От мнимой защищенности к реальной

текст: Яков Шпунт

Недавно принят закон 187-ФЗ «Об обеспечении безопасности критической информационной инфраструктуры». Его очень давно ждали, ведь он касается такой серьезной и крайне актуальной темы, как организация защиты систем MES/АСУ ТП и технологических сетей. Долгое время этой темой всерьез не занимались, хотя проблем в данной сфере накопилось немало и многие из них из разряда застарелых.

Параллельные вселенные

На протяжении многих лет ИТ и АСУ ТП были своего рода параллельными вселенными. Хотя уже достаточно давно при создании систем промышленной автоматики используются стандартные массовые компоненты. Например, АРМ диспетчерской системы, или SCADA, представляет собой по большому счету обычный персональный компьютер с соответствующим ПО. Но при этом промышленная автоматизация — область весьма консервативная. В итоге те же АРМ SCADA-систем работают под управлением в лучшем случае Windows XP, если не Windows 2000 или даже DOC. Вряд ли надо напоминать, что они давно сняты с поддержки и у них не закрыты очень многие бреши в безопасности.

При этом установка постороннего ПО, в том числе защитного, на комплексы АСУ ТП не допускается. И здесь, надо сказать, есть свои резоны. Во-первых,

Многие аудиты безопасности, в том числе и в российских компаниях, выявляют тот факт, что персонал применяет данную инфраструктуру для компьютерных игр

нужно предусмотреть технологические окна для обновления баз, что далеко не всегда возможно. Во-вторых, любое постороннее ПО занимает процессорное время, что делает реакцию системы потенциально непредсказуемой. Учитывая, что счет часто идет даже не на секунды, а на доли секунды, такой риск неприемлем. Да и вопросы организации АРМ настолько регламентированы, что считается недопустимым даже использование клавиатур и мышей не из рекомендованного списка. Ведь любое взаимодействие компонентов требует тщательного тестирования, в котором необходимо предусмотреть любую мелочь.

Долгое время с потенциальными уязвимостями мирились, поскольку комплексы MES/АСУ ТП не были подключены к публичному Интернету. Но по мере внедрения систем автоматизации бизнес-процессов возникала потребность интеграции ERP- и низкоуровневых систем, что без интерфейсов для связи между ними, естественно, сделать невозможно. И даже если такая связь была организована сеансами по несколько минут, этого оказывалось достаточно для успешной атаки или заражения вредоносным ПО. Первым серьезным инцидентом стало заражение червем Slammer одной из американских АЭС, чрезвычайно быстро распространявшимся и перегружавшим сети, в которые проникал. Были проблемы и с системами управления на отдельных российских железных дорогах из-за того, что те же черви забивали сетевой трафик.

В некоторых отраслях, например энергетике и коммунальном хозяйстве, технологические системы просто связаны с интернет-порталами самообслуживания. А их будут пытаться взламывать обязательно, поскольку речь идет о живых деньгах, и такие атаки происходят постоянно. Наиболее активны здесь румынские злоумышленники, но подобные инциденты отмечаются по всему миру, в том числе и в России. И случаи, когда злоумышленники вместо транзакционного модуля попадают в технологическую систему, далеко не единичны. Причем иногда с довольно серьезными последствиями. Так, несколько лет назад на одном из водоканалов США было нарушено функционирование системы обеззараживания стоков. Оказалось, в управляющий комплекс, построенный на базе рабочей станции IBM 1980-х годов выпуска, проникли злоумышленники, которые изменили текстовый конфигурационный файл, где и хранились параметры работы комплекса обеззараживания стоков.

Далеко не редкость и то, что технологические сети, деликатно выражаясь, используются не по назначению. Так, многие аудиты безопасности, в том числе и в российских компаниях, выявляют тот факт, что персонал применяет данную инфраструктуру для компьютерных игр.

Серьезной проблемой для наших условий становится и падение уровня квалификации персонала. В итоге растет количество ошибок, в том числе и таких, которые чреваты весьма тяжелыми последствиями. При этом нельзя исключать и того, что с помощью манипулятивных технологий или шантажа работника могут вынудить совершить те или иные действия, например запустить программного зловреда или посетить зараженный веб-сайт.

