Решение задач информационной безопасности в сфере АСУ ТП

Устаревшая производственная база промышленных предприятий, требующая модернизации или полной замены, необходимость повышения эффективности производства и снижения капитальных и операционных затрат приводят ко все более широкому использованию ИТ-технологий в сфере АСУ ТП и к интеграции АСУ ТП с системами управления предприятия. Появляются распределенные и локальные сети АСУ ТП, построенные с использованием стандартного телекоммуникационного оборудования IP/Ethernet, происходит их объединение с корпоративными сетями для обмена информацией, в системах автоматизации широко используются популярные ОС, БД, приложения и протоколы. Все эти процессы свидетельствуют о том, что границы между ИТ и АСУ ТП стираются и становятся все более открытыми. В свою очередь столь глубокое проникновение информационных технологий в область АСУ ТП делает задачу защиты информации, которая там обрабатывается, передается и хранится, критически важной. Любое нарушение доступности информации, ее целостности или конфиденциальности может привести к нарушению технологического процесса (ТП) с самыми негативными последствиями. Решение этих задач призвана обеспечить политика информационной безопасности (ИБ) предприятия

Очевидно, наиболее запоминающимся событием 2010 года, связанным с проблемами ИБ в АСУ ТП, стало обнаружение червя Stuxnet, созданного специально для атаки на сервера АСУ ТП и ПЛК и, по мнению ряда экспертов, ставившего своей целью блокирование работы центра ядерных исследований в иранском городе Натанз.

Первая публичная информация о Stuxnet появилась в июне 2010 года, хотя его ранние версии были созданы еще год назад. И хотя по отдельности решения, используемые в Stuxnet, встречались и раньше, их реализацию в одной вредоносной программе эксперты увидели впервые. Перечислим некоторых из них:

- использование для подписи зараженных драйверов цифровых сертификатов, украденных у двух производителей комплектующих для ПК;
- использование четырех неизвестных ранее уязвимостей в операционной системе Windows;
- возможность самообновления через Интернет и удаленного выполнения команд;
- возможность самообновления через ЛВС от других зараженных ПК;
- обход антивирусов и хостовых систем предотвращения вторжения;
- заражение приложений АСУ ТП SiemensWinCC/Step7;
- заражение сменных USB-накопителей;
- сложность и большой объем программного кода, на создание которого могло потребоваться около полугода работы команды из нескольких программистов с использованием тестового оборудования и специализированного ПО.

Самыми интересными особенностями Stuxnet являются возможность встраиваться в обмен данными между приложениями АСУ ТП и ПЛК, возможность получать доступ к передаваемой информации, модифицировать ее и скрывать свое присутствие. Благодаря способности перехвата команд червь внедрял свой код в ПЛК и, обнаружив подключение двух конкретных типов частотно-регулируемых электроприводов, начинал подавать команды на резкое изменение числа оборотов двигателей центрифуг.

Без всяких сомнений, Stuxnet является примером нового кибер-оружия, разработка которого вряд ли была бы возможна без помощи со стороны государственных спецслужб. И хотя повторение такого объема работы для менее значимых целей затруднительно, потенциальные злоумышленники смогут перенять новые подходы и технологии. А для специалистов в области ИБ Stuxnet фактически подтвердил опасения о незащищенности АСУ ТП и необходимости принятия в этой области срочных мер.

Существует как минимум три мифа, которые помог развеять Stuxnet.

Миф 1. ПО АСУ ТП обладает большей надежностью и меньшим количеством ошибок

На самом деле количество ошибок в ПО напрямую зависит лишь от его сложности. В проекте Open Source Hardening Project по результатам анализа нескольких сотен проектов была получена некоторая усредненная величина – 1 ошибка на 1000 строк кода. Представьте, сколько их может быть хотя бы в ядре ОС Linux, которое насчитывает более 11 миллионов строк.

