Риски промышленных систем

написано Александр Астахов | 10 июня, 2023

Автоматизированные системы управления (АСУ и АСУТП) в настоящее время используются в большинстве отраслей промышленности, в нефте- и газодобыче, на электростанциях и железных дорогах, на пивоварнях и лыжных курортах. В мире эксплуатируются миллионы промышленных систем, стоимость каждой из которых измеряется десятками тысяч и миллионами долларов. Степень зависимости критической инфраструктуры государства от таких систем неуклонно возрастает, и вопросы обеспечения их информационной безопасности приобретают первостепенное значение.

В отличие от других видов автоматизированных информационных систем, промышленные системы, особенно те, которые используются для управления критической инфраструктурой, имеют ряд особенностей, обусловленных их особым назначением, условиями эксплуатации, спецификой обрабатываемой в них информации и требованиями, предъявляемыми к функционированию. Главной же особенностью этих систем является то, что с их помощью в автоматическом, либо полуавтоматическом, режиме в реальном времени осуществляется управление физическими процессами и системами, от которых непосредственным образом зависит наша безопасность и жизнедеятельность: электричество, связь, транспорт, финансы, системы жизнеобеспечения, атомное и химическое производство и т.п.

Промышленные системы эволюционировали от экзотических программных и аппаратных средств в 70-х годах прошлого века до вполне современных систем, в которых используются стандартные IBM-совместимые ПК, операционные системы семейства Microsoft Windows, сетевые протоколы TCP/IP, Web-браузеры и Интернет-подключения. Благодаря такой стандартизации, а также распространенной практике подключения промышленных систем к локальным сетям (ЛВС) предприятий и использованию в них технологий беспроводного доступа, множество угроз в отношении

этих систем значительно расширилось.

Угрозы в отношении промышленных систем, в зависимости от того, кто выступает в качестве «агента угрозы», можно разделить на следующие основные группы:

1. *Вредоносное ПО.* Промышленные системы, так же как и любые другие ИТ системы, потенциально подвержены угрозам со стороны компьютерных вирусов, сетевых червей, троянских программ и программ шпионов.
2. *Инсайдеры.* Недовольные внутренние пользователи, хорошо знающие систему изнутри, как показывает практика, представляют собой одну из основных угроз. Инсайдер может умышленно повредить оборудование или программное обеспечение. Администраторы и инженеры, обслуживающие систему, могут также неумышленно нанести вред ее функционированию, допустив ошибку в настройках системы или нарушение определенных правил безопасности.
3. *Хакеры.* Аутсайдеры могут быть заинтересованы в исследовании возможности получения доступа и контроля над системой, мониторинге трафика и реализации атак на отказ в обслуживании.
4. *Террористы.* Это наиболее серьезная угроза, создающая основные различия между системами, относящимися к критической инфраструктуре и обычными ИТ системами. Террористы заинтересованы в том, чтобы вывести систему из строя, нарушить процессы мониторинга и управления либо получить контроль над системой и нанести как можно больший вред.

В Афганистане были получены доказательства того, что террористическая организация Аль Кайда проявляет повышенный интерес к промышленным системам. Можно также предположить, что среди членов Аль Кайды имеются квалифицированные специалисты (например, арестованный Халид Шейх Мухамед, их главный

распорядитель, обучался на инженера в Северной Каролине, а позже работал в водной промышленности на Среднем Востоке).

По сообщению газеты Вашингтон Пост в Афганистане был найден ноутбук, принадлежащий людям Аль Кайды. Было установлено, что с этого ноутбука многократно посещался французский Интернет-сайт, принадлежащий некому Анонимному Обществу (Societe Anonyme). На этом сайте размещено «Руководство по саботажу», содержащее такие разделы, как «планирование нападения», «методы ухода от наблюдения» и т.п. Имеются также свидетельства, подтверждающие, что с компьютеров, принадлежащих террористам, осуществлялся поиск в Интернет программных средств для взлома сетей.

Следователи из США зафиксировали посещения людьми из Аль Кайды сайтов, предоставляющих ПО и инструкции по программированию цифровых переключателей, используемых в энергетических, водных, транспортных и коммуникационных сетях. На некоторых допросах, люди Аль Кайды в общих словах выражали намерения использовать эти инструменты.

Еще совсем недавно в качестве основных источников угроз для безопасности киберпространства США рассматривались Китай, Россия и другие страны. Считалось, что люди Аль Кайды «менее квалифицированы в области использования сетевых технологий», чем многие рядовые хакеры, и поэтому не представляют здесь серьезной угрозы. В связи с указанными фактами разведслужбы США изменили свое мнение относительно возможности использования киберпространства террористами.

