СЛУГИН А. Г., ЖУКОВ С. А., ШИШОВ О. В.

ПРОБЛЕМА КИБЕРУГРОЗ В ПРОМЫШЛЕННЫХ СИСТЕМАХ АВТОМАТИЗАЦИИ

Аннотация. Рассматриваются причины возникновения возможности кибератак на промышленные объекты. Анализируются основные пути повышения промышленной сетевой безопасности.

Ключевые слова: промышленная автоматизация, контроллер, кибератака, политика безопасности, цифровая промышленная сеть.

SLUGIN A. G., ZHUKOV S. A., SHISHOV O. V.

THE PROBLEM OF CYBER THREATS IN INDUSTRIAL AUTOMATION SYSTEMS

Abstract. The article considers the reasons of cyberattacks on industrial facilities. In this connection, the main ways of industrial network security improvement are analyzed.

Keywords: industrial automation, controller, cyberattack, security policy, digital industrial network.

В IT-мире необходимость постоянной защиты от киберугроз ни у кого не вызывает споров. В настоящее время ее необходимость становится очевидной и в промышленных системах управления технологическим оборудованием. Так, успешная кибератака на промышленную систему может повлечь за собой производственные потери, урон системе безопасности и окружающей среде, кражу интеллектуальной собственности. Работая в безостановочном режиме, в жестко регламентированных условиях, промышленные сети, как правило обходят, большую часть политик безопасности и регламентов, действующих для информационных сетей.

В прошлом основной причиной защиты промышленного сегмента сети был человеческий фактор или сбой в сети. Соответственно, промышленное оборудование для автоматизации проектировалось без учета возможностей появления паразитного или неспециализированного сетевого трафика. Риск кибератак извне, особенно нацеленных на промышленные системы связи связи, практически не брался в расчет.

Еще не так давно системы управления использовали закрытые протоколы передачи данных и полевые шины, не связанные напрямую с информационной сетью предприятия и сетью Интернет. Таким образом, безопасность промышленной сети (сети технологической системы) обеспечивалась методом ее изоляции. За последние 10–20 лет наметилась тенденция миграции промышленных сетей с собственных технологий и стандартов на готовые коммерческие решения и технологии. Возрастает потребность в on-line доступе к

технологическим данным извне, что означает прямое соединение технологической сети с информационной сетью предприятия и сетью Интернет. Работа современной технологической сети требует постоянного удаленного доступа, обновления данных. В результате технологическая сеть предприятии не может быть больше изолирована от общей сети. Например, де-факто стандартом в технологических сетях связи становится Industrial Ethernet. Технологическое оборудование использует протоколы на базе IP, в том числе стандартные TCP/IP, UDP, наследуя все их слабые места. С возникновением необходимости взаимодействия систем производственно-технологического управления (SCADA/DMS) с ERP/MES-системами верхнего уровня изоляция промышленного контура сети стала невозможной. Кроме связи с корпоративной сетью, необходимо учитывать интерфейсы удаленного управления и USB-порты рабочих станций как возможные дополнительные пути проникновения вредоносного промышленного обеспечения.

Конечные устройства в технологической сети (контроллеры) проектировались с фокусом на максимальную надежность. Сегодня встроенные в них средства защиты от несанкционированного доступа по сети находятся на начальном уровне, недостаточном для защиты от современных киберугроз и требуют развития. При этом простое копирование методов обеспечения кибербезопасности из IT-сетей невозможно: архитектура, характер оборудования, типы трафика, внешняя среда и установленные регламенты существенно отличаются. Различаются и типы угроз. Появление специфического класса промышленного вредоносного программного обеспечения подразумевает специализированные методы и средства зашиты. В этой связи важно использовать технологии и решения, предназначенные именно для промышленного сектора.

В настоящее время можно с уверенностью сказать, что возникло новое научное направление – промышленная сетевая безопасность. В этой связи было исследовано множество уязвимостей промышленных систем управления, исходных кодов вредоносного программного обеспечения.

Хорошим базисом для выработки политики безопасности специально для промышленных систем управления является серия стандартов для обеспечения кибербезопасности промышленных систем автоматизации и управления ANSI/ISA99. Стандарты описывают общую концепцию по обеспечению кибербезопасности, модели, отдельные элементы системы безопасности применительно к промышленным системам управления, они в свою очередь являются базовыми документами для стандарта IEC 62443 «Безопасность систем управления».

Стандарт IEC 62443 описывает способы повышения промышленной сетевой безопасности. Он относится к промышленной безопасности в общем, без привязки к какой-либо отрасли. Сегодня на рынке доступны разработанные в соответствии с этим стандартом промышленные межсетевые экраны, позволяющие организовывать безопасные зоны с ПЛК или OPC-серверами.

Отдельные отрасли тоже имеют свои собственные стандарты сетевой безопасности, например, стандарт NERC CEP предназначен для североамериканской энергетики. В отличие от стандарта IEC 62443, сертификация по которому является добровольной процедурой, NERC CIP обязателен в США.

