Контроль привилегированных пользователей в АСУ ТП

В руках так называемых суперпользователей находятся важнейшие информационные потоки, поэтому управление привилегированными учетными записями – ключевой аспект информационной безопасности автоматизированных систем.

Дмитрий СЛОБОДЕНЮК, коммерческий директор, ARinteg

Практика показывает, что в восьми из десяти случаев потеря конфиденциальной информации происходит по внутренним причинам. Большая часть нарушений ИБ приходится на привилегированных пользователей, что неудивительно, поскольку привилегированная учетная запись открывает расширенный доступ к информационным ресурсам и сервисам, сетевым устройствам и операционным системам.

Современные системы автоматизированного управления заняты в обслуживании критически важных объектов стратегических отраслей экономики, а количество угроз и кибератак на промышленные объекты увеличивается. Однако защищенность этих систем находится на весьма низком уровне, более того, у системных интеграторов нет четкого представления об особенностях обеспечения безопасности АСУ ТП.

Напомним типовую структуру систем, обслуживающих технологический процесс предприятий.

- Нижний уровень, или уровень управляющих устройств. Представлен первичными измерительными приборами, нормирующими преобразователями, локальными автоматическими регуляторами.
- Средний уровень, или уровень технических средств АСУ ТП. Представлен контроллерами и управляемыми автоматическими регуляторами.
- Верхний уровень, или уровень оперативного персонала АСУ ТП. На этом уровне задействован оператор, который запускает технологический процесс и может остановить его полностью или частично.

Программный пакет диспетчерского управления и сбора данных (supervisory control and data acquisition, SCADA) – важная часть АСУ ТП – базируется на широко распространенных платформах Microsoft Windows Embedded Edition или Linux и является самым уязвимым местом в архитектуре, через которое злоумышленники получают доступ к технологическому процессу. Для защиты периметра и обеспечения безопасности АСУ ТП компании-интеграторы активно применяют межсетевые экраны, системы предотвращения вторжений, средства анализа защищенности и изменений ПО. Системы обнаружения вторжений реагируют на попытки использования уязвимостей как на периметре сети, так и в центре обработки данных, и нейтрализуют их. Для контроля степе-

Инструмент контроля доступа привилегированных пользователей

Для эффективного контроля доступа к информационным ресурсам и управления учетными записями пользователей (Identity and Access Management, IAM) сегодня разработаны специализированные продукты. В них применяется строгая аутентификация пользователей, построенная на использовании криптографии и инфраструктуры открытых ключей. С привилегированными учетными записями ситуация осложняется тем, что одной учетной записью одновременно могут пользоваться несколько сотрудников. Поэтому управление сводится к точной идентификации пользователя, работающего под учетной записью администратора в конкретный момент времени.

Для управления привилегированными учетными записями существуют специальные мониторинговые системы, обеспечивающие безопасный доступ с правами администратора к корпоративным ресурсам. Компоненты такой системы регистрируют все активности в рамках сеанса привилегированного доступа: определяют время обращения к конфиденциальным данным, имя пользователя, ведут журнал выполненных действий. Мониторинг активностей делает работу привилегированных пользователей прозрачной, так как позволяет точно знать, для чего они используют свои права. Системы поддерживают двойной контроль доступа по принципу «четырех глаз», который позволяет избежать ошибок, вызванных человеческим фактором. Действия привилегированного пользователя отслеживаются и контролируются администратором в режиме реального времени. Таким образом, по результатам внутренних проверок можно точно указать, кто и как совершил ошибку, а также предъявить доказательства неправомерных действий, что становится актуальным, если речь идет о финансовых убытках и возбуждении уголовных дел.

ни защищенности АСУ ТП служат средства анализа изменений ПО, которые исследуют исходный код приложений на соответствие требованиям регуляторов, автоматически описывают несоответствия и выдают рекомендации по их устранению.

