УДК 621.3

Промышленные сети в условиях возросших киберугроз

Плешко Д. Ю.
Научный руководитель – САПОЖНИКОВА А. Г.

В условиях интеграции систем АСУ ТП с локальными сетями *Ethernet* и сетью *Internet* важным вопросом становится сетевая безопасность, устойчивость сети предприятия к возможным хакерским атакам и проникновению вредоносного ПО. В 2010 году промышленные системы автоматизации тяжело пережили атаку уже широко известного компьютерного вируса *Stuxnet*. Это событие было самым широко освещаемым в профильных СМИ, но не стало единственным: с того момента промышленные сети и системы стали одной из основных целей для кибератак.

Даже если род деятельности промышленного предприятия не связан с критически важными процессами (энергетика, транспорт, оборонная промышленность), большинство технологических процессов автоматизировано с помощью *SCADA* (система диспетчерского управления и сбора данных) или типовых систем автоматического управления. Такие системы в последние годы стали подвержены атакам вредоносного ПО не меньше, чем «традиционные» финансовые и правительственные структуры. Отличие лишь в том, что атаки, направленные на промышленные системы, как правило, не регистрируются и их последствия обычно выглядят как сбои в работе, не связанные с действиями какого-либо вредоносного ПО.

Ещё в недалеком прошлом системы управления использовали закрытые протоколы передачи данных и различные полевые шины, не связанные напрямую с информационной сетью предприятия и *Internet*. Таким образом, безопасность технологической сети обеспечивалась методом её изоляции. За последнюю декаду промышленные сети мигрировали с собственных технологий и стандартов на готовые коммерческие решения и технологии. Несмотря на то что адаптация стандарта *Ethernet* к промышленному использованию сначала протекала медленно, сейчас с появлением протоколов *Real-time Ethernet* (гарантированной доставки пакета данных в заданный промежуток времени) и технологий резервирования каналов связи (автоматического восстановление сети после сбоя) Ethernet становится стандартом де-факто.

В дополнение к этому возрастает потребность в *online* доступе к технологическим данным извне, что означает необходимость прямого соединения технологической сети связи с информационной сетью предприятия и сетью *Internet*. Работа современной технологической сети требует постоянного удалённого доступа, обновлений, то есть обмена данными, и как результат технологическая сеть предприятия больше не может быть изолированной от общей сети.

Конечные устройства в технологической сети, такие как ПЛК или распределённые системы управления, проектировались с фокусом на максимальную надёжность. В то же время встроенные в них средства защиты от несанкционированного доступа по сети находятся на начальном уровне, недостаточном для защиты от современных угроз. Работая в безостановочном режиме, в жёстко 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 от основного был так называемый человеческий фактор или сбои в сети. Соответственно, промышленное оборудование для автоматизации (ПЛК, распределённые системы, блоки телеметрии) не рассчитано на паразитный или неспециализированный сетевой трафик. Для обеспечения надёжности производства специализированные промышленные межсетевые экраны используются для разрешения только необходимого для функционирования трафика.

Риск кибератак извне, особенно нацеленных на промышленные системы связи, практически не брался в расчёт, однако возросший в новом тысячелетии уровень терроризма, особенно с применением кибероружия, заставляет взглянуть на проблему по-иному. Переломным моментом стала атака на ядерный комплекс по обогащению урана *Natanz* в Иране, проведённая с помощью вредоносного ПО (компьютерного вируса) *Stuxnet* в 2010 году. Физическое разрушение турбин реакторов показало, что урон от кибератаки может быть более чем реален.

Вирус *Stuxnet* успешно преодолел изолированность технологической сети связи от общей сети с помощью пресловутой *USB*-флэшки. Открытие данного вируса и публикация механизма его действия привело к некоторым изменениям. Возникло новое направление – промышленная сетевая безопасность. Уже в 2011 году было исследовано и опубликовано множество уязвимостей промышленных систем управления, исходных кодов вредоносного ПО – больше чем за 10 прошлых лет. Также появилось новое, более устойчивое вредоносное ПО. На основе вируса Stuxnet образовался новый класс вредоносного ПО, известный как *APT* (*Advanced Persisitent Threats* – целенаправленные устойчивые угрозы). В отличие от вируса Stuxnet, который был нацелен на остановку технологического процесса и порчу технологического оборудования, ПО типа *APT* сфокусировано на промышленном шпионаже и краже бизнес-информации. Данный тип вирусов тяжело поддаётся обнаружению, ПО может скрытно собирать информацию годами и в итоге нанести не менее тяжелый ущерб финансам или репутации предприятия, чем иная авария на производстве. В финансовой сфере вредоносное ПО такого характера бытует уже годами, но в промышленной сфере это явление новое. Например, вирус с названием *Night Dragon* был пойман на краже финансово-экономической информации у нефтехимических компаний в Северной Америке, в том числе сведений о заключённых сделках по продаже энергоносителей, о коммерческих предложениях по поставке нефти, будущем сейчас самое время позаботиться об усилении мер кибербезопасности на промышленных объектах.