К счастью, в критичных отраслях, преимущественно использующих промышленные системы, отсутствуют два основных мотивирующих фактора для киберпреступности. Это экономические стимулы, к которым относятся кредитные карты и электронные счета, лежащие в основе многих компьютерных преступлений, и коммерческие тайны, являющиеся основной целью промышленного шпионажа.

Существует большое количество зарегистрированных инцидентов безопасности, затрагивающих системы управления критической инфраструктурой. В ряде научно-исследовательских институтов, ФБР и других организациях ведется соответствующая статистика. Согласно этой статистике в США на промышленные системы осуществляется не менее 100 кибератак в год и существует тенденция к непрерывному увеличению их числа. Зафиксированы все категории кибератак, за исключением кибертерроризма.

Справедливости ради следует признать, что, хотя теоретически и существует возможность электронных вторжений в критичные системы управления, создающих серьезные, в том числе и физические, угрозы безопасности, получение контроля над такими системами извне является крайне маловероятным событием. В настоящее время реальность такова, что было бы проще и дешевле разбомбить цель, чем поразить ее путем взлома компьютерной системы.

Кибератаки действительно могут иметь серьезные последствия, хотя и не связанные с нанесением ущерба жизни и здоровью людей, массовыми разрушениями и другими катастрофами. В худшем случае, хорошо спланированная массированная кибератака может временно вывести из строя системы телекоммуникаций в густонаселенных районах. (Описание наихудших возможных сценариев кибер-атак приведено в Приложении №3).

Ядерный завод в штате Агайо функционировал в автономном режиме в течение года после того, как сетевой червь SQL Slammer привел к отключению Системы Отображения Периметра Безопасности на пять часов и заводского компьютера, используемого для мониторинга производственного процесса, на шесть часов. Для обеих систем были предусмотрены дублирующие аналоговые системы, которые не пострадали. Заводская производственная сеть была непосредственно подключена к корпоративной сети, в которую «червь» проник по удаленному каналу из партнерской сети.

Примером хакерской атаки на критическую инфраструктуру США может служить удаленный взлом в 2001 году компьютерной сети Независимого Системного Оператора Калифорнии, управляющего электросетью штата. Хотя тогда хакерам не удалось получить доступ к действующей системе управления электросетью, они имели доступ к корпоративной сети в течение 17 дней. Намерения хакеров и их происхождение так и остались невыясненными.

На начальном этапе развития в промышленных системах использовалось малоизвестное специализированное оборудование и программное обеспечение, а их сетевое взаимодействие с внешним миром было сильно ограничено. Круг возможных угроз был слишком узок, поэтому внимания вопросам информационной безопасности со стороны разработчиков и владельцев таких систем практически не уделялось. Со временем разработчики переходят на стандартные ИТ платформы, а владельцы промышленных систем, с целью повышения эффективности управления, подключают их к смежным системам. Существующая тенденция к повышению открытости и стандартизации промышленных систем повышает их уязвимость к кибератакам, однако среди экспертов не существует единого мнения относительно того, насколько сложной для аутсайдера задачей является получение доступа к промышленной системе. Большинство из них признает тот факт, что кибератаки действительно могут иметь серьезные последствия, хотя и не связанные с нанесением ущерба жизни и здоровью людей.

Эксперты из американской компании Riptech, известного поставщика услуг в области информационной безопасности, на основании своего опыта по обследованию большого количества крупнейших американских промышленных предприятий делают однозначный вывод об уязвимости критичных для американской экономики SCADA-систем в отношении кибератак. По их мнению, среди менеджеров подобных систем существует три общих заблуждения, препятствующих достижению адекватного уровня защищенности:

- *Заблуждение №1:* «SCADA-система размещается в физически изолированной сети».
- *Заблуждение №2:* «Существующие соединения между SCADA-системой и корпоративной сетью надежно защищены при помощи средств контроля межсетевого доступа».
- *Заблуждение №3:* «Для управления SCADA-системой требуются узкоспециализированные знания, что делает задачу получения удаленного контроля над подобной системой для хакера чрезвычайно сложной».

SCADA-системы действительно изначально создаются на базе физически изолированных компьютерных сетей и их системы защиты строятся исходя из этого предположения. Однако на практике для повышения эффективности управления подобными системами и оперативности принятия решений создаются соединения между SCADA-системой и корпоративной сетью. В результате большинство SCADA-систем оказываются опосредованно подключенными к сети Интернет.