По некоторым данным, в 2008-2010 годах было обнаружено не менее 17 уязвимостей в ПО компонентов АСУ ТП. Цифра не очень большая, но сюда надо добавить сотни и тысячи уязвимостей, унаследованных от ИТ-технологий вместе с теми техническими решениями, которые используются на предприятиях. Хотя они и не являются

направленными, тем не менее, представляют конкретную угрозу.

Миф 2. Сеть АСУ ТП полностью изолирована и состоит всего из нескольких компьютеров

Stuxnet, помимо распространения через ЛВС, также способен записывать свою копию на USB-накопители. В результате оператор АСУ ТП, заразив USB-накопитель, записывает на него какой-то безобидный файл, например обновление для сервера или текстовый файл, и переносит его на компьютер, установленный в сегменте АСУ ТП. Там при открытии диска происходит заражение, причем для этого пользователю ничего не нужно запускать. После успешной установки Stuxnet будет скрывать собственные файлы на USB-накопителе, а остальные компьютеры попробует заразить через сеть.

Миф 3. Использование средств безопасности на периметре сегмента АСУ ТП достаточно

Этот миф частично перекликается с мифом № 2 (в том, что любую периметральную защиту можно легко обойти, используя зараженный USB-накопитель). Поэтому сегмент АСУ ТП должен быть последним рубежом обороны, обеспечивая защиту на уровне хостов, и должен использовать возможности телекоммуникационной инфраструктуры для разделения трафика в целях ограничения дальнейшего распространения червя или вируса.

Миф 4. Исправления ПО, сделанные его производителем, помогут исправить уязвимость и остановить угрозу

Это утверждение верно лишь частично, так как практически всегда существует задержка между публичным анонсом об обнаружении уязвимости и появлением исправлений от производителя. Задержка может составлять от нескольких недель до года, как в случае с ПО для АСУ ТП, так и в отношении ИТ-продуктов. Это означает, что в течение всего этого времени АСУ ТП будет уязвимой! Примером может быть одна из уязвимостей в ОС Windows, используемая червем Stuxnet для эскалации привилегий, которая по прошествии нескольких месяцев по-прежнему остается неустраненной.

Когда дело доходит до внедрений, в большинстве случаев меры по ИБ начинаются и заканчиваются на границе между технологическим и корпоративным сегментами ЛВС. Но чтобы противодействовать современным угрозам в сфере АСУ ТП, недостаточно поставить межсетевой экран на границе и установить на серверах и АРМ'ах антивирус. Нужно применять технологии ИБ ниже, внутри АСУ ТП, на уровне серверов, ПЛК и интеллектуальных датчиков и исполнительных механизмов.

И тут мы сталкиваемся с другой проблемой, которая в большей степени лежит вовсе не в технической области. Разные цели, зоны ответственности, опыт и багаж знаний специалистов разных департаментов создают существенную разницу в восприятии задач ИБ. Например, если ИБ-специалисты считают своей главной задачей обеспечение защищенности вверенного им сегмента сети любой ценой, то для "асутэпэшников" самым важным является "доступность", то есть исключение какого-либо возможного негативного влияния на АСУ ТП, в том числе вызванного средствами обеспечения ИБ. Прямой, директивный подход к реализации мер ИБ может встретить вполне понятное противодействие с их стороны. В свою очередь, сотрудники департамента ИБ не стремятся разрабатывать и внедрять политики ИБ внутри сегментов АСУ ТП из-за нежелания брать на себя ответственность и разбираться в деталях работы систем автоматизации.

Существуют также проблемы на техническом уровне, которые не позволяют использовать стандартные подходы и продукты внутри АСУ ТП. Например, ПЛК, интеллектуальные датчики и исполнительные механизмы в большинстве случаев можно защитить только путем сегментации на уровне коммутаторов Industrial Ethernet и использования сетевых средств безопасности, таких как межсетевые экраны, сенсоры систем предотвращения вторжения (IPS). В соответствии с принципом "не навреди" IPS часто внедряется в сетях АСУ ТП в режиме мониторинга копии трафика, что фактически является шагом назад для ИБ-технологий.