Успешная кибератака на промышленную систему может повлечь за собой производственные потери, урон системе безопасности и окружающей среде, кражу интеллектуальной собственности, включая информацию из корпоративной сети предприятия. Также взлом промышленного сегмента сети образует «дверь» в общую корпоративную сеть предприятия. В условиях поточного производства промышленное оборудование работает в безостановочном режиме с минимальными периодами простоя и временем жизни от 10 до 20 лет. Для повышения уровня кибербезопасности сети технологического оборудования, занятого в поточном производстве, повсеместная замена оборудования – невыгодный вариант.

Способы повышения промышленной сетевой безопасности базируются на принятом стандарте *ISA IEC* 62443 (ранее *ISA*99). Он относится к промышленной безопасности в общем, без привязки к какому-либо вертикальному рынку (отрасли). Ведущие нефтегазовые и химические компании, такие как *Exxon, Dow* и *Dupont* весьма успешно построили систему безопасности своих промышленных систем на базе этого стандарта.

Отдельные отрасли тоже имеют свои собственные стандарты сетевой безопасности, например, стандарт *NERC CIP* для североамериканской энергетики. Корпорация *NERC* (*North American Electric Reliability Corporation*) не только разрабатывает стандарты безопасности, но и регламенты по её обеспечению, систему сертификации персонала. В отличие от стандарта *IEC* 62443, сертификация по которому является добровольной процедурой, *NERC CIP* обязателен в США.

Далее, резюмируя стандарты безопасности, выделим 7 шагов для обеспечения безопасности *SCADA* и систем управления.

Шаг 1: Оценка рисков для систем управления производством.

Оценку рисков для конкретного производства стоит начать с выделения типовых угроз для систем управления промышленным производством: несанкционированный удалённый

доступ; атаки через офисную корпоративную сеть (*firewall*); атаки на промышленные системы посредством поиска уязвимостей (*Simatic Win CC*); (*D*)*DoS*-атаки; саботаж и ошибки персонала; внедрение вредоносного кода на переносных и внешних носителях; чтение и перезапись команд управления (ПЛК); несанкционированный доступ к ресурсам; атаки на сетевые устройства; технические сбои и форс-мажорные события.

Данный шаг применительно к конкретной системе безопасности выполняется в два этапа: анализ рисков и ранжирование их по степени тяжести возможных последствий. Оценка рисков производится для каждой системы управления в отдельности и зависит от степени вероятности и от тяжести последствий наступления каждого случая.

При анализе уязвимостей также следует учитывать различия в подходах к обеспечению безопасности в корпоративных сетях и в промышленных системах управления.

Шаг 2: Выработка правил и процедур по информационной безопасности. Хотя политики безопасности в каждой организации свои, некоторые пункты в них должны быть упомянуты обязательно: удалённый доступ; портативные носители данных; установка обновлений и патчей; управление антивирусной защитой; замена оборудования и ПО; создание и восстановление резервных копий; действия в случае инцидентов.

Шаг 3: Обучение персонала средствам и регламентам информационной безопасности. Данный шаг проводится в два этапа. Первый – ознакомление персонала с выработанными политиками, процедурами и стандартами. Учитывая тот факт, что специалисты АСУ ТП имеют ограниченное понятие об обеспечении ИТ-безопасности промышленного сектора, важно донести значение этого вопроса, сформировав обязательную программу, которая реализуется под контролем начальства. Второй этап – проведение тренингов для персонала, раскрывающих непосредственно механизм применения политик безопасности. 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. Персонал 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.