В большинстве SCADA-систем существуют точки входа из корпоративной сети, незащищенные межсетевыми экранами (МЭ) и системами предотвращения атак (IPS), а некоторые из них могут быть вообще никак не защищены.

Третье заблуждение основано на предположении о том, что у атакующих отсутствует «инсайдерская» информация об архитектуре и средствах управления SCADA-системой. Однако если в качестве источника угроз рассматриваются организованные террористические группы, то это предположение вряд ли можно считать корректным. Кроме того, стремление к стандартизации подталкивает разработчиков SCADA-систем делать информацию об их архитектуре, интерфейсах и протоколах взаимодействия, а также о средствах управления общедоступной.

Джон Дубиэл, консультант из компании Gartner, принимавший участие в проведении атак на электросети во время военных учений, установил, что SCADA-системы могут быть атакованы

путем создания избыточной нагрузки (разновидность атаки на отказ в обслуживании). Это может привести к сбою или неправильному функционированию системы, что, в свою очередь, может привести к сбоям в работе других элементов системы управления, входящих в состав компьютерной сети предприятия, — эффект «цепной реакции».

Так, в 1996 году вдоль всего Западного Побережья США на протяжении 9 часов было отключено электричество. Это случилось из-за падения дерева на линии электропередачи, что, в комбинации с некоторыми другими факторами, привело к каскадному отключению других элементов электросети. В 1990 году похожее событие происходило с коммутатором компании AT&T, сбой которого вызвал цепную реакцию, повлекшую выход из строя телекоммуникационной сети по всей территории США. К аналогичным последствиям могла бы привести и успешная хакерская атака.

26–27 сентября 2007 года CNN и Associated Press обнародовали видеоролик, отснятый Департаментом Национальной Безопасности США (DHS), на котором запечатлен результат специально смоделированной кибератаки, направленной против электростанции.

Фильм демонстрирует перегрев турбины электростанции и ее разрушение. Этот тест был проведен Национальной Лабораторией Идахо. В ходе теста использовалась уязвимость в АСУТП, контролирующей турбину. Эта конкретная уязвимость была немедленно устранена, однако наверняка существуют и другие, поскольку при разработке подобных систем вопросы информационной безопасности серьезно не прорабатывались.

Многие предприятия имеют подключения к сети Интернет с управляющих терминалов SCADA-систем, что не могло не привести к серьезным инцидентам.

В ноябре 2001 года 49-летний Вайтек Боуден был осужден на два года лишения свободы за использование Интернет, беспроводного доступа и похищенного управляющего ПО для осуществления слива загрязненной воды в реку у побережья Маручидора в Квинсленде (Австралия). Ранее Боуден работал консультантом в водном проекте. Он пошел на это преступление после того, как правительством Маручи ему было отказано вработе на полную ставку. Он пытался получить доступ к системе водоочистки 45 раз, прежде чем ему удалось осуществить спуск отравленной воды.

_____

Показательным примером кибератаки со стороны инсайдера может послужить дело Вайтека Бодена, приговоренного к двум годам лишения свободы за причинение умышленного ущерба канализационной системе Совета Австралийского Графства Маручи. Боден работал контролером в компании, которая устанавливала данную систему, включавшую 150 насосных станций. Станции обменивались данными между собой и с центральным компьютером при помощи локальных процессоров. Когда проект был завершен, Боден уволился из компании и попытался устроиться на работу к бывшему заказчику, но получил отказ. После этого начались проблемы на насосных станциях. Постепенно стало ясно, что причина заключается не в системных сбоях. Система сигнализации отключалась, связь неожиданно обрывалась, насосы не включались в нужное время, – в результате происходил выброс нечистот. Боден проделывал все это из собственного автомобиля при помощи ноутбука, радиопередатчика и локального процессора, позаимствованного у бывшего работодателя.

_____

«Весь подводный мир у побережья был уничтожен, прибрежные воды окрасились в черный цвет, и вонь порой становилась невыносимой для местных жителей», – рассказывает Джанель Брайент, руководитель исследовательской группы Австралийского Агентства Защиты Окружающей Среды.

Тот факт, что злоумышленник оставался незамеченным на протяжении всех своих 44 попыток получения доступа к системе, красноречиво свидетельствует о неудовлетворительном состоянии информационной безопасности на общественных предприятиях. Проверка 50 предприятий, проведенная в 1997 году, установила, что на 40% водных предприятий операторам систем управления был разрешен прямой доступ к сети Интернет, а к 60% SCADA-систем можно получить доступ при помощи модема! Факты, прямо скажем, настораживающие. Однако одних этих фактов еще недостаточно для того, чтобы судить об уязвимости предприятий в отношении кибератак.

