Актуальные вопросы защиты АСУ ТП

Вирус Petya/NotPetya в 2017 году был примером того, насколько крупный бизнес может пострадать от такого рода атаки.
Компании и госструктуры подсчитывают потенциальные убытки, которые могут понести в случае, если не будут готовы к внезапному вторжению в свою экосистему. Поэтому тема безопасности сегодня особенно актуальна, если речь идет об объектах инфраструктуры, от которых напрямую зависит жизнедеятельность целых городов, отдельных регионов, а то и всей страны.
Какие существуют типовые проблемы безопасности АСУ ТП, повлияет ли 187-ФЗ на зрелость процессов обеспечения ИБ в промышленности и в чем сложность реализации защиты АСУ ТП? На эти и другие вопросы редакции ответили эксперты информационной безопасности:

Дмитрий Даренский, *руководитель практики промышленной кибербезопасности Positive Technologies*
Андрей Нуйкин, *начальник отдела обеспечения безопасности информационных систем, блок вице-президента по ИТ, ЕВРАЗ*
Игорь Тарви, *ведущий архитектор систем безопасности АСУ ТП, АО "ДиалогНаука"*

– Что вы можете сказать об актуальной специфике защиты АСУ ТП?

Дмитрий Даренский

– Сегодня основная проблема при обеспечении безопасности АСУ ТП связана с распределением зон ответственности на предприятиях. За АСУ ТП, как правило, отвечают службы эксплуатации, основная задача которых – функциональная безопасность. Риски АСУ ТП с точки зрения информационной безопасности исторически не учитываются. Отсутствует и опыт минимизации этих угроз, и понимание их опасности. А ИБ-специалисты, если они есть в штате, на предприятии заняты защитой офисной ИТ-инфраструктуры. Для решения этой проблемы сегодня на некоторых промышленных объектах создаются объединенные группы, состоящие из специалистов по эксплуатации и информационной безопасности, либо ИБ-специалисты включаются в штат службы эксплуатации. И это положительная тенденция, на наш взгляд.

Наибольшее понимание проблем ИБ сейчас мы видим у металлургов, а самая консервативная пока отрасль по вполне понятным причинам – энергетика. Несмотря на огромный объем работы, которую делаем мы и другие компании, развитие направления информационной безопасности в АСУ ТП здесь идет довольно медленно.

Андрей Нуйкин

– В настоящий момент актуальны вопросы разделения корпоративных и технологических сетей, выявление всех потоков информации и организация правильных настроек безопасности. Вопрос разделения сетей достаточно сложен в связи с тем, что технологические системы крайне сложно менять и простая смена адресации может быть практически невыполнима. Множество тонкостей также возникает при защите MES-систем.

Игорь Тарви

– Защита АСУ ТП – это отдельная область информационной безопасности, которая накладывает определенную специфику. В каждом случае от специалистов по защите требуется серьезное погружение в технологические процессы защищаемых систем. Оборудование, входящее в состав АСУ ТП, порой уникально, предназначено для выполнения конкретных целей и спроектировано для решения определенных задач. В АСУ ТП также могут применяться уникальные технологические протоколы.

Зачастую в ходе построения системы защиты возникает необходимость взаимодействия с разработчиками АСУ ТП, тестирования на их стендах предлагаемых заказчикам программно-аппаратных средств защиты, получения подтверждения о совместимости продуктов. При этом не редкость, когда разработчик не отечественный, а документацию на систему нельзя назвать исчерпывающей.

– Какие существуют типовые проблемы безопасности АСУ ТП?

Дмитрий Даренский

– Наибольшая угроза связана с действиями сотрудников, имеющих доступ к АСУ ТП. Это могут быть специалисты по эксплуатации, администраторы, инженеры, подрядчики, аутсорсеры и т.д. При этом их действия зачастую связаны с выполнением должностных обязанностей. Это может быть, к примеру, скачанный с торрентов и установленный на контроллер файл прошивки или USB-модем, необходимый для того, чтобы работать с системой удаленно. Антивирусные решения на рабочих станциях SCADA могли быть установлены несколько лет назад и при этом быть ни разу не обновленными. Причем все это может существовать в рамках "устоявшейся практики" на отдельно взятом предприятии.