Шаг 4: Формирование технологических сетей передачи данных. Industrial Ethernet становится стандартом де-факто в технологических сетях связи. Технологическое оборудование использует протоколы на базе *IP*, в том числе стандартные *TCP/IP*, *UDP*, наследуя тем самым все их уязвимости. С возникновением необходимости взаимодействия систем производственно-технологического управления (*SCADA/DMS*) с *ERP/MES*-системами верхнего уровня стала невозможной изоляция промышленного контура сети. Кроме связи с корпоративной сетью, необходимо учитывать интерфейсы удалённого управления и *USB*-порты рабочих станций как возможные дополнительные пути проникновения вредоносного ПО.

Формирование защищённой технологической сети заключается в её сегментации. Каждый сегмент образует зону, защищённую на нескольких уровнях от различных киберугроз. Такие зоны включают в себя физический или логический набор оборудования с идентичными требованиями к безопасности. Обмен данными между зонами осуществляется только по защищённым каналам связи (путям), все типы данных, проходящих по ним, должны быть регламентированы, а любой неописанный трафик запрещён. Соответственно, любая возможность электронного обмена данными должна осуществляться только через зарегистрированный путь. Основными технологиями защиты путей являются межсетевые экраны и *VPN*-каналы. Детально эти процессы описаны в стандарте *ANSI/ISA*99.

Шаг 5: Регламенты доступа персонала к системам управления. После определения зон и путей и обеспечения их информационной безопасности следует позаботиться о контроле физического и логического доступа к критически важному оборудованию. Физический

контроль доступа – понятное для понимания мероприятие, заключающееся в иерархической системе доступа в кабинеты с помощью замков и ключей. Как и в случае с межсетевыми экранами, идея состоит в том, чтобы доступ к критически важному оборудованию имел лишь тот персонал, которому это необходимо для работы.

Логический контроль доступа предполагает действия по следующим пунктам:

– аутентификация и авторизация пользователей;
– ролевой контроль доступа;
– лист привилегий;
– журналы контроля доступа;
– технологии *Active Directory, Radius, ldap,* др.;
– отслеживание изменений.

Шаг 6. Контроль функционала производственных систем. Усиление безопасности компонентов системы подразумевает запрещение всех ненужных функций, отключение не используемых для работы компонентов и функций операционной системы (например мультимедийных), отключение всех лишних коммуникационных интерфейсов и связанных с ними сервисов (например *Web*-сервера на ПЛК, если он не используется).

На рабочих станциях должно быть установлено антивирусное ПО, а операционные системы и программы обновлены с помощью официальных пакетов обновлений (патчей). Контроль актуальности антивирусных баз и обновления системы должен производиться в соответствии со специальным регламентом. Немаловажным средством для выявления уязвимостей является специализированное программное обеспечение типа *Nessus* или *Bandolier*. Данное ПО проверяет систему на наличие известных уязвимостей и правильной конфигурации серверов и рабочих станций, исходя из соображений безопасности. Однако тестирование работающей системы проводить не рекомендуется.

Шаг 7: мониторинг и управление системой информационной безопасности. Постоянный сетевой мониторинг должен быть неотъемлемой частью работы оператора системы. Этот процесс подразумевает множество действий, в том числе установку обновлений ПО и антивирусных баз, мониторинг сети на подозрительную активность. Последнее может проводиться, например, путём анализа *log*-файлов на неавторизованную активность. Также существуют специальные технологии под общим названием «Системы обнаружения вторжений (СОВ)», или в оригинале *Intrusion Detection Systems* (*IDS*). СОВ тоже не является панацеей и не в состоянии защитить систему управления от любого вредоносного ПО, это только часть стратегии защиты в глубину.

Важно использовать технологии и решения, предназначенные именно для промышленного сектора. Жёсткие условия эксплуатации, опыт персонала, уникальные протоколы связи и фокус на безопасность и надёжность приводят к различию требований промышленной и ИТ-безопасности.

Литература

1. Фаронов, А. Е. Основы информационной безопасности при работе на компьютере / А. Е. Форонов. – М. : ИНУИТ, 2016. − 155 с.

2. Добротун Е. Б. Построение модели угроз безопасности информации в автоматизированной системе управления критически важными объектами на основе сценариев действия нарушителя / Е. Б. Добротун. – М. : Инсайд, 2016. − 42 с.