УДК 004.056

В.С. Аввакумова

АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РАМКАХ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА ПРОЕКТНОЙ ОРГАНИЗАЦИИ

Аввакумова Валерия Сергеевна, *студентка 3-го курса специальности «Прикладная информатика в экономике» факультета информационных систем и технологий УлГТУ. [e-mail: val-avvakumova@yandex.ru].*

Аннотация

В данной статье рассматриваются основные проблемы информационной безопасности автоматизированных систем управления технологическим процессом крупных предприятий (в том числе, проектных организаций), описываются аспекты информационной безопасности автоматизированных систем управления технологическим процессом, а также опровергаются некоторые мифы о состоянии и степени защищенности автоматизированных систем управления технологическим процессом.

Ключевые слова: автоматизированная система управления технологическим процессом, информационная безопасность, инсайдеры, вирусы, Stuxnet.

Введение

Сегодня промышленные системы представляют собой сложный комплекс, состоящий из персональных и панельных компьютеров, программируемых логических контроллеров (PLC), активного и пассивного оборудования, поэтому, как и любые другие программно-технические продукты, данные системы имеют множество проблем с безопасностью. Например, кроме промышленных протоколов также используются стандартные протоколы (TCP/IP, IPX, NWLink, NetBEUI и др.) и распространенное программное обеспечение (SCADA-системы, системы автоматизированного проектирования, системы контроля и управления доступом). Кроме того, на многих предприятиях вводится система удаленной диспетчеризации, позволяющая проникнуть в SCADA-систему, которая является одной из основных составляющих автоматизированной системы управления (АСУ) технологическим процессом (ТП) и обеспечивает операторский контроль за ТП в реальном времени, через веб-интерфейс, доступный в сети Интернет, и нередко с паролями, установленными по умолчанию.

Специалистам в области информационной безопасности необходимо понимать, что SCADA-системы уязвимы, как и любые другие системы. Они также могут стать целью злоумышленников, однако риски при этом гораздо более высоки, вплоть до нарушения работоспособности системы и остановки производства.

Требуется разработать правильный подход к обеспечению безопасности АСУ ТП, так как основной проблемой в данном случае является не защита конфиден-

циальных данных, а обеспечение непрерывности производственного процесса. Основной целью злоумышленников является вывод из строя датчиков и приборов для остановки работы производства, что может быть на руку потенциальным конкурентам.

Инсайдерские атаки

Инсайдер – это человек, который имеет доступ к информации «для внутреннего пользования» различной степени секретности. Любое предприятие владеет информацией, доступ к которой есть лишь у ограниченного круга лиц. К этой информации относятся, к примеру, финансовые отчеты или технологические разработки. Еще Фрэнсис Бэкон отмечал, что знания являются силой, а в век информационных технологий это утверждение как никогда актуально, потому что утечка информации может подорвать деятельность любой организации. Сам термин «инсайдер» не несет в себе отрицательной нагрузки, однако в современных экономических реалиях использование внутренней информации, как правило, практически всегда связано с личной корыстью, именно поэтому на многих предприятиях уже внедрены соответствующие меры предосторожности, к которым относятся строгие системы контроля – различные регламенты, правила и инструкции для сотрудников предприятия. На большинстве контроллеров устанавливается пароль для предотвращения их несанкционированного перепрограммирования, мониторингом системы обычно занимаются несколько человек. Таким образом, у лиц, ответственных за обеспечение информационной безопасности на предприятии, есть возможность заранее отследить негативные изменения в системе, внесенные инсайдером.

Компьютерные вирусы

Компьютерный вирус – вид вредоносного программного обеспечения, способный создавать копии самого себя и внедряться в код других программ, системные области памяти, загрузочные секторы, а также распространять свои копии по каналам связи с целью нарушения работы программно-аппаратных комплексов, удаления файлов, приведения в негодность структур размещения данных, блокирования работы пользователей и выведения из строя аппаратных комплексов компьютера. Опасность вирусов усугубляется теми фактами, что либо не устанавливаются антивирусные программы на автоматизированные рабочие места (АРМ), либо не обновляются их антивирусные базы. Обновления – это ахиллесова пята защиты информации АСУ ТП. Зачастую сервер перестает отвечать на запросы клиентов из-за неправильно установленных обновлений. На устранение данной проблемы уходит достаточно много времени, и если в случае блокирования новостного сайта или интернет-магазина восстановление сервера после такого сбоя не влечет серьезных последствий, то в случае аварийной остановки центрального сервера АСУ ТП даже на короткий промежуток времени может понадобиться полный перезапуск производственной линейки, что приведет к существенным материальным затратам.

Ошибочно принято считать, что если технологическая сеть ни с чем не соединена, то и компьютерные вирусы в этой изолированной среде появиться никак не могут. Однако всегда нужно иметь в виду различные носители информации, например, флэш-накопители, которые могут послужить причиной заражения локальной сети всего предприятия.

Однако считается, что вирусы в данной ситуации не так страшны, потому что вирус в любом случае не сможет отправить информацию через Интернет, так как сеть является изолированной. Трояны так же бесполезны без доступа в Интернет. Возможно, система будет работать медленнее, но это не критично. Чтобы повлиять на систему, автономному вирусу придется решить ряд серьезных проблем, среди которых возможность использовать малоизвестные нестандартные протоколы, которые зачастую привязаны к конкретному производителю. Кроме того, большинство технологических систем чрезвычайно уникально, поэтому на них сложно повлиять автоматическими методами, что приводит к следующему выводу: в данной ситуации вирус должен быть очень высокой сложности и должен быть написан под определенную систему, поэтому вероятность подобной атаки близка к нулю.

Может показаться, что информационная безопасность АСУ ТП на данный момент находится на вполне приемлемом уровне, но данное впечатление глубоко ошибочно. Как уже говорилось, АСУ ТП перестала быть некой отдельной сверхспецифичной информационной системой, которая находится в абсолютной изоляции. Сейчас в АСУ ТП используются в основном стандартные общедоступные технологии и программное обеспечение. Построены данные системы также в основном по принципу иерархии, и все ее элементы сильно взаимосвязаны, а сама она взаимодействует с другими информационными системами [1].

Для обеспечения информационной безопасности АСУ ТП нужно обезопасить каждый из уровней иерархии, потому что всегда необходимо помнить, что безопасность всей системы определяется ее слабейшим элементом. В свою очередь, АСУ ТП состоит из нескольких элементов, среди которых различные технологические устройства, сетевое оборудование, приложения, операционные системы (ОС) хостов и серверов и их сетевая взаимосвязь. Таким образом, взлом одного из элементов данной системы неизбежно приведет к компрометации всей системы.

Допущения при организации информационной безопасности предприятия

Специалисты в области информационной безопасности принимают решения, основываясь на определенных допущениях.

Допущение 1. Промышленные системы не подвержены угрозам, потому что используют специфические технологии.

Возможно, в какой-то переходный момент это и было так. Использовались специальные промышленные протоколы, форматы. Производители применяли специфические конфиденциальные разработки для взаимодействия с оборудованием и на АРМ.

Теперь же все производители переходят на общедоступные стандартные технологии:

Сетевые – Ethernet, TCP/IP.

ОС – Windows, nix-системы (*BSD, Linux, QNX).

Службы каталогов – MS ActiveDirectory, Novell eDirectory, OpenLDAP.

Прикладное программное обеспечение – веб-серверы (IIS, Apache), СУБД (Access, MS SQL server, Oracle DB).

Технологии – Java, .NET, XML, HTTP, SOAP, SQL и т. д.

Последствия, которые влечет за собой применение этих технологий, достаточно серьезные, так как промышленные системы вместе со всеми положительными аспектами использования общедоступных технологий унаследовали и все их проблемы. Уязвимости данных технологий также широко известны. Хотя эксплуатация уязвимостей в промышленной среде и имеет свою специфику, но возможна и почти не отличается от эксплуатации в корпоративной сети. Существует множество автоматизированных программ, позволяющих эксплуатировать уязвимости системы всего за несколько шагов и получить над ней контроль. Причем в функционал данных систем уже входят всевозможные средства для атаки на распространенные промышленные контроллеры и SCADA. Таким образом, даже начинающий хакер может подключиться к сети АСУ ТП и получить над ней контроль.

Допущение 2. Промышленные системы не подвержены угрозам, потому что они изолированы.

В современных реалиях данное утверждение ложно, так как зачастую промышленные локальные сети являются распределенными и полностью ограничить физические подключения иногда невозможно. Локальные распределенные компьютерные сети – это сети, в которых компьютеры установлены в разных зданиях, расположенных на значительном удалении друг от друга. В этих случаях часто используются беспроводные технологии доступа: радиоканал (Radio), инфракрасный диапазон (англ. IR: InfraRed, инфракрасный), ультразвуковой диапазон (англ. SS: SuperSonic, ультразвуковой).