Как утверждает Элен Вэнко, представитель Североамериканского совета по обеспечению безопасности электроэнергетического комплекса, наличие подключения к сети Интернет или модемного подключения не следует во всех случаях рассматривать как уязвимость. «Все предприятия электроэнергетики подключены к Интернет тем или иным способом, однако это не означает, что наши системы управления доступны из Интернет».

Тем не менее подключение к Интернет открывает дополнительные возможности проникновения злоумышленников в компьютерные системы. «При анализе безопасности сетевой инфраструктуры эксперты прежде всего обращают внимание на подключения к Интернет» – говорит Крис Висопал, директор исследований и разработок компании @Stake.

Подключение систем управления к сети Интернет всегда таит в себе серьезную опасность. МЭ и другие средства сетевой защиты никогда не обеспечивают стопроцентной защищенности. В 1989 году хакерская группа «The Legion of Doom», получила контроль над телефонной сетью компании BellSouth, включая возможность прослушивания телефонных каналов связи, маршрутизацию вызовов, маскировку под технический персонал станции и даже вывод из строя системы 911. Компания BellSouth задействовала 42 сотрудника, которые трудились в течение 24 часов над восстановлением контроля над системой.

Уязвимость SCADA-систем признается многими экспертами. Так, президент и технический директор компании Foundstone, известного игрока на рынке информационной безопасности, Стюарт МакКлу дает на вопрос об уязвимости SCADA-систем однозначно положительный ответ. Более того, он оценивает сложность осуществления подобной атаки весьма невысоко: на 4–5 баллов по 10-балльной шкале. Происходит это потому, что, при отсутствии соответствующего регулирования со стороны государства, частные компании предпочитают экономить на безопасности. Кроме того, многие SCADA-системы функционируют в реальном времени, и требования безопасности идут вразрез с требованиями производительности.

После террористического акта 11 сентября 2001 года многие концепции обеспечения безопасности как на государственном, так и на частном уровне, подверглись пересмотру, и безопасность SCADA-систем была провозглашена в качестве одной из основных целей Национальной Стратегии Обеспечения Безопасности Киберпространства (The National Strategy to Secure Cyberspace) США, разработанной по инициативе американского Президента в конце 2002 года.

Однако пока даже самые серьезные кибератаки по своим последствиям далеки от сценариев массовых разрушений. Инцидент с заражением воды в Квинсленде, к примеру, не создал угрозы человеческим жизням и стоил примерно 13 тысяч долларов, затраченных на очистку воды, которая оперативно была произведена штатными сотрудниками.

Многие эксперты по безопасности признают, что широкомасштабное разрушение информационной инфраструктуры является чрезвычайно труднореализуемой задачей. Даже если злоумышленнику удастся проникнуть во внутреннюю сеть, для получения контроля над системой управления ему обязательно потребуется «инсайдерская» информация и очень глубокие знания этой системы.

Во время эксперимента по сценарию «Перл Харбор» аналитики из компании Gartner подтвердили это мнение. Очень сложно

атаковать что-то, о чем ты не обладаешь специфичными знаниями, признает аналитик Дэвид Фрэйли, который имитировал атаки на системы телекоммуникаций.

Даже во время успешной атаки на столичную электростанцию, многие критичные системы, такие как госпитали, продолжали функционировать, т.к. они перешли на автономные генераторы. Все предприятия резервируют критичные элементы своей информационной инфраструктуры для того, чтобы продолжать нормальное функционирование даже в случае сбоя системы управления.

Даже если хакеру, к примеру, удастся увеличить уровень хлора в водных резервуарах на станции водоочистки, отравленная вода не попадет в водопроводы, т.к. она проходит пятикратное тестирование. Агентство по защите окружающей среды требует от предприятий исследовать воду на наличие в ней более 90 видов отравляющих веществ. Более простой и опасной атакой является непосредственное физическое добавление террористами отравляющих веществ в водные резервуары.

Компьютерная сеть железнодорожной промышленности является одной из крупнейших в США и контролирует более 500 железных дорог. Поэтому федеральные власти США всегда уделяли повышенное внимание вопросам защиты информации в этой сети. Периодически там действительно возникают инциденты с сетевыми атаками, однако, по словам Нэнси Вильсона, вице-президента Ассоциации Американских Железных Дорог, они никогда всерьез не воспринимались, т.к. железнодорожные компании и компании других отраслей предпринимают серьезные меры по резервированию данных и оборудования, которые в большинстве случаев обеспечивают адекватный уровень защищенности.