Ряд корпораций не только разрабатывают стандарты безопасности, но и регламенты по ее обеспечению, систему сертификации персонала. Хотя политики безопасности в каждой организации свои, некоторые факторы в них должны быть упомянуты обязательно:

- удаленный доступ;
- портативные носители данных;
- установка обновлений и патчей;
- управление антивирусной защитой;
- замена оборудования и ПО;
- создание и восстановление резервных копий;
- действия в случае инцидентов.

Формирование защищенной технологической сети заключается в использовании принципа зашиты в глубину. Согласно этому принципу зашита сета передачи данных промышленного предприятия не ограничивается охраной периметра сети с помощью межсетевого экрана. Промышленная сеть должна быть сегментирована, а критически важные участки вынесены в безопасные зоны. Каждая зона должна быть защищена индивидуальным промышленным межсетевым экраном, что обеспечит максимальный уровень безопасности при сохранении необходимых коммуникаций между зонами. Особенность промышленных межсетевых экранов состоит в том, что они оптимизированы для промышленных протоколов MODBUS или OPC. Наличие тонких настроек для фильтрации специализированных протоколов связи позволяет ограничить доступ к критически важным сегментам сети.

Кроме технических решений по обеспечению кибербезопасности большое внимание должно уделяться организационным проблемам, в частности работе с персоналом. Персонал предприятия должен владеть средствам и регламентам информационной безопасности. Он должен быть ознакомлен с выработанными политиками, процедурами и

стандартами. Учитывая тот факт, что специалисты АСУ ТП имеют ограниченное понятие об обеспечении IT-безопасности промышленного сектора, важно донести значение этого вопроса, сформировав обязательную программу, которая реализуется на предприятии. Различные категории персонала должны быть ознакомлены с теми ролями, которые относятся к их зоне ответственности. К примеру, персонал можно разделить по категориям: посетители, подрядчики, операторы, инженеры, обслуживающий персонал, управленцы. Персонала первой категории (посетители) должен быть проинструктирован о том, какие действия разрешены и запрещены. На производственном участке, инженерный состав должен уметь обращаться со средствами обеспечения безопасности, управленцы обязаны знать алгоритмы действий при возникновении угроз безопасности систем АСУ ТП.

Сегодня главной проблемой в обеспечении кибербезопасности промышленных объектов в России даже при наличии соответствующих методик и средств является слабое понимание специалистами АСУ ТП критической важности внедрения этих средств. 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. В России пока нет обязательных стандартов промышленной кибербезопасности. Сейчас не существует единой, простой и понятной методики, в которой специалисту по информационной безопасности были бы предложены шаги, необходимые для обеспечения достаточного уровня защищенности своей АСУ ТП.

Кроме всего прочего свое негативное влияние оказывает существующая на сегодняшний момент сложная бюрократическая процедура внесения изменений в работу ответственных технологических узлов. 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, к сожалению, в основном сводится к ограничению доступа пользователя по паролю, который нередко хранится в открытом виде в базе данных 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 кодом. В то время как на сайте производителя находится свежая прошивка, в которой уже может быть закрыт ряд известных проблем с информационной безопасностью, их наличие

никто не проверяет даже на этапе развертывания системы просто потому, что этого никто не требует.

Нужно учитывать и то, что, автоматизацией технологических процессов, как правило, занимаются не сами предприятия, а сторонние фирмы-подрядчики, которые, в первую очередь, заинтересованы в реализации лишь функциональной составляющей проекта, поскольку это те самые свойства системы, за которые они получают деньги. В этой связи грамотная реализация функций информационной безопасности для них подразумевает лишние затраты. Таким образом, заказчик должен понимать необходимость обеспечения кибербезопасности, ставить перед подрядчиками соответствующие задачи и контролировать их выполнение.

ЛИТЕРАТУРА

1. Шишов О. В. Технические средства автоматизации и управления: учеб. пособие. – М.: ИНФРА-М, 2011. – 397 с.

2. Шишов О. В. Современные технологии промышленной автоматизации: учеб. пособие. – Саранск: Изд-во Мордов. ун-та, 2009. – 276 с.

3. Шишов О. В. Современные технологии автоматизации: электрон. учеб. – Саранск: Мордов. ун-т., 2008. – ФГУП НТЦ «Информрегистр». Депозитарий электрон. изд. № 0320802194.

4. Шишов О. В. Конфигурирование, программирование и работа в сети базовых копонентов систем промышленной автоматизации: лаб. практикум. – Саранск: Изд. ИП Афанасьев В. С., 2014. – 160 с.

5. Шишов О. В., Бобров М. А. Общие проблемы оптимизации структур и ресурсов распределенных систем управления // Технические науки: тенденции, перспективы и технологии развития: Сб. науч. тр. междунар науч.-практич. конф. – Волгоград, 2014. – С. 14–15.