ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ SCADA В ЭПОХУ «ИНТЕРНЕТА ВЕЩЕЙ»

ЭД НЬЮДЖЕНТ (ED NUGENT)
МАЙК РЭТТ (MIKE RATTE)

По мере того как индустриальный «Интернет вещей» (Industrial Internet of Things, IIoT) играет все более важную роль, меняется и традиционное использование программного пакета автоматизированной диспетчерской системы управления технологическим процессом — SCADA (Supervisory Control and Data Acquisition). Системы SCADA изначально не были предназначены для выполнения требований кибербезопасности, поэтому сегодня предприятиям нужно как-то приспосабливаться к новой реальности.

SCADA, а также более широкие системы управления производством — ICS (Industrial Control System), которые включают в себя SCADA, человеко-машинные интерфейсы (Human-Machine Interface, HMI), системы управления и обслуживания здания (Building Management System, BMS), системы оперативного управления производством (Manufacturing Execution System, MES), а также компьютеризированные системы управления техническим обслуживанием (Computer Maintenance Management System, CMMS), — решают задачи в области конкретных присущих им технологий, традиционно изолированных от инфраструктуры корпоративных информационных технологий (ИТ). Соответственно, эти платформы изначально не были разработаны с целью обеспечения требований по кибербезопасности.

Сегодня традиционная роль систем управления производством расширилась. Она стала не только включать в себя обеспечение предприятия информацией, в том числе ее обработку, но и отвечать на указания от ERP — системы планирования ресурсов предприятия (Enterprise Resource Planning; подразумевает полное планирование ресурсов, управления и оптимизации, начиная с момента поступления заказа и заканчивая поставкой продукции). Если рассматривать все это в целом, как законченную систему, то мы увидим потенциальные киберугрозы для таких систем, что и было наглядно продемонстрировано в проведенном Центром по защите национальной инфраструктуры анализе «Обеспечение перехода на IP-основе SCADA / PLC сети», который строился на обзоре четырех лучших практических решений сетей SCADA на основе IP-адресов [1]. Сейчас, когда акцент в сфере подключаемых технологий сфокусирован на «Интернете вещей» и тесно связанных с ним индустриальном «Интернете вещей» (IIoT) или «Индустрии 4.0», у производителей есть огромное потенциальное преимущество в стратегии агрегации данных и ситуационной осведомленности. Но поскольку IIoT-устройства используют протоколы Интернета (IP), это увеличивает их подверженность кибератакам.

Все преобразования, связанные с IIoT, изменяют роль традиционной диспетчерской с ее тенденцией к использованию мобильных устройств для контроля и управления [4]. Возникающий при этом в системах управления производством с поддержкой IIoT контекстный компонент человеко-машинного интерфейса обеспечивает повышение производительности для организаций, эксплуатирующих и обслуживающих системы управления производством, при одновременном расширении периметра этих систем. Однако необходимо добавить в систему и элементы защиты от киберугроз.

ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ

Чтобы система менеджмента качества соотвествовала уровню требований ISO 9001 в области разработки

и выпуска продукции, поставщики современных программных платформ систем управления производством включают в них элементы управления кибер-рисками (Cyber Risk) и устойчивостью (Resilience Management), разработанные Software Engineering Institute (Институт программной инженерии Карнеги-Меллон, США). Их цель состоит в том, чтобы обеспечить необходимую прозрачность внутренней или внешней уязвимости и при этом достаточно быстрое реагирование на угрозу для минимизации риска для клиентов.

Участие в процессе обеспечения кибербезопасности таких организаций в области стандартизации, как Институт инженеров электротехники и электроники (IEEE) и Международная электротехническая комиссия (IEC), посредством открытого обсуждения проблем и соответствующей обратной связи, призвано содействовать достижению должной прозрачности. Их деятельность имеет решающее значение для быстрого претворения в жизнь исходящих от них рекомендаций. Так, Национальный институт стандартов и технологий США (NIST) предоставил схему, которая имеет большое значение для систематического определения критически важных активов организации, обеспечения их безопасности и выявления угроз [4]. Эта схема состоит из четырех базовых элементов (рисунок): идентификации, защиты, обнаружения и реагирования.

РАСПОЗНАВАНИЕ И ИДЕНТИФИКАЦИЯ ПОДОЗРИТЕЛЬНОГО ПОВЕДЕНИЯ

Приведем пример: перед Бостонским марафоном 2016 г. Национальная администрация по ядерной безопасности (NNSA) провела оценку фонового излучения по всей дистанции с использованием низколетящих вертолетов. Такие измерения естественного фонового излучения для установки базовых уровней являются нормальной составляющей обеспечения безопасности и готовности к чрезвычайным ситуациям [4].

Поэтому и для определения базового нормального поведения ICS крайне важно заблаговременно провести инвентаризацию активов и потоков данных. Промышленные сети могут быть большими и сложными, а их протоколы отличаются от тех, что применяются в корпоративных ИТ-сетях. Решением вопроса может стать использование автоматизированных инструментов, которые отображают и контролируют сетевое оборудование с помощью простых протоколов управления сетью (SNMP), тем самым повышая эффективность и точность такой инвентаризации.

Важный фактор в создании надежной базовой линии для ICS — это инструменты инвентаризации и мониторинга, которые являются частью системы управления. Вместе с технологией, которая способна обеспечить базовый шаблон связи между ICS, программируемым логическим контроллером (Program Logic Controller, PLC) и другими элементами управления, большое значение имеет мониторинг ICS. При идеальном раскладе такие системы будут способны на:

- извлечение метаданных из сетевого потока с помощью пассивных датчиков;
- быстрое построение визуализированных списка компонентов и карты соединений;
- изучение ICS и выдачу статистических и поведенческих описаний нормального функционирования системы управления;
- выдачу рекомендаций по принятию необходимых превентивных мер;
- инициацию ответа на инцидент при наличии заданного компромисса.

IIoT-устройства часто обмениваются данными с помощью беспроводных технологий, поэтому, в отличие от обычных ИТ-сетей, сети ICS не используют статический IP-адрес. Когда промышленные сети подключаются к еще более обширной сети — Интернету, системы мониторинга работоспособности ищут изменение или дублирование IP- и MAC-адресов, отслеживают перемещение устройств или переключение кабелей, а также несанкционированные подключения. Кроме того, условия эксплуатации сильно усложняются из-за мобильных датчиков, подключенных через точки беспроводного доступа с динамическими IP-соединениями [6].

ЗАЩИТА РАССРЕДОТОЧЕННОГО ПЕРИМЕТРА

На недавнем саммите Tech Talks в Массачусетсе Майк Ратте обсудил с участниками современное состояние ИТ-безопасности [2]. Главная его мысль: «Идентичность — это новый периметр». Он аргументировал это тем, что:

- почти половина нарушений кибербезопасности вызвана именно скомпