УДК 621.3

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ *SCADA*

Плешко Д.Ю.

Научный руководитель – Сапожникова А.Г.

SCADA (*Supervisory Control And Data Acquisition*) – программный пакет, предназначенный для разработки или обеспечения работы в реальном времени систем сбора, обработки, отображения и архивирования информации об объекте мониторинга или управления. *SCADA* может являться частью АСУ ТП, АСКУЭ, системы экологического мониторинга, научного эксперимента, автоматизации здания и т. д. *SCADA*-системы используются во всех отраслях хозяйства, где требуется обеспечивать операторский контроль за технологическими процессами в реальном времени. Данное программное обеспечение устанавливается на компьютеры и, для связи с объектом, использует драйверы ввода-вывода или *OPC*/*DDE* серверы. Программный код может быть, как написан на одном из языков программирования, так и сгенерирован в среде проектирования.

В основе большинства из ныне существующих *SCADA*-систем лежит платформа *Microsoft Windows*, так как подобного рода системы предлагают наиболее гибкие, полные и расширяемые решения в области *HMI*. Усиление позиций *Microsoft* на рынке ОС АСУ ТП влечёт соответствующую реакцию со стороны разработчиков *SCADA*-систем (например, Siemens) для множества различных платформ, которая заключается в приоритезации дальнейшего развития именно платформы *Windows NT*. Таким образом, основу глобального рынка программного обеспечения *SCADA*-систем на данный составляет ОС MS Windows NT, тогда как её предшественники, такие как *MS DOS*, стремительно вытесняются. Использованию *Windows* также способствует отлаженный механизм коммуникаций с драйверами оборудования различных производителей, определяющий универсальность ОС.

Первоначально АСУ ТП имели мало сходства с *IT*-системами. Различие заключалось в том, что АСУ ТП являлись изолированными системами, использовавшими свои собственные протоколы управления, специализированное оборудование и программное обеспечение. Сегодня относительно дешёвые и доступные устройства, использующие для связи протокол *IP*, вытесняют специализированное оборудование. Данный факт ведёт к увеличению вероятности возникновения уязвимостей и инцидентов в области информационной безопасности.

Уязвимости в АСУ ТП могут возникать в результате недостатков, неправильного или ненадлежащего технического обслуживания технических платформ, включая аппаратную часть, операционные системы и приложения, а также благодаря неполным, несоответствующим или попросту несуществующим руководящим документам и политикам в области ИБ. Данные уязвимости могут быть уменьшены благодаря различного рода средств контроля безопасности, таких как проведение обновлений ОС и приложений, контроль физического доступа, специализированное ПО в области информационной безопасности (например, антивирусное ПО).

Корпоративная политика безопасности может уменьшить число уязвимостей определяя обязательное использование парольной защиты или, например, регламентируя параметры обслуживания или требования в отношении подключения модемов к компонентам АСУ ТП. Факторы риска современных АСУ ТП (*SCADA*-систем) базируются на необходимости поддержки их конкурентоспособности на рынке ПО (расширяемость, адаптируемость и т. д.). Также на факторы риска *SCADA*-систем влияет опасность осуществления их аудитаи реализации необходимых изменений.

Таким образом, среди факторов риска современных *SCADA*-можно выделить следующие: внедрение стандартизованных протоколов и технологий со списком известных уязвимостей, связанность сети системы управления с другими сетями (например, сетью ИТ-системы), широкая доступность и распространение технической информации и документации о системах управления, высокие риски проведения аудита, высокие риски

внесения исправлений. Актуальные сценарии проведения современных атак на *SCADA*-системы включают атаку при помощи эксплойта, атаку злоумышленным служащим, а также управление посредством внедрения вируса.