Существует необходимость подключения АСУ ТП к какому-либо серверу в корпоративной сети для предоставления менеджерам актуальной информации о производстве. Кроме того, иногда к промышленной сети организован удаленный доступ для дистанционного обслуживания, а так как корпоративные и технологические сети часто находятся на расстоянии, то используются защищенные, но проходящие через Интернет каналы, такие как виртуальные частные сети (VPN), позволяющие обеспечить одно или несколько сетевых соединений поверх другой сети (например, Интернет).

Получается, что сети имеют «входы» и фактически не так уж и изолированы. Основным разделителем, делающим данную среду изолированной, остается межсетевой экран (файрволл).

Межсетевой экран предназначен для защиты от хакерских атак, но, увы, существуют разнообразные технологии, позволяющие либо обходить межсетевые экраны, либо взламывать их. Злоумышленники могут подменять свои IP-адреса в корпоративных сетях, могут внедряться в соединения по сети, прослушивать и модифицировать данные, передающиеся по сети.

Таким образом, злоумышленники могут передавать команды в промышленную сеть и получать обратно результат через DNS-запросы (данный протокол чаще

всего не фильтруется файрволлами), могут использовать IPv6 (новая версия протокола IP, призванная решить проблемы, с которыми столкнулась предыдущая версия (IPv4) при ее использовании в Интернете, за счет использования длины адреса 128 бит вместо 32) для инкапсуляции в него IPv4 (некоторые файрволлы не умеют корректно обрабатывать IPv6-трафик и пропускают его).

При конфигурировании межсетевых экранов требуется учитывать массу факторов и максимально ограничивать доступ в промышленную сеть извне. Кроме того, злоумышленники могут взломать сам межсетевой экран и настроить необходимые им правила фильтрации, и даже если межсетевой экран успешно выполняет свои функции, пользователи / интеграторы АСУ ТП, в нарушение политик и регламентов, подключают к своим компьютерам всевозможные устройства для выхода в Интернет (например, GSM-модемы). Таким образом, необходимо учитывать вероятность того, что у злоумышленников есть возможность попасть в промышленную сеть [2].

Защита информации АСУ ТП. Stuxnet

Stuxnet – высокотехнологичное вредоносное программное обеспечение. Данный червь использует четыре ранее неизвестных уязвимости ОС семейства Microsoft Windows (XP, CE, Vista, 7, Windows Server 2003, 2008 и 2008R2, как 32-разрядную, так и 64-разрядную).

Уязвимости, которые эксплуатирует вирус, позволяют ему заражать компьютеры как по сети, так и через USB, даже при полностью отключенном автозапуске для всех носителей. Кроме того, вирус устанавливает в ОС специальные драйверы, что значительно затрудняет его обнаружение.

После внедрения в систему вредоносное программное обеспечение осуществляет поиск SCADA-системы фирмы Siemens, причем им атакуются только системы SCADA WinCC/PCS7.

Когда червь определяет, что оказался на машине с WinCC, он заходит в систему, используя стандартные учетные записи. Стоит отметить, что Siemens официально не рекомендует менять стандартные пароли на своих системах, так как это может повлиять на работоспособность системы, и использование червем стандартных паролей гарантирует почти 100 %-ную вероятность успешных авторизаций. Затем Stuxnet сканирует локальную сеть предприятия на наличие других подобных АРМ для заражения.

Также Stuxnet имеет возможность перепрограммировать PLC Simatic фирмы Siemens. На данных контроллерах построен технологический процесс на огромном количестве объектов, в том числе стратегических и военных. Например, атомная станция в Иране (Бушер), которую многие эксперты считают целью этого кибероружия (именно так охарактеризовал червя Евгений Касперский, российский программист, один из ведущих мировых специалистов в сфере информационной безопасности), конечно, не использует контроллеры Siemens для управления самим реактором, но использует их в большом количестве для управления вспомогательным оборудованием. Этого вполне достаточно, чтобы червь мог парализовать работу атомной станции.

Процесс поражения системы происходит следующим образом. Троян не записывает в контроллеры некорректную информацию и не выводит их из строя. Находясь в системе достаточно долгое время, Stuxnet накапливает информацию о ТП: режимах работы оборудования, показаниях датчиков температуры, давления, частоте работы двигателей, и в какой-то момент троян их меняет.

Пример: допустим, аварийные показания температуры охлаждающей жидкости в установке равны 75 °С. Нормальная температура работы – 40–45 °С. Изменение значения аварийной остановки в контроллере с 75 до 40 °С приведет к тому, что контроллер будет инициировать остановку агрегата из-за аварии в тот момент, когда он достигает своей нормальной рабочей температуры, или же показание меняется в другую сторону, и агрегат продолжает работать после перегрева до полного самоуничтожения. При этом на экране SCADA-системы оператор продолжает видеть нормальные значения, которые троян подменяет в реальном времени. И если речь идет, например, об установке, перекачивающей газ, то изменение параметров показаний может привести к исчезновению с карты всей компрессорной станции вместе с прилегающими к ней районами.

