Как и зачем защищать АСУТП от вирусов и целевых атак

«Лаборатория Касперского»

Рассматривается история кибератак на промышленные объекты за последние годы. Приводится анализ существующей ситуации на промышленных предприятиях в области информационной безопасности. Предлагаются комплексные мероприятия, направленные на повышение кибербезопасности в промышленности.

Ключевые слова: кибератака, АСУТП, промышленная безопасность, критически важные объекты, ПЛК, SCADA-системы.

На протяжении последних десятилетий автоматизация промышленных предприятий и ТП неуклонно набирает обороты. Бизнес требует непрерывного повышения эффективности управления производством, растет степень информатизации и связности систем, промышленные объекты подключаются к корпоративным сетям и все чаще управляются удаленно через Internet. Но вместе с преимуществами новых технологий в промышленный мир пришли и новые угрозы, к которым он оказался не готов. Жизненный цикл работающих сейчас АСУТП измеряется десятилетиями, и многие из них разработаны без учета вопросов информационной безопасности.

Новая реальность

Нарушить стабильность функционирования производственной сети сегодня может не только отказ технологических узлов или ошибка оператора, но также ошибки в ПО, случайное заражение рабочих станций вредоносными программами или целенаправленные действия со стороны киберпреступников. А они, к слову, в последние годы проявляют все больший интерес к инфраструктурным и промышленным объектам.

Например, с 2010 г. и по настоящее время продолжается кампания кибершпионажа, известная как Crouching Yeti или Energetic Bear. Более 2800 предприятий, значительная часть которых связана с энергетикой и машиностроением, уже пострадали от действий организаторов этой операции — предположительно похищена конфиденциальная информация, составлявшая коммерческую тайну. Большая часть предприятий-жертв находится в США и Испании, однако в их числе есть и некоторые российские объекты.

Другой пример: 2 января 2014 г. системный администратор японской АЭС Monju обнаружил многократные удаленные подключения к одному из восьми компьютеров в центре управления реактором. Причиной этого инцидента стала установка одним из сотрудников обновления бесплатного видеоплеера GOM Media Player. В результате инцидента злоумышленниками была украдена часть информации, в том числе конфиденциальной.

Казалось бы, в этих условиях достаточно обеспечить сетевую изоляцию АСУТП. Но несостоятельность этой концепции продемонстрировал печально известный инцидент с Stuxnet: компьютерный червь размером в 500 Кб проник в изолированные сети через USB-накопитель и инфицированные SCADA-проекты, заражал ПЛК и физически вывел из строя центрифуги на ядерном объекте в Иране. Более того, потом этот червь «вырвался на свободу» и затронул ряд других критически важных объектов.

В конце 2014 г. также была зафиксирована атака на одно из металлургических предприятий в Германии. При помощи фишинга и методов социальной инженерии, в частности, посредством писем, содержавших вредоносные вложения, киберпреступники проникли во внутреннюю сеть предприятия и получили доступ к системам управления производством. Инцидент привел к тому, что сталеплавильную печь невозможно было остановить в штатном режиме, что привело к значительным убыткам. Это второй случай после Stuxnet, когда проникновение вредоносного ПО в АСУ ТП закончилось для предприятия реальным физическим ущербом.

Однако АСУТП критически важных объектов угрожают не только целенаправленные атаки со стороны кибертеррористов. Специфика этих систем такова, что они вполне могут пострадать и от самых обычных, «офисных» вирусов. Однако в промышленных сетях обычное вредоносное ПО способно причинить несравнимо больший вред, чем при заражении офисного или домашнего компьютера, например, заблокировать выполнение критически важных приложений, что приведет к сбою в работе оборудования. Например, червь Conficker сумел заразить производственную сеть, только потому, что в ней не было своевременно установлено обновление ОС Windows. Зловред посылал миллионы сетевых запросов, тем самым вызывая паралич производственной сети.

Даже средства автоматизированного проектирования могут использоваться для распространения вредоносного кода. Так, например, был зарегистрирован случай проникновения в производственную сеть вредоносной программы, написанной на языке AutoLisp (AutoCAD). Она внедрила вредоносный код в чертеж, открытие которого привело к массовому уничтожению данных.

«Болевые точки»

Основным показателем защищенности АСУТП является их способность поддерживать стабильность, непрерывность и корректное функционирование ТП, будь то выработка и передача электричества, очистка воды, управление производством или что-то другое,

независимо от внешних воздействий. Но в реальной жизни всегда существует масса факторов, из-за которых промышленные системы могут выйти из строя, особенно если им «помогают» киберпреступники.