Когда инфраструктура торчит наружу

В последнее время изоляция технологических сетей от публичного Интернета становится мнимой. Так, работники подключают АРМ с помощью мобильных модемов. Еще одна

распространенная ситуация — организация удаленного канала, с помощью которого технический персонал может управлять системами АСУ ТП со своих личных ПК. Причем делается это, как правило, очень неаккуратно. Итог вполне очевиден: достаточно лишь нескольких часов, чтобы о данном факте стало известно всем желающим. Согласно отчету «Безопасность АСУ ТП: итоги 2016 года», опубликованному компанией Positive Technologies, более 162 тысяч компонентов АСУ ТП подключены к публичному Интернету. Учитывая, что ПО, используемое при создании комплексов АСУ ТП, имеет уязвимости, из которых 60% относится к критичной или высокой степени, часто применяются простые, легко подбираемые пароли, взлом такой системы превращается в тривиальную задачу даже для не очень квалифицированного злоумышленника. Кстати, в данном качестве могут выступать и бывшие сотрудники, желающие, например, отомстить за свое увольнение.

Естественно, комплексы АСУ ТП становятся желанной мишенью для кибернападения в ходе межгосударственных и межкорпоративных конфликтов. Прецеденты уже есть. Первым стал Stuxnet, направленный против иранской ядерной программы. Это была целая спецоперация, где вредоносное ПО, к слову, сложное и предназначенное для совершенно определенного комплекса, стало лишь одним из элементов. Stuxnet заразил множество SCADA-систем по всему миру, но нигде, кроме Ирана, вреда не нанес. Более серьезный прецедент — атака сирийских кибернаемников на нефтяные компании Катара и Саудовской Аравии, проведенная с помощью вредоноса Shamoon. Он был написан, что называется, на коленке, но свою задачу выполнил, на несколько дней парализовав добычу нефти. Но чаще всего под ударом хакеров оказываются энергетики. Так, по некоторым данным, вторжения в технологические системы являются причиной до двух третей энергоаварий в США. Были предприняты и масштабные атаки на энергосистемы Израиля и Украины.

Атака на АСУ ТП, которая управляет критически важным или потенциально опасным объектом, представляет интерес для хактивистов (политически мотивированных хакеров), террористических группировок или просто криминала. Как уже было сказано, подобное кибернападение не потребует от исполнителя высокой квалификации, но последствия будут сравнимы с крупным терактом, артиллерийским или ракетным обстрелом. Но при существенно более низких затратах всех возможных ресурсов. Так что многие группировки, в частности запрещенные в России сети «Аль-Каида» и ИГИЛ, активно работают над созданием хакерских групп.

АСУ ТП под надзором. Теперь и у нас

Естественно, разные государства и отраслевые сообщества не остаются в стороне. Существуют нормативы, в том числе законы, всякого рода стандарты и регламенты, которым необходимо следовать. И наша страна не исключение. Закон 187-ФЗ, о котором шла речь в начале статьи, лишнее тому подтверждение. Впрочем, очень многие предприятия не стали ждать его принятия и начали предпринимать меры сами. Раньше других за дело взялись транспортники и энергетики, где ситуация с угрозами была наиболее напряженной.

Под действие 187-ФЗ подпадают информационные системы госорганов и госучреждений, а также предприятия целого ряда отраслей, включая ВПК, химическую, металлургическую, горнодобывающую, ракетно-космическую промышленность, энергетику, банки и финансы, транспорт, связь. В законе прописаны меры, регламентирующие защиту от инцидентов, и меры, которые необходимо принимать в том случае, если атака все же случилась. Также предусмотрена ответственность за неисполнение требований 187-ФЗ и подзаконных актов к нему, вплоть до уголовной, причем весьма серьезной, до 8 лет лишения свободы, если инцидент привел к тяжким последствиям. Впрочем, этот закон начинает действовать в полной мере еще не очень скоро, учитывая, что подготовлена далеко не вся нормативная база, но начало положено. И надо быть готовым к тому, что эти меры придется соблюдать.