Очевидно, что решать задачи ИБ в АСУ ТП можно только коллегиально, с привлечением специалистов департаментов ИТ, ИБ и АСУ ТП. Положительную роль здесь может сыграть организация рабочей группы, которая включала бы сотрудников названных департаментов и выполняла бы задачу по анализу текущей ситуации, разработке политик и мер обеспечения ИБ на основе анализа рисков. Результаты работы такой комиссии должны быть донесены до высшего руководства компании напрямую.

С чего следует начать при разработке мер обеспечения ИБ? Большим подспорьем для предприятий, которые стоят перед необходимостью внедрения ИБ в АСУ ТП, может стать использование Рекомендаций по безопасности Smart Grid (Guidelines for Smart Grid Cyber Security), разработанных под эгидой Национального Института Стандартов и Технологий (NIST).

В числе других стандартов можно назвать два принятых стандарта Международного Общества Автоматизации ISA (International Society of Automation) – ANSI/ISA-99.00.01-2007 и ANSI/ISA-99.02.01-2009 (также приняты как IEC/TS 62443-1-1 и IEC 62443-2-1), еще 12 стандартов находятся в стадии проекта или рассмотрения. В энергетическом секторе необходимо отметить стандарты NERC (North American Electric Reliability Corporation) с CIP-002-1 по CIP-009-2 и упомянутые рекомендации NIST в области защиты SmartGrid.

Огромное количество стандартов в области ИБ, применяемых при обеспечении безопасности информационных систем, также могут быть более чем полезны. Это и многочисленные стандарты RFC, ISO/IEC серии 27000, публикации NIST и другие стандарты и рекомендации.

Заслуживают внимания и тщательного анализа и рекомендации производителей. Одним из примеров таких практических рекомендаций может быть руководство по проектированию и внедрению конвергированной Ethernet

сети предприятия (Converged Plantwide Ethernet Design and Implementation Guide), разработанное компаниями Cisco и Rockwell Automation. Назначение этого документа – определение эталонных сетевых архитектур, ориентированных на применение на производственных предприятиях и облегчающих объединение промышленных и корпоративных сетей с учетом требований по ИБ. С документом можно ознакомиться по адресу http://www.cisco.com/en/US/docs/solutions/Verticals/CPwE/CPwE_DIG.html.

В России за обеспечение ИБ в ключевых системах информационной инфраструктуры (КСИИ), куда можно отнести и технологические сети, отвечает Федеральная служба по техническому и экспортному контролю (ФСТЭК). В 2007 году были приняты документы, которые описывают основные требования по обеспечению ИБ. Однако эти документы находятся под грифом ДСП и доступны только лицензиатам ФСТЭК. Кроме того, их правовой статус не определен, так как перечень КСИИ неизвестен.

При следовании перечисленным выше стандартам хотелось бы предостеречь от принятия любого из них "как есть", без какой-либо правки. Подобный подход может привести к получению чрезмерно подробного документа, который будет слабо применим к техническим, производственным, и организационным особенностям конкретной компании и, соответственно, никогда не будет исполняться.

С другой стороны, нужно понимать, что без конкретных мер на техническом уровне любой стандарт или политика ИБ так и останутся на бумаге, создавая ложное ощущение защищенности.

Очевидно также, что формальное следование требованиям стандартов не всегда сможет обеспечить защиту от угроз наподобие Stuxnet. Для борьбы с такими угрозами необходима многоуровневая защита, обеспечивающая противодействие как внешним, так и внутренним угрозам (рисунок). Этот подход предполагает несколько уровней защиты в различных сегментах сети АСУ ТП с используя политик и процедур, направленных на разные типы угроз. Например, меры защиты на сетевом уровне обеспечивают безопасность компонентов АСУ ТП, имеющих сетевое IP/Ethernet-подключение и передаваемые данные. При этом следует иметь в виду, что ни один уровень сам по себе не способен обеспечить полной защиты АСУ ТП.