Наибольшему риску АСУТП сегодня подвергаются в первую очередь из-за устаревшего ПО, оборудования и коммуникационных протоколов, изначально не предполагавших даже самой возможности существования киберугроз. Проблема усугубляется еще и тем, что для обновления этого ПО нужно преодолеть массу административных и технологических трудностей, и не каждая компания пойдет на это.

Немало вопросов вызывает также интеграция АСУТП в общую сеть предприятия. Обычно АСУТП функционируют в изолированной технологической сети (к которой имеют доступ сторонние, например сервисные компании, что также чревато проблемами). Но нередки случаи, когда эта изолированная сеть интегрировалась в общую корпоративную сеть, а то и подключалась к Internet.

Если говорить непосредственно о компонентах АСУТП, то наиболее уязвимыми элементами в них являются ПЛК, а также SCADA-системы. Первые «страдают» из-за жестко запрограммированных логина и пароля администратора, которые обычно устанавливаются производителем. Также контроллеры подвержены сетевым атакам вроде DoS/DDoS. Что касается SCADA, то как и обычные Windows приложения, они подвержены всем тем же уязвимостям, и это дает злоумышленникам «простор для творчества». Наиболее часто встречающиеся проблемы здесь — это переполнение буфера памяти, все тот же DoS, межсерверное выполнение сценариев, неправомерное исполнение кода и ряд других. На данный момент только в открытых источниках указаны около 650 уязвимостей в SCADA-системах, и эта цифра продолжает расти.

Итак, поскольку АСУТП находятся под угрозой не только проникновения простых вирусов, но также являются объектами целевых атак, то, следовательно, они должны иметь защиту от самых распространенных зловредов и уязвимостей в ПО, а также располагать специальными средствами и политиками безопасности для противодействия направленным атакам.

Текущие трудности

К сожалению, сегодня в России защиту промышленной инфраструктуры затрудняют как архитектурные, так и организационные и технологические факторы. Не способствует решению проблемы и сложная бюрократическая процедура внесения изменений в работу технологических узлов.

Как известно, российские АСУТП, однажды пройдя процедуру ввода в эксплуатацию, «опечатываются», и работают без обновлений многие годы. Строгие регламенты и нормативные акты не позволяют вносить в уже сертифицированную систему какие-либо изменения, даже в виде обновления ОС. Между тем, когда происходила приемка системы, проверка встроенных свойств безопасности, скорее всего, не проводилась. Да и само понятие безопасности, как правило, до сих пор сводится к ограничению доступа пользователя по паролю, который, нередко хранится в открытом виде в базе данных самого приложения.

Вычислительное оборудование АСУТП тоже, как правило, вводится в эксплуатацию с уже устаревшими прошивками (внутренним исполняемым микрокодом). Однако на сайте производителя всегда доступна свежая прошивка, в которой ряд известных проблем с информационной безопасностью уже закрыт, но их наличие никто не проверяет даже на этапе развертывания системы просто потому, что с администраторов этого никто не требует.

С другой стороны, автоматизацией ТП обычно занимаются не сами предприятия-операторы, а сторонние фирмы-подрядчики. Они в свою очередь заинтересованы в реализации именно функциональной составляющей, не придавая особого значения информационной безопасности, поскольку ее реализация — довольно трудозатратное занятие. Таким образом, предприятие получает только ту степень защиты от киберугроз, которая требуется действующим законодательством, ни о каких специальных настройках и проверках речь не идет. В конце концов, использующееся ПО «падает» или поддается несанкционированному управлению без особых проблем.

Помимо этого, существуют трудности с обнаружением киберугроз из-за отсутствия сетевого мониторинга, а также с необходимостью привлечения сторонних экспертов, в то время как предприятия не горят желанием сообщать об инцидентах. Наконец, проще переустановить, чем разбираться.

Защита возможна

Надежную защиту АСУТП можно обеспечить только при сотрудничестве государства, самих предприятий, проектных, научных организаций и производителей решений информационной безопасности. Необходимо выработать методологии и практики для построения защищенной инфраструктуры критически важных объектов, прийти к соглашению по единым критериям защищенности промышленной инфраструктуры, которые должны оперативно дорабатываться и адаптироваться под изменения ландшафта угроз, разработать методы стимулирования и юридической поддержки тех предприятий, которые уже применяют эффективные меры защиты, а также в обязательном порядке проводить образовательные программы для операторов АСУТП.

Государству также необходимо предпринимать и другие меры, например, организовывать регулярные кибертеррористические тренировки, разработать и внедрить единую политику в области обеспечения и контроля поставок оборудования и ПО для АСУТП, создать единые стандарты по приемке и сертификации АСУТП при вводе их в эксплуатацию, которые включали бы критерии информационной безопасности.

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.