КИБЕРАТАКИ НА КРИТИЧЕСКИ ВАЖНЫЕ ОБЪЕКТЫ – ВЕРОЯТНАЯ ПРИЧИНА КАТАСТРОФ

Автоматизированные системы управления технологическими процессами (АСУ ТП) критически важных объектов (КВО) находятся под угрозой как со стороны обычных вирусов, так и целенаправленных атак. Соответственно, защита их ИТ–инфраструктуры – это первоочередная задача для специалистов в области информационной безопасности. О средствах защиты, рисках, уязвимостях и других проблемах заместителю председателя редакционного Совета журнала «Вопросы кибербезопасности» Анатолию Тарасову рассказал ***Андрей Духвалов*** *– руководитель управления перспективных технологий, стратег по развитию технологий ЗАО «Лаборатории Касперского».*

Андрей Петрович Духвалов *– Главный Стратегический Архитектор Лаборатории Касперского, руководитель Департамента Перспективных Технологий. В софтверном бизнесе – около 30 лет. Большую часть своей профессиональной деятельности занимался разработкой разнообразного ПО в качестве программиста, ведущего инженера, архитектора, лидера проекта. Участвовал в различных проектах по созданию программных продуктов системного и прикладного уровня. Последние 15 лет Андрей разрабатывает ПО в области информационной безопасности.*

В настоящее время возглавляет подразделение Лаборатории Касперского, занимающееся исследованием новейших технологий

А.Т.: Выделите, пожалуйста, основные критерии защищенности ИТ-инфраструктуры критически важных объектов.

А.Д.: Основным критерием защищенности, на наш взгляд, является способность всей структуры АСУ ТП КВО к поддержанию стабильного, непрерывного и корректно работающего технологического процесса в рамках предопределенных ограничений и независимо от внешних воздействий. Именно технологический процесс (выработка и передача электричества, транспортировка газа, переработка руды, очистка воды, управление городскими коммунальными службами и т.д.) является основной функциональностью таких объектов, а поддержание его корректного функционирования и есть ключевая задача всех ИТ-систем.

Во-первых, АСУ ТП - это системы, построенные на основе и с применением тех же информационных технологий, которые используются в офисной и других сетях. И они имеют те же самые, знакомые нам на протяжении последних 15-20 лет проблемы и «болячки». Компании, предлагающие средства информационной безопасности, имеют большой опыт борьбы с этими проблемами, а «плохие ребята» - большой опыт использования этих проблем в своих целях. И огромное число «обычных» компьютерных вирусов вполне комфортно чувствуют себя в индустриальных сетях. Причем последствия от их вредоносного воздействия могут быть гораздо более значимыми, пусть даже это и не входило в изначальные планы «разработчиков».

Представьте себе самый прозаичный вирус из семейства winblocker'ов, который блокирует работу операционной системы Windows, вымогая 50 рублей за платное SMS-сообщение. Что если он вдруг заразит компьютер, контролирующий процесс производства азотной кислоты? Каковы могут быть ущерб и последствия? Часто владельцы индустриальных процессов, таких, например, как небольшие электрические подстанции, станции водоподготовки или отвода сточных вод недооценивают необходимость мер защиты от компьютерных вирусов ссыла-

ясь на то, что мы, мол, совершенно незаметная цель и никому в голову не придет нас атаковать. Однако они должны знать и помнить, что необязательно быть целью, что бы стать жертвой.

Нужно сказать и о намеренном информационном воздействии, о компьютерных атаках. Средств для осуществления намеренного вредоносного воздействия на промышленные объекты, к сожалению, более чем достаточно. Повторюсь, это происходит в частности из-за того, что для организации АСУ ТП применяются те же технологии, что с успехом применялись и для организации обычных компьютерных сетей. И знакомы они не только специалистам, но и хакерам. Целенаправленные атаки на информационные объекты, их в последнее время называют APT (advanced persistent threat – постояннодействующая, тщательно разработанная угроза), характеризуются очень высокой степенью профессиональной подготовки. Обычно они бывают очень длительными по времени и очень хорошо замаскированными.

Начальные фазы таких атак предназначены для тщательного и скрупулезного сбора информации об атакуемом объекте. Потом, как правило, следует фаза подготовки воздействия. И только на самом последнем этапе происходит это самое воздействие, которое, как правило, бывает очень непродолжительным по времени. При этом последняя фаза совсем не обязательно должна идти сразу за фазой подготовки. Интервал между ними может быть месяцы и годы: кто-то исследовал объект, подготовил атаку и ожидает подходящего момента для нанесения заключительного удара.

Поскольку атаки готовятся высококвалифицированными «специалистами», обнаружить их, а тем более противодействовать им без специализированной подготовки, не представляется реальным.