Для реализации подхода многоуровневой защиты необходимо организовать процесс, который должен включать в себя:

- определение приоритетов (например, доступность, конфиденциальность, целостность);
- определение требований (например, необходимость удаленного доступа из корпоративной сети);
- определение ресурсов;
- определение потенциальных внутренних и внешних угроз и рисков;
- разработку архитектуры;
- разработку и внедрение политик ИБ, ориентированных на защиту АСУ ТП.

Проектирование и внедрение полноценной системы ИБ должно подчиняться основным целям АСУ ТП и рассматриваться как расширение задач системы автоматизации.

Эшелонированная защита включает в себя следующие уровни:

- уровень физической безопасности – ограничение физического доступа к панелям управления, диспетчерским комнатам и другим помещениям, устройствам, кабелям;
- уровень сетевой безопасности, который включает сетевую инфраструктуру, например межсетевые экраны со встроенными сенсорами систем предотвращения вторжения, и интегрированные в сетевое оборудование (коммутаторы и маршрутизаторы) средства безопасности;
- уровень безопасности рабочих станций и серверов, который включает в себя управление обновлениями ПО, антивирусное ПО, удаление неиспользуемых приложений, протоколов и сервисов;
- уровень безопасности приложений, обеспечивающий аутентификацию, авторизацию и аудит при доступе к приложениям;
- уровень безопасность устройств, осуществляющий контроль изменений и ограничение доступа.

Особое внимание необходимо уделять сетевому уровню, так как большое количество компонентов в АСУ ТП подключено к сетевой инфраструктуре IP/Ethernet и может не иметь возможности для установки средств обеспечения ИБ, таких как антивирусы или системы предотвращения вторжений на уровне хоста.

Система сетевой безопасности должна включать следующие компоненты:

- демилитаризованную зону (ДМЗ) – буферную зону обеспечивающую разделение сегментов корпоративной и промышленной сети, безопасный и защищенный обмен данными между ними, а также использование общих сервисов. При этом трафик не может проходить напрямую из корпоративной сети в сеть АСУ ТП и наоборот, информационный обмен возможен только через ДМЗ (более подробно концепция ДМЗ была рассмотрена в статье "Интеграция технологических и корпоративных сетей", REM № 6, 2007);
- защиту внешнего периметра АСУ ТП, включающую средства межсетевого экранирования с поддержкой сенсоров систем обнаружения вторжений;
- защиту внутреннего периметра, в которую входят листы контроля доступа (ACL) на сетевых устройствах, таких как коммутаторы и маршрутизаторы, возможно также использование межсетевых экранов и систем обнаружения вторжений в режиме мониторинга;
- защиту конечных устройств, назначение которой состоит в ограничении доступа, наложении запрета на несанкционированные подключения к ЛВС и контроль за изменениями;
- сегментирование, которое используется для изоляции сетевых устройств по ролям с применением технологий виртуализации, таких как виртуальные ЛВС (VLAN), VRF, частные VLAN (PVLAN);
- системы мониторинга сетевой активности, обеспечивающие сбор событий сетевого оборудования и устройств безопасности, анализ статистики Netflow для поиска аномалий;
- политику удаленного доступа, отвечающую за организацию удаленного доступа к компонентам АСУ ТП из корпоративной сети или удаленных площадок в соответствии с персональными правами доступа.

Использование функций ИБ на уровне сети позволит полностью реализовать принцип эшелонированной, многоуровневой защиты АСУ ТП от современным многовекторных угроз. Построение таких систем ИБ, глубоко интегрированных в АСУ ТП, требует принципиально нового уровня кооперации между подразделениями ИТ, ИБ и АСУ ТП, но только совместными усилиями можно обеспечить решение задач информационной безопасности на уровне автоматизированных систем управления технологическими процессами.

Андрей Гречин, системный инженер-консультант, компания Cisco