Сетевая архитектура современных предприятий объединяет компоненты корпоративной сети и компоненты АСУ ТП, что обуславливает уязвимость *SCADA*-систем перед атаками с использованием эксплойтов. В данной схеме для корпоративной, внутренней и управляющей сети используются свои собственные межсетевые экраны. Однако, зачастую, на практике межсетевые экраны заменяются простыми маршрутизаторами (сетевыми коммутаторами), таблицы маршрутизации которых могут дополнительно быть неправильно настроены с точки зрения ИБ. В некоторых небезопасных случаях все три сети (корпоративная, внутренняя и управляющая) могут быть объединены воедино без использования каких-либо сетевых инструментов.

Одной из проблем практически всех АСУ ТП и *SCADA*-систем является невысокая защищённость от злонамеренных действий конечных пользователей – управляющего и обслуживающего персонала (например, инженеров, операторов, администраторов и т. д.). Под понятием «инсайдер» подразумевается сотрудник компании, имеющий непосредственный доступ к конфиденциальным данным, системе безопасности, управляющему, сетевому или производственному оборудованию. Негативные действия инсайдера могут иметь как случайный характер, вызванный ошибкой или невнимательностью персонала, так и преднамеренный, обусловленный сознательным желанием вывести из строя АСУ ТП предприятия или создать чрезвычайное происшествие.

Современные вирусы используют уязвимости ОС, позволяющие производить повышение уровня привилегий до уровня администратора. Они используют специальные методы загрузки ПО, позволяющие не быть замеченными антивирусами, программами анализа поведения и программами для предотвращения вторжений.

Вирусное ПО может самостоятельно осуществлять вредоносную деятельность или создавать скрытый канал для последующей атаки системы злоумышленником. Первым шагом злоумышленника при атаке эксплойтом, как правило, является взлом и взятие под контроль некоторого элемента корпоративной сети, с которого впоследствии производится последующая атака элемента внутренней сети.

Примером может служить атака через сервер системы системного анализа и разработки программ (*SAP*) к серверу логирования, расположенному во внутренней сети. Взлом может быть осуществлён во время приёма/передачи данных системных журналов, дневной статистики, данных о текущих заказах, данных о текущем спросе и др. Имея в распоряжении сервер логирования (как правило, устройство класса *Windows Server*), злоумышленник может вывести его из строя, скрыть предыдущие атаки, получить доступ к чтению и редактированию конфиденциальных данных.

Следующим шагом атаки злоумышленника является попытка взлома одного из элементов управляющей сети (*SCADA*-системы), выполняемая с использованием ранее захваченного элемента внутренней сети. Атакующий продвигается от сервера логирования к станции HMI, расположенной внутри управляющей сети. Проникновение может быть осуществлено во время обмена данными системных журналов и системной статистики, а также посредством протокола *OPC* и сервисов домена (*domain services*). Захват станции *HMI* (как правило, устройство класса *Windows Workstation*) позволяет злоумышленнику управлять настройками, манипулировать данными о текущем технологическом процессе в целях обмана сотрудников. Необходимо отметить, что для создания мнимой картины функционирования технологического процесса необходим захват и синхронизированное управление всех станций *HMI*, что предполагает наличие межпрограммного взаимодействия.

Далее атака может идти в направлении сервера приложений, обслуживающего управляющие рабочие станции, посредством информационного обмена в рамках чтения/записи текущих параметров процесса и настроек, аварийных оповещений, диагностики управляющей шины. Управление сервером приложений (как правило,

устройством класса *Windows Server*) позволяет осуществлять фальсификацию данных о технологическом процессе для вышестоящих компонентов (например, сервера логирования), нарушать синхронизацию отдельных компонентов *SCADA*-системы или продолжить атаку в направлении управляющих рабочих станций или *PLC*. Захват управляющей рабочей станции (как правило, устройства класса *Windows Server* или *Windows Workstation*) позволяет злоумышленнику получить доступ к PLC.

Доступность *PLC* позволяет управлять его работой, просматривать, модифицировать и обновлять ПО для *PLC*.