Предотвращение инцидентов безопасности невозможно без детального изучения технологических процессов конкретного предприятия. Разработка и реализация таких решений – процесс сложный и многопараметрический, требует индивидуального подхода ко всей структуре АСУ ТП. Для обеспечения безопасности верхнего уровня необходимы регламентирующие положения и внутрикорпоративные стандарты, учитывающие специфику бизнеса и территориальную распределенность компании. К сожалению, сегодня полноценных отечественных решений для защиты АСУ ТП нет. Для комплексной защиты всех уровней АСУ ТП многие отечественные предприятия промышленного сектора идут по пути создания единого информационного пространства для департаментов автоматизации и ИТ-безопасности. Это так называемое встречное движение обусловлено тем, что люди, работающие с АСУ ТП, не соблюдают политику информационной безопасности, а специалисты по информационной безопасности, в свою очередь, не разбираются в специфике технологических процессов. При этом из поля зрения выпадает тот факт, что защита АСУ ТП и защита информации – два совершенно разных процесса (см. таблицу). В первом случае объектом обеспечения безопасности выступает непрерывность технологического процесса, а во втором – сохранность данных. Кроме того, системы информационной безопасности АСУ ТП из-за отраслевой специфики технологических проектов промышленной автоматизации сильно отстают от корпоративных информационных систем.

Различия информационной безопасности ИТ-инфраструктуры и АСУ ТП

Аспекты информационной безопасности	Традиционные ИТ-системы	АСУ ТП
Антивирус	Широко применяется / общая практика	Сложно реализуется / применяется редко
Жизненный цикл технологий	Три–пять лет	До 20 лет и более
Аутсорсинг	Широко применяется / общая практика	Используется редко
Установка патчей	Регулярно / по расписанию	Происходит долго / делается редко
Управление изменениями	Регулярно / по расписанию	Наследуемые системы (плохая реализация требований ИБ)
Контент, критичный ко времени	Задержки допустимы	Задержки критичны
Доступность	Задержки допустимы	24 x 365 (непрерывно)
Повышение осведомленности персонала	Организовано неплохо	Обычно слабо
Аудит	Планируется и организуется третьей стороной	Время от времени (после сбоев)
Физическая безопасность	Обеспечивается	Реализуется неплохо, но часто удаленно и автоматизированно

Перечисленные выше средства обеспечения безопасности направлены в основном на защиту нижних уровней, делая акцент на сохранности данных, в то время как самый критичный сценарий разворачивается, если в результате несанкционированного доступа в руках злоумышленников оказывается возможность управления этими данными. Тогда в зависимости от профиля деятельности предприятия можно изменить транспортные потоки, спровоцировать аварии ТЭЦ или ГЭС, вызвать чрезвычайную ситуацию и подорвать национальную безопасность. Огромный финансовый ущерб могут нанести неправомерные действия привилегированных пользователей, которые обладают практически неограниченными правами. Например, если меняются маршруты движения опасных грузов через глобальную навигационную спутниковую систему или происходит хищение составов, перевозящих цветные металлы, нефтепродукты или газ, то потери в денежном эквиваленте будут несопоставимы с ущербом от внешних атак. Кроме того, в силу специфики АСУ ТП действия привилегированных пользователей могут оставаться неизвестными в течение длительного времени. Поэтому одно из ключевых направлений информационной защиты АСУ ТП – контроль привилегированных пользователей.

По оценкам аналитиков, в ближайшее время решения для управления привилегированными учетными записями достаточно глубоко проникнут на рынок, и это неудивительно, так как безопасность бизнеса доминирует над комфортом пользователей.

■ ■ ■

Разработка решений по защите АСУ ТП – это целый комплекс мер, включающий выбор оптимальной архитектуры, обеспечение физической изоляции, четкое выполнение политики информационной безопасности и многое другое. Следует помнить, что цель обеспечения безопасности – непрерывный, правильно построенный технологический процесс. Сегодня вопросы защиты АСУ ТП находятся в фокусе внимания разработчиков, экспертов и государственных органов. Системные интеграторы не могут не реагировать на сложившуюся рыночную ситуацию, поэтому в числе приоритетных задач – разработка эффективных и скоординированных мер по защите автоматизированных систем. ИКС