В одной из версий червя, детально изученной специалистами компании Symantec, известной в мире компанией по производству программного обеспечения в области информационной безопасности и антивирусов найден функционал управления частотно-регулируемыми приводами (ЧРП) электродвигателей, причем двух конкретных производителей, при работе на определенной частоте. Это очень серьезная проблема, так как в России Stuxnet может, например, вывести из строя сверхскоростные поезда «Сапсан», которые полностью построены на системах Simatic и используют в работе большое количество тех самых ЧРП. И не только «Сапсан», а огромное количество самых разных систем.

Кроме того, примерно через год после Stuxnet появился аналогичный промышленный вирус под названием Duqu, который включает функционал для удаленного управления.

При всем разрушительном потенциале Stuxnet – вирус высокотехнологичный, а значит, по утверждениям антивирусных компаний, создавала его группа высококвалифицированных специалистов, и, скорее всего, на его разработку было потрачено немало денег.

Куда опаснее могут быть последствия от хакерских атак. Ведь человек, взламывая систему, сможет подстроиться под ее специфику, обойти присутствующие механизмы безопасности, атаковать более тихими методами и более конкретные элементы системы. К тому же хакер сможет более осознанно повлиять на технологический процесс, что делает такую атаку гораздо опаснее. Для успешной хакерской атаки при нынешнем уровне безопасности промышленных сетей чаще всего требуется только сетевой доступ в промышленную сеть.

Связано это во многом с тем, что в АСУ ТП очень редко обновляется прикладное программное обеспечение, ОС и системы управления базой данных. Все это имеет множество общеизвестных уязвимостей. И, как уже было сказано, существуют специальные программы, позволяющие эксплуатировать данные уязвимости, что приводит к удаленному проникновению в ОС и повышению привилегий.

Заключение

АСУ ТП является сверхкритичным объектом: даже непродолжительная остановка системы может привести к очень крупным финансовым потерям. Однако внимание к информационной безопасности данного класса систем находится на низком уровне.

Производители программного обеспечения считают, что безопасность – это проблема их клиентов. А у клиентов нет понимания масштаба этой проблемы, потому что в штате зачастую нет специалиста по информационной безопасности, который мог бы проанализировать все риски.

Из-за того что производители АСУ ТП перекладывают вопросы безопасности на плечи клиентов, большая часть АСУ ТП, как известно, имеет многочисленные критичные уязвимости, а построить на основе небезопасных элементов защищенную АСУ ТП очень непросто.

В том случае, если промышленная сеть хотя бы в одном месте подсоединена к другим сетям, если есть возможность удаленного доступа или применяются беспроводные технологии, то вероятность хакерской атаки велика. Если же нет – остаются эффективные компьютерные вирусы, которые могут повлиять на ТП [3].

Таким образом, несмотря на всю изолированность и уникальность каждой промышленной сети, существуют компьютерные вирусы, которые могут влиять на ТП.

До сих пор не получено ответа на вопрос «Как часто в реальности происходят проникновения в промышленные сети?». Достоверную информацию найти очень сложно, так как раскрытие сведений о том, что компания была взломана, может сильно подорвать ее репутацию. Кроме того, многие инциденты происходят незаметно: начались неполадки на производстве, осуществили перезапуск системы. Главная цель – как можно скорее запустить все заново, ведь простой производства влечет большие финансовые затраты, и нет возможности проводить расследование и разбираться в причинах: для этого нужно изымать технику и анализировать ее. Промышленный шпионаж предполагает, что факт его присутствия не должен быть обнаружен.

Неисправности в работе АСУ ТП могут повлечь за собой не только нарушение (или полный отказ) ТП и экономические убытки, но и другие катастрофические последствия, связанные с безопасностью людей и серьезным ущербом для окружающей среды. В связи с этим важно понимать, что обеспечение безопасности АСУ ТП (как физической, так и информационной) – приоритетная задача любого производства.

СПИСОК ЛИТЕРАТУРЫ

1. Норенков И.П. Основы автоматизированного проектирования. – М. : Издательство МГТУ им. Н.Э. Баумана, 2009. – 430 с.

2. Шишов О.В. Современные технологии промышленной автоматизации: учебник для вузов. – Саранск: Издательство МГУ им. Н.П. Огарева, 2007. – 376 с.

3. Проектирование систем автоматизации технологических процессов / А.С. Клюев [и др.]. – М. : Энергоатомиздат, 1990.