когда предприятие имеет филиальную структуру, решение с применением однонаправленных шлюзов может использоваться для сбора/передачи данных в головные SIEM-системы и центры компетенций.

Другим вариантом эффективного взаимодействия в условиях гарантированной защиты от внешнего воздействия может быть организация стриминга данных через "диод" с автоматизированных рабочих мест в защищенном сегменте и демонстрации этих данных получателю через стандартные средства воспроизведения видеопотока. Такой сценарий позволяет обеспечить эффект присутствия внешнего специалиста или эксперта и своевременно оказать качественную поддержку сотрудникам предприятия в режиме реального времени. Рассмотрим такой кейс более подробно на примере следующей схемы передачи видеотрафика и снимков рабочего стола (онлайн) (см. рис.).

Стриминг и воспроизведение видео от источника/источников в закрытом сегменте к приемнику в открытом сегменте осуществляется по протоколу UDP в режиме unicast (см. схему организации стриминга на рис.). Передача UDP-потока с одной рабочей станции на другую в изолированный сегмент сети осуществляется через "диод" и исключает возможность какого-либо воздействия на защищаемый сегмент. В качестве ПО для просмотра полученного сигнала на рабочих станциях также могут применяться общедоступные и бесплатные решения/плееры.

Следует обратить внимание на то, что описанный выше сценарий может быть реализован как с использованием аппаратно-программного решения ("диодов", включающих и программную, и аппаратную компоненты), так и аппаратного решения.

Подводя итог

Еще несколько лет назад межсетевые экраны были фактически единственной доступной технологией, способной защитить наиболее критические объекты сети и отделить их от сетей сторонних обслуживающих организаций и сети Интернет, обеспечивая при этом мониторинг и сбор информации из закрытого сегмента. Однако современные компьютерные атаки демонстрируют способность планомерно и эффективно обходить все программные средства обеспечения безопасности, в том числе межсетевые экраны. Поэтому современное предприятие в области энергетики, равно как и в других областях, безусловно, должно рассматривать весь перечень доступных средств защиты своих процессов и организации их безопасного мониторинга. Это связано не только с ростом числа атак на промышленные объекты, но и с ростом количества точек сопряжения локальных сетей с внешними, не контролируемыми сетевыми сегментами. Возможно, в данном случае не стоит дожидаться формирования более четких требований и рекомендаций по применению "диодов" со стороны регуляторов, которые, в свою очередь, могут отставать от западных практик на 2–3 года. ●

Ваше мнение и вопросы присылайте по адресу
is@groteck.ru

[2] *NSA and CISA Recommend Immediate Actions to Reduce Exposure Across Operational Technologies and Control Systems, https://us-cert.cisa.gov/ncas/alerts/aa20-205a*

[3] *NIST SP800-82. Guide to Industrial Control Systems (ICS) Security https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf*

[4] *Cybersecurity for Industrial Control Systems - Документ Национального агентства по безопасности информационных систем Франции, https://www.ssi.gouv.fr/uploads/2014/01/industrial_security_WG_Classification_Method.pdf*