Сегодня в России нет организаций, которые занимались бы мониторингом ситуации с безопасностью АСУТП системно, это вне компетенции любого из существующих госорганов. Именно поэтому «Лаборатория Касперского» видит необходимость в создании Национальной российской тестовой лаборатории по исследованию проблем информационной безопасности критически важных объектов. Такой единый центр мог бы на федеральном уровне исследовать как уже известные, так и перспективные подходы по организации защиты АСУТП, своевременно обнаруживать проблемы информационной безопасности в используемых программных и аппаратных средствах, вырабатывать рекомендации по их устранению, информировать соответствующие предприятия, рекомендовать к использованию протестированные программно-аппаратные средства, обладающие высокими показателями устойчивости к кибератаке и т. д.

Наряду с этим для защиты ИТ-инфраструктур промышленных объектов нужны и принципиально новые методы и продукты. Многие производители решений информационной безопасности сейчас пытаются внедрять свои обычные, «офисные» продукты в АСУТП, однако это неверный подход. В промышленных системах есть своя специфика, и нужны продукты, ее учитывающие. Именно поэтому «Лаборатория Касперского» сейчас работает над созданием ряда специальных решений, предназначенных для защиты АСУТП от самых разных киберугроз.

Контактный телефон (495) 797-87-00)
Http://www.kaspersky.ru/contacts

Мониторинг активности в промышленных системах и сетях как безопасный подход к борьбе с киберугрозами

А.С. Шипулин, А.Ю. Соболев (Компания КРОК)

Развитие средств и систем автоматизации, активное использование на уровне управления ТП компонентов ИТ-инфраструктуры и развитых средств коммуникаций приводит к проникновению киберугроз, к возрастанию рисков нарушения штатного функционирования систем и остановке или выходу из-под контроля ТП. Это происходит за счет умышленного несанкционированного доступа к управлению или неумышленных ошибочных действий персонала и нецеленаправленного распространения и воздействия вредоносного ПО (ВПО). Рассматривается один из возможных подходов к борьбе с киберугрозами, основанный на использовании решений по мониторингу активности в промышленных системах и сетях.

Ключевые слова: кибербезопасность, вредоносное ПО, кибератака, мониторинг активности, информационная безопасность.

В последнее время все больше внимания уделяется кибербезопасности промышленных сетей и систем. Внимание к этому вопросу вызвано усиливающимся присутствием современных информационных технологий в компонентах промышленных систем (ОС, сетевые протоколы и службы) со своими преимуществами и недостатками в области безопасности. Все чаще обнаруживаются уязвимости в ПО, а также ИТ-инфраструктуре промышленных систем и сетей. Проблема усугубляется отсутствием механизмов безопасности у большинства промышленных протоколов.

Не каждое промышленное предприятие и его системы могут стать объектами успешных целенаправленных атак, приводящих к физическому ущербу и остановке производства. Предприятие должно быть привлекательно атакующему, у которого должны быть как значительные финансовые и временные ресурсы, так и знания в области ТП, систем управления ими и хакерские навыки. Такие атаки под силу лишь крупным криминальным организациям либо целым государствам. В качестве примера подобной атаки можно привести известный многим инцидент с атакой вируса Stuxnet в 2010 г. на заводе по обогащению урана в Иране [1], приведшей к выходу центрифуг из строя. Другой пример — кибератака 2014 г. на системы управления металлургического завода в Германии [2], результатом которой стала остановка работы доменной печи. Подробности последнего инцидента пока не раскрываются, но он уже назван вторым после Stuxnet в Иране подтвержденным случаем кибератаки, приведшей к физическому ущербу.

Однако жертва кибератаки вовсе не обязательно всегда предполагается конечной целью этой атаки. Наиболее вероятные для большинства предприятий угрозы связаны с неумышленным воздействием, вызванным ошибочными или халатными действиями сотрудников в процессе эксплуатации промышленных систем и сетей и беспорядком в ИТ-инфраструктуре организации, что создает благоприятные условия для воздействия ВПО и получению локального и удаленного доступа к системам посторонних лиц, в частности, хакеров-любителей. В качестве примера инцидента в результате таких угроз можно назвать случай 2003 г., когда в объединенной энергосистеме США и Канады произошла авария, одной из причин которой стал компьютерный сбой в системе управления. В результате северо-восток США на несколько дней остался без электричества. Ущерб инцидента превысил 6 млрд. долл. США.

Для борьбы с умышленными и неумышленными угрозами необходим последовательный, комплексный и эшелонированный подход, включающий этапы обследования, проектирования, разработки организационных процедур и политик, проектирование, внедрение, сопровождение и эксплуатацию технических систем кибербезопасности. Выбор организационных и технических мер должен осуществляться на основе оценки рисков (в том числе и тех, которые вызваны применением самих мер защиты), с учетом критичности промышленных систем и принципа «не навреди».