Одна учетная запись на 20 инженеров – практически классика нашего АСУ ТП. В некоторых случаях запрос пароля просто отключен. Причина вполне объяснима: в случае аварии дежурные инженеры должны иметь доступ ко всем системам. Однако такая ситуация существенно упрощает работу злоумышленнику и снижает персональную ответственность. Есть кейс, когда на предприятии была остановлена технологическая установка на 10 мин в связи с установкой некорректной конфигурации контроллера (отмечу, что время простоя на предприятии всегда имеет четкий расчет финансовых и материальных потерь). При этом два инженера использовали одну учетную запись. В данном случае на объекте был только один из них, поэтому виновника определить удалось, а вот если бы присутствовали оба – ответственность могли бы понести также оба (один из них незаслуженно), которая, к слову, может быть как материальной (если это прописано в трудовом договоре), так и уголовной.

Андрей Нуйкин

– Отсутствие четкой границы между корпоративными и технологическими сегментами. Наличие настроек по умолчанию, например учетные записи с паролем по умолчанию. Отсутствие обновлений ОС и ИС в технологической сети.

Игорь Тарви

– При реализации проектов по построению систем защиты АСУ ТП встречается ряд типовых проблем, носящих системный характер:

- отсутствие на объектах заказчиков специалистов по защите с необходимой квалификацией;
- фокусировка на задачах обеспечения безопасности корпоративного сегмента сети и отсутствие внимания к технологическому аспекту, в силу недостаточных знаний об архитектуре и функционировании АСУ ТП или недостаточной вовлеченности специалистов в технологические процессы (как следствие, во многих компаниях подход к защите АСУ ТП ограничивается исключительно защитой периметра технологической сети и, возможно, установкой антивирусных средств);
- применение в системах АСУ ТП средств защиты корпоративного уровня, которые могут негативно повлиять на технологический процесс в силу их неприспособленности к специфической среде функционирования и не учитывающие особенности реализации технологических процессов.

– Нас уже несколько лет пугают четвертой промышленной революцией. Что это такое и сделает ли она АСУ ТП безопасней?

Дмитрий Даренский

– Представим, что вы выбираете автомобиль на сайте: цвет кузова, обивка сидений, тип коробки и колесных дисков. Сегодня эти данные уходят дилеру, а затем по длинной цепочке и с участием большого количества людей – на предприятие. Цифровая революция в промышленности (в идеальном виде) предполагает автоматизацию этой цепочки: ваш заказ будет сразу идти в системы управления складскими запасами, производственными линиями и т.д. Разумеется, у злоумышленников в этом случае появляется множество вариантов для атаки, от поддельного заказа на тысячу розовых автомобилей (условно) до блокировки сайта и остановки производственной линии. Недоступен сайт – значит, заказчики не могут заказать автомобили, так как вся остальная цепочка автоматизирована. Остановилась линия – тоже понятно, что это беда.

С развитием цифровизации "всего" окончательно канет в Лету миф об изолированности технологической сети, и ее придется все-таки защищать от кибератак. Уже сегодня, если хакер изменит параметры, скажем, пастеризации молока, то завод может успеть изготовить тонны некачественной продукции до того момента, когда это будет обнаружено. В фармацевтике, если отдел качества пропустит факт нарушения рецептуры, такая атака может привести к наличию пострадавших от некачественных или даже опасных лекарств. Последствия и для потребителей, и для самого предприятия настолько серьезные, что их даже объяснять не стоит.

Андрей Нуйкин

– Мне кажется, что тема Internet of Things станет такой революцией. Однако на сегодня эта тема скорее ухудшает безопасность, так как нет четких требований по обеспечению безопасности при работе с подобными устройствами.

Игорь Тарви

– Вопросы возможности перехода к Индустрии 4.0 – внедрению технологий сбора и обработки больших объемов данных (BigData), использованию облачных технологий и технологии распределенного реестра – возникают все чаще, в основном в контексте обеспечения более эффективного управления предприятием, при этом такие кардинальные изменения, естественно, не смогут не отразиться на АСУ ТП.

Привлечение в производство современных технологий изменяет не только архитектуру АСУ ТП, но и ландшафт потенциальных угроз, образуя новые. Если ранее АСУ ТП функционировали

автономно, то теперь, под влиянием бизнес-процессов, появляется острая необходимость объединения их в общую технологическую сеть, организации их взаимодействия как между собой, так и с общим центром. Зачастую при организации таких связей используются сети сторонних компаний, а также общедоступная сеть Интернет. Это порождает новые угрозы, к которым системы АСУ ТП изначально готовы не были, и, как следствие, растет количество инцидентов ИБ.