Наиболее вероятный сценарий запланированной атаки инсайдером на АСУ ТП включает в себя несколько этапов. На первом этапе происходит создание дополнительного контура управления системой для перехвата управления и вызова аварийной ситуации. Как правило, подобные действия совершаются от имени подставного пользовательского (операторского) аккаунта в целях сокрытия следов действий инсайдера. После проведения атаки управляющий контур самоуничтожается, стирая максимально возможно количество информации в системных журналах. Выполнение данных действий может включать необходимость изменения ПО контроллеров (например, контроллера ПАЗ), что может быть осуществлено при помощи программного скрипта, выполняющего записанные ранее действия.

На втором этапе ключевые элементы АСУ ТП заражаются вредоносным ПО, позволяющим в нужный момент вывести оборудование из строя или нарушить работоспособность компьютера, имитирую атаку устройства злоумышленником. Дальнейшие действия инсайдера могут развиваться по следующей схеме. В запланированное сотрудником-инсайдером время начинается имитация атаки компьютеров АСУ ТП злоумышленниками.

Нормальная работа станций управления нарушается, сотрудники предприятия оказываются в замешательстве. Критически важное управляющее оборудование самостоятельно отключается, аварийные блокировки не срабатывают, производственное оборудование остаётся без управления. Выполнение технологического процесса нарушается, возникает существенный риск создания ЧП. Во время процедуры расследования подобного инцидента будет выявлено заражение станций вредоносным ПО, отмечены действия операторов по созданию аварийной ситуации, а также выявлен отказ системы противоаварийной защиты.

Таким образом, вина в произошедшем событии ложится на плечи неизвестного злоумышленника, заразившего систему вирусом и атаковавшего её. Злоумышленник-инсайдер остаётся вне подозрений.

Для примера атаки вирусом-червём рассмотрим классического представителя данной категории вирусов – *Stuxnet*. В качестве первого из аргументов в пользу его сложности необходимо отметить факт того, что вирус способен распространяться тремя совершенно разными путями, а именно:

– посредством инфицированных отчуждаемых носителей данных (например, *USB*-флеш-накопитель);

– посредством трафика внутри локальной сети;

– посредством инфицированных файлов проекта *Siemens*.

Вирус инфицирует компьютеры посредством *USB*-флеш-накопителей (даже в случае выключенного автозапуска) путём ранее неизвестной уязвимости (*MS*10-046), связанной с ярлыками (файлами с расширением **.lnk*). Версии *Stuxnet*, выпущенные до марта 2010, распространялись при помощи *USB*-флеш-накопителей путём уязвимости, связанной с автозапуском, нежели с расширением **.lnk*. Вирус распространяется по локальной сети на компьютеры с наличием сетевых ресурсов в общем доступе путем регистрации всех учетных записей пользователей компьютера и домена. Затем программа пытается использовать все доступные сетевые ресурсы для того, чтобы скопировать и выполнить себя на удалённом ресурсе, тем самым заражая удалённый компьютер.

Вирус распространяется по локальной сети, предоставляя сервис печати с помощью уязвимости нулевого дня в *Windows Print Spooler* (MS10-061). Вирус распространяется по локальной сети посредством уязвимости *MS*08-067 *Windows Server Service Vulnerability* (*MS*08-067). Вирус инфицирует компьютеры, использующие базу данных *Siemens WinCC*, с помощью внутренних неизменяемых системных паролей, подключаясь к *SQL*-серверу в целях передачи и исполнения копии вируса. Вирус распространяется, копируя себя в любые найденные файлы проектов *Siemens STEP* 7 (файлы с расширением **.S7P*, **.MCP* и **.TMP*), а затем исполняясь автоматически при открытии проекта.

Литература

1. Матвейкин, В.Г. Применение SCADA-систем при автоматизации технологических процессов / В.Г. Матвейкин. – М. : Машиностроение, 2000. – 272 с.

2. Чичкарёв, Е.А. Системный анализ сложных систем управления / Е.А. Чичкарёв. – Пермь : ПГТУ, 2005. – 59 с.