По результатам наших исследований и по мнению партнеров, следы начальных замаскированных фаз таких атак довольно часто обнаруживаются на промышленных объектах. Такие объекты неведомо для их владельцев и по чьему-то злому умыслу находятся под угрозой внезапного непредсказуемого поведения.

Угрозу АСУ ТП может представлять и банальное мошенничество. Для многих является большим искушением заработать на обмане клиентов, хозяев производств или еще кого-то. Информационные технологии предоставляют таким людям новые возможности. Например, обладая некоторыми знаниями, можно настроить компьютерную систему на бензоколонке так, чтобы она в определенных условиях наливала на 15% больше бензина. Или, наоборот, на 1% меньше, но всем подряд. Обнаружить такие неправомерные «настройки» очень непросто, но такие факты нам известны. Большая проблема заключается в том, что такие «специалисты», подкручивая настройки, сами того не осознавая, могут привести систему в такое состояние, когда она вообще не сможет выполнять свои функции.

При этом следует отметить, что в реальной жизни существует масса факторов, из-за которых системы АСУ ТП могут выйти из строя, и далеко не всегда это связано с вредоносным программным обеспечением (ПО), хакерской целенаправленной атакой или мошенничеством. Иногда это просто проявление халатности, допущения ошибки, недостатка компетенции, или недобросовестного действия (бездействия) со стороны персонала. Поэтому к критериям защищенности нужно отнести не только защиту от внешних или случайных атак, но и инструменты предупреждения и предотвращения некорректных или ошибочных действий со стороны собственных операторов.

Еще одним источником сбоев являются ошибки в программном обеспечении (ПО) АСУ ТП, не обнаруженные на этапе тестирования. Особо подчеркнем, что защищенная инфраструктура не должна допускать сбоев технологических систем из-за ошибок в ПО.

А.Т.: Какие вы можете назвать известные ИБ-риски, специфичные для КВО? Расставьте их, пожалуйста, по величине возможного ущерба?

А.Д.: Главный и принципиальный риск заключается в том, что любая успешная атака на КВО чревата реальным ущербом, вплоть до катастроф и потери многих человеческих жизней. Нам бы не хотелось в явном виде указывать риски ИБ КВО, чтобы не провоцировать злоумышленников и не давать им подсказки, поэтому ограничимся обобщенными формулировками.

Среди рисков ИБ, специфичных для КВО, можно назвать следующие. Во-первых, использование в АСУ ТП устаревшего программного

обеспечения, оборудования и коммуникационных протоколов, изначально не предполагавших даже самой возможности киберугроз. Во-вторых, это административные и технологические трудности для обновления ПО. В-третьих, неконтролируемое подключение сети АСУ ТП к общей сети предприятия или даже к интернету. В-четвертых, это доступ сторонних компаний к технологической сети.

А.Т.: Какие факторы затрудняют защиту ИТ-инфраструктур КВО?

А.Д.: Нужно особо отметить недостаток внимания к проблеме защиты АСУ ТП в целом. Владельцы критических объектов по разным причинам недооценивают информационные угрозы. Существует явный недостаток таких необходимых процедур, как информационный аудит, тестирование на проникновение, сканирование уязвимостей, тренинг персонала и т.д. Свое негативное влияние оказывает сложная бюрократическая процедура внесения изменений в работу ответственных технологических узлов.

Так, например, российские АСУ ТП, однажды пройдя процедуру ввода в эксплуатацию, «опечатываются», и работают без обновлений многие годы. Строгие регламенты и нормативные акты предприятия не позволяют вносить в уже сертифицированную систему какие-либо изменения даже в виде обновления операционной системы. А при приемке систем в программной методике испытаний для них часто отсутствует проверка встроенных свойств информационной безопасности. Да и сама безопасность сводится к ограничению доступа пользователя по паролю, который нередко хранится в открытом виде в баз данных (БД) самого приложения или на бумажке, приклеенной к монитору.

Если говорить об используемом в АСУ ТП вычислительном оборудовании, то, как правило, оно даже вводится в эксплуатацию с уже устаревшим внутренним исполняемым микрокодом. В то время как на сайте производителя находится свежая прошивка, в которой уже может быть закрыт ряд известных проблем с ИБ, их наличие никто не проверяет даже на этапе развертывания системы просто потому, что этого никто не требует.

Как правило, автоматизацией технологических процессов КВО занимаются не сами предприятия, а сторонние фирмы-подрядчики. Они заинтересованы в реализации именно функциональной составляющей, поскольку это те самые свойства системы, за которые они получают деньги, тогда как грамотная реализация функций ИБ для них – только затраты. Вот и получается, что подрядчики реализуют ту ИБ, что требует от них заказчик, а тот, в свою очередь, ссылается на требования действующего законодательства, «чтобы проблем не было». Соответственно, ни о какой проверке разрабатываемого ПО современными методами, например, фаззинга и пентестинга не идет и речи.