Технические решения информационной безопасности (ИБ) условно можно разделить на две категории:

— управление доступом/предотвращение угроз. К их числу относятся промышленные и традиционные межсетевые экраны, системы управления запуском приложений, инструменты антивирусной защиты, шлюзы однонаправленной передачи данных и др.;

— мониторинг активности/обнаружение угроз (их состав ниже).

Зачастую критичность промышленных систем такова, что риски от применения решений для предотвращения киберугроз выше, чем риски от самих угроз (например, применение систем антивирусной защиты), так как механизмы защиты вмешиваются в процесс функционирования компонент систем и могут стать причиной проблем в их работе.

При наличии подобных опасений со стороны владельцев и операторов промышленных систем рекомендуется обратить внимание на решения из категории «Мониторинг активности/обнаружение угроз». Последние не вмешиваются в работу компонентов самих промышленных систем и сетей, позволяя наблюдать за их активностью, обнаруживать потенциальные проблемы и оперативно оповещать ответственные службы для принятия решений о ручном их устранении.

К категории «Мониторинг активности/обнаружение угроз» можно отнести следующие классы систем: обнаружения компьютерных атак; обнаружения сетевых аномалий; мониторинга событий информационной безопасности; пассивного анализа уязвимостей; анализа конфигураций оборудования; анализа правил доступа сетевого оборудования; мониторинга беспроводных сетей; контроля целостности данных и ПО; «приманки» атакующих (Honeypot).

Распишем подробнее назначение, особенности применения и общие функциональные возможности каждого класса данных систем подробнее.

Системы обнаружения компьютерных атак

Распространенные решения в офисных сетях, позволяющие обнаруживать атаки на информационные системы на основе сигнатурных методов, могут справиться с обнаружением атак на ИТ-инфраструктуру промышленных сетей.

Многие из традиционных решений поддерживают сигнатуры атак на промышленное ПО и протоколы.

Лучшая защита от кибермогики — невежество.

Ремейк по фразе Кеяог Олбран

Системы пассивно собирают сетевой трафик, анализируют его и при обнаружении подозрительных действий уведомляют администратора об атаке.

Системы обнаружения сетевых аномалий

Эти специализированные решения способны анализировать прикладные промышленные протоколы и обнаруживать аномальные данные в них (коды, уставки и др.) Они пассивно собирают и анализируют сетевой трафик, формируют профиль нормального поведения в сетях, обнаруживают аномалии и отклонения от него и оповещают администратора об обнаруженных аномалиях.

Аномальным поведением может быть изменение в составе сети, например, появление новых устройств, сетевых соединений (в том числе с Internet), увеличение объема и направления трафика. Учитывая статичность сетевого взаимодействия в промышленных сетях, данные решения можно легко адаптировать к отдельной промышленной сети и начать обнаруживать подозрительную активность.

Системы мониторинга событий информационной безопасности

Данные системы осуществляют сбор и анализ информации о событиях ИБ с оборудования промышленных сетей (обладающего возможностью регистрации событий) с целью обнаружения нарушений, например, попыток несанкционированного доступа, изменения конфигураций, создания новых пользователей или изменения их полномочий и др.

Системы получают информацию по стандартным протоколам передачи данных о событиях либо через штатные интерфейсы доступа с правами чтения журналов событий.

Системы пассивного анализа уязвимостей

Системы пассивно собирают и анализируют сетевой трафик на предмет наличия сигнатур уязвимостей и оповещают администратора о них. Решения способны выявить в трафике пароли, уязвимые версии прикладного и системного ПО и др., но при этом не производят активного сканирования сети, тем самым не создавая активного воздействия на промышленное оборудование. В результате для эффективной работы требуется значительное время на накопление информации пассивным способом.

Системы анализа конфигураций оборудования

Данные решения осуществляют сбор данных о конфигурации и состоянии компонент промышленных систем и сетей через штатные интерфейсы доступа без сетевого сканирования. Анализируют и обнаруживают потенциальные проблемы безопас-

ности в конфигурации систем и оповещают администратора. Использование данных решений рекомендуется для проверки оборудования в период простоев или «технологических окон».

Системы анализа правил доступа сетевого оборудования

Системы осуществляют регулярную проверку соответствия текущих правил доступа сетевых устройств заданной политике межсетевого экранирования, оповещают администратора об обнаруженных несоответствиях и проблемах, моделируют возможные сценарии атак, составляют актуальную карту сети, собирают данные для анализа с сетевого оборудования через штатные интерфейсы доступа с правами чтения.

Системы мониторинга беспроводных сетей

Эти системы осуществляют контроль радиоэфира (беспроводной сети Wi-Fi). При санкционированном наличии беспроводных сетей на промышленном объекте обнаруживают атаки и несанкционированные подключения к беспроводной сети. При запрете сетей обнаруживают несанкционированные попытки создания беспроводных сетей и подключений беспроводных устройств к промышленной сети или компьютерам.