– Как влияет 187-ФЗ на зрелость процессов обеспечения ИБ в промышленности?

Дмитрий Даренский

– Ранее для АСУ ТП существовали нормативные документы, такие как 31-й приказ и рекомендации по КССИ, однако они носили рекомендательный характер. 187-ФЗ сделал требования к обеспечению критичных систем, в том числе и промышленных, обязательными и ввел довольно однозначные понятия ответственности.

Для некоторых компаний 187-ФЗ – кнут, которого им хочется избежать, и не все пока понимают, подпадают ли они под действие этого закона. На предприятиях с более высоким уровнем зрелости и понимания проблематики ввод 187-ФЗ существенно ничего не изменил: вопросами безопасности там как занимались, так и занимаются. Более того, он позволил лучше структурировать эту работу и в целом подтвердил целесообразность деятельности в данном направлении.

Андрей Нуйкин

– Данный закон заставил многие компании взглянуть на свои промышленные системы под новым углом и задуматься об их безопасности. Хотелось бы верить, что реализация закона не остановится на бумажной безопасности и позволит реально защитить критические системы. Крупные компании и без закона активно занимались обеспечением безопасности своих технологических систем и сетей. ЕВРАЗ начиная с 2016 г. реализует проекты в области защиты технологических систем и сетей.

Игорь Тарви

– На сегодняшний день обеспечение ИБ АСУ ТП является одним из наиболее актуальных направлений для большого числа российских компаний, доля вовлеченности которых из различных сегментов промышленности продолжает увеличиваться с каждым годом. Если еще буквально несколько лет назад данной тематике уделяли больше внимания компании тяжелой, военной, добывающей промышленности, то теперь к ним присоединяются обрабатывающая, легкая и даже пищевая промышленность.

Такая ситуация складывается в том числе благодаря принятию 187-ФЗ, определившему достаточно широкий перечень видов деятельности, на которые распространяются требования по защите информации. Поэтому появление соответствующих приказов ФСТЭК России, являющихся обязательными к применению для значимых объектов критической информационной инфраструктуры, в дополнение к рекомендательному 31-му приказу ФСТЭК России от 14.03.2014, позволит промышленным организациям по-другому взглянуть на вопросы защиты АСУ ТП. Повышение уровня зрелости процессов обеспечения ИБ будет напрямую зависеть от степени формальности отношения к предъявляемым требованиям.

– В чем сложность реализации защиты АСУ ТП?

Дмитрий Даренский

– Не так сложно, как может показаться. Для решения многих проблем зачастую достаточно организационных мер, таких как обучение сотрудников основам ИБ, выстраивание процессов соблюдения и контроля за выполнением политик безопасности, информирования персонала. Сегодня существует достаточное количество общепринятых практик, стандартов, отраслевых и международных рекомендаций, международно признанных обучающих и сертификационных курсов в области ИБ АСУ ТП, и ИБ-специалисту в промышленности есть на что опереться. Это, например, документация NIST, стандарты IEC, IEEE и т.д. То есть весь необходимый базис для того, чтобы на конкретном предприятии можно было хотя бы начать заниматься

вопросами безопасности, есть. Его можно брать, адаптировать по свои задачи и использовать.

Андрей Нуйкин

– Основная сложность в том, что АСУ ТП нельзя останавливать и при реализации защиты нужно быть полностью уверенным, что внедряемые средства защиты не будут влиять на производственный процесс и не приведут к остановкам и сбоям.

Большой проблемой также для старых систем АСУ ТП является сложность или невозможность внесения изменений в системы, и приходится перерабатывать средства защиты для того, чтобы их внедрение, с одной стороны, выполняло защитную функцию, а с другой – не нарушило работу АСУ ТП.

Игорь Тарви

– Многие технологические процессы и реализующие их АСУ ТП чувствительны к временным задержкам. На мой взгляд, основная сложность заключается в отсутствии эффективных средств защиты, которые могли бы выполнять свои функции в условиях сильного ограничения системных ресурсов (процессорного времени, объемов выделенной памяти), не влияя при этом на временные характеристики.

При реализации защиты АСУ ТП немало сложностей вызывает также отсутствие квалифицированных специалистов по защите информации, имеющих достаточный опыт работы непосредственно с АСУ ТП, понимающих специфику их работы и способных выстраивать процессы и систему защиты таким образом, чтобы избежать негативного влияния на технологические процессы. ●

Ваше мнение и вопросы присылайте по адресу is@groteck.ru