А.Т.: Нужны ли для защиты ИТ-инфраструктур КВО принципиально новые ИБ-методы и ИБ-продукты? И какие?

А.Д.: Разумеется, нужны. Многие участники рынка ИБ сейчас пытаются внедрять свои обычные, «офисные» продукты в АСУ ТП. Желание предоставить меры защиты однозначно полезно, однако, тут нужно проявлять осторожность. В АСУ ТП своя специфика, и нужны продукты, ее учитывающие. Со своей стороны «Лаборатория Касперского» сейчас готовит ряд продуктов, учитывающих специфику АСУ ТП.

Что касается разработки новых методологий защиты и стандартов, применимых в АСУ ТП, то это, конечно, очень важно. Сейчас не существует единой, простой и понятной методики, в которой специалисту по ИБ были бы предложены шаги, необходимые для обеспечения достаточного уровня защищенности своей АСУ ТП

А.Т.: Готова ли ИБ-индустрия, в первую очередь отечественная, сегодня обеспечить защиту ИТ-инфраструктур КВО?

А.Д.: Специалистов по информационной безопасности в России достаточно. Накоплен огромный опыт по реализации и интеграции крупных проектов по информационной безопасности обычных информационных структур, как силами российских специалистов, так и в кооперации с ведущими западными компаниями. Да, конечно, в отношении ИБ КВО требования несколько меняются, но сейчас многие российские компании, в том числе и Лаборатория Касперского, активно работают в этом направлении и разрабатывают решения для защиты АСУ ТП. Я уверен, что в ближайшем будущем такие решения появятся и на рынке.

А.Т.: Как вы оцениваете состояние российской нормативной базы, относящейся к области ИБ КВО?

А.Д.: Вопрос об информационной безопасности КВО в России давно назрел, и его следует решать комплексно. Необходимо отметить, что руководство России понимает серьезность существующих проблем, и на уровне ведущих ведомств разрабатываются различные меры по исправлению ситуации и предупреждению возможных негативных последствий. Так, Совет Федерации Федерального Собрания РФ в 2012 году разработал «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации». В настоящее время на публичное обсуждение представлена вторая редакция проекта Федерального Закона «О безопасности критической информационной инфраструктуры российской федерации». ФСТЭК разрабатывает технические рекомендации по информационной защите АСУ ТП критически важных объектах.

Помимо законодательной базы, конечно, должны быть разработаны и типовые отраслевые методики построения защищенной инфраструктуры КВО; выработаны критерии оценки защищенности инфраструктуры, которые в необходимых случаях могут оперативно дорабатываться и адаптироваться под изменения ландшафта угроз; разработаны также методы стимулирования и юридической поддержки критически важных объектах; подготовлены и реализовываться образовательные программы для работников и управляющих КВО.

Ведь надежную защиту способно обеспечить только реальное сотрудничество государства, владельцев КВО и других участников рынка.

На мой взгляд, государству необходимо предпринимать также и другие меры, например, организовывать регулярные антикибертеррористические тренинги, разрабатывать и внедрять единую политику обеспечения и контроля цепочек поставок (supply chains) оборудования и ПО для критически важных объектах, создавать единые стандарты по приемке и сертификации АСУ при вводе их в эксплуатацию на КВО по целому ряду критериев, включая ИБ.

К сожалению, сегодня в России никто конкретно не занимается исследованиями проблем безопасности АСУ ТП в комплексном и системном режиме, поскольку это направление во многом находится вне предметной компетенции государственных органов.

В том числе именно поэтому Лаборатория Касперского видит необходимость в создании Национальной Российской тестовой лаборатории по исследованию проблем информационной безопасности КВО. Такой единый центр мог бы на федеральном уровне исследовать как уже известные, так и перспективные подходы по обеспечению информационной безопасности АСУ ТП, своевременно обнаруживать проблемы ИБ в используемых программных и аппаратных средствах, вырабатывать рекомендации по их устранению, информировать соответствующие предприятия, рекомендовать проверенные решения к использованию на КВО, организовывать и проводить специальные учения на федеральном уровне и т.п.

Создание эффективных механизмов по предупреждению возможных негативных проявлений и последствий от кибератак на критически важные объекты – это стратегически-важная задача сегодняшнего дня, реальный путь предупреждения масштабных катастроф, обеспечения национальной безопасности государства.

Не следует забывать, что к критически важным объектам относятся объекты, нарушение (или прекращение) функционирования которых приводит к потере управления, разрушению инфраструктуры, необратимому негативному изменению (или разрушению) экономики страны, субъекта или административно-территориальной единицы, или существенному ухудшению безопасности жизнедеятельности населения, проживающего на этих территориях, на длительный период времени.