Системы контроля целостность данных и ПО

Данные системы вычисляют контрольные суммы критических данных промышленных систем (конфигурации, файлы проектов, прошивки оборудования) и следят за их неизменностью. При обнаружении несанкционированных изменений в контролируемых данных оповещают администратора.

Системы «приманки» атакующих (Honeypot)

Системы класса Honeypot имитируют работающие компоненты промышленных систем и сетей для отвлечения внимания потенциальных злоумышленников и регистрации попыток атак. Данные решения разворачиваются с возможностью доступа взломщиков и позволяют оценить вероятность атаки на «боевые» промышленные системы.

В приведенных классах существуют как решения с открытым кодом (open source) [3], так и коммерческие продукты российского и зарубежного производства. На сегодняшний день число данных решений позволяет выбрать наиболее подходящее для каждого отдельного случая.

Заключение

Комплексное использование приведенных классов решений позволит обеспечить высокий уровень безопасности промышленных систем, сетей и производства в целом без риска сбоя производственных процессов. Это достигается за счет оперативного оповещения ответственных служб о происходящих процессах и изменениях в них, потенциальных угрозах в области безопасности как умышленного, так и неумышленного характера. Компания КРОК работает с предприятиями всех ключевых сегментов промышленности уже более 10 лет. Уникальный опыт экспертов КРОК в полной мере раскрывается при реализации комплексных решений по информационной безопасности в промышленных системах и сетях. Мониторинг вредоносной активности в промышленных системах — новое направление в деятельности компании, вызванное требованиями современных реалий.

Список литературы

1. Stuxnet и Иран: загадка модуля A26. http://www.atominfo.ru/news4/d0249.htm.
2. Rachael King Cyberattack on German Iron Plant Causes ‘Widespread Damage’. Wall Street Journal. http://blogs.wsj.com/digits/2014/12/18/cyberattack-on-german-iron-plant-causes-widespread-damage-report.
3. Kelly Jackson Higgins/ Using Free Tools To Detect Attacks On ICS/SCADA Networks. Dark Reading. http://www.darkreading.com/perimeter/using-free-tools-to-detect-attacks-on-ics-scada-networks/d/d-id/1318527.

Шипулин Антон Сергеевич – руководитель проектов по информационной безопасности,
Соболев Александр Юрьевич – руководитель группы АСУТП компании КРОК.
Контактный телефон (495) 974-2274.
E-mail: AnShipulin@croc.ru ASobolev@croc.ru

Обнаружена новая критическая уязвимость GHOST

Компания Qrator Labs, специализирующаяся на противодействии DDoS-атакам, и компания Wallarm, занимающаяся безопасностью Web-сайтов, сообщают об угрозе взлома серверов Linux в связи с публикацией информации о критической уязвимости GHOST. По своим масштабам новая проблема вполне может быть сопоставимой с ранее обнаруженными уязвимостями Heartbleed и Shellock.

Новая серьезная уязвимость GHOST позволяет злоумышленникам удаленно захватить контроль над серверами Linux. Информация об уязвимости опубликована специалистами американской компании Qualys.

Ошибка кроется в библиотеке GNU C Library (glibc), являющейся неотъемлемой частью Linux — ОС, которая не столь часто используется на домашних устройствах, но является оплотом для построения инфраструктуры большинства интернет-компаний.

Вероятно, учитывая серьезность проблемы, специалисты из Qualys не опубликовали в открытом доступе так называемый эксплоит — инструментарий, позволяющий использовать найденную ошибку для получения результата (в данном случае захвата сервера). Однако в лаборатории специалисты компании смогли получить доступ к командной строке сервера, отправив специально сформированное e-mail-сообщение, которое эксплуатирует уязвимость.

В отличие от нашумевшей в 2014 году уязвимости Heartbleed, найденной в библиотеке OpenSSL и позволяющей читать память сервера, сейчас злоумышленник имеет возможность реализовать атаку «Удаленное выполнение кода» (RCE) и сразу получить контроль над ОС.

Уязвимы системы Debian 7 (wheezy), Red Hat Enterprise Linux 6 & 7, CentOS 6 & 7, Ubuntu 12.04 — многие из них являются так называемыми дистрибутивами с длительной поддержкой (TLS) и потому повсеместно используются. Для защиты серверов необходимо установить патч (заплатку) на систему от своего Linux-вендора, которые были заранее уведомлены об уязвимости и сегодня должны выпустить обновления.

Ghost не такая суровая уязвимость, как Heartbleed, поскольку задевает только сервера. От тотального заражения пока спасает относительная сложность эксплуатации уязвимости. Ведь в сравнении с недавним нашумевшим Shellshock выполняются только бинарные инструкции, а не консольные команды. Для рабочей эксплуатации необходимо обойти несколько механизмов защиты, предусмотренных в ядре ОС Linux. Однако это только дает время защищающейся стороне.

Http://www.qrator.net www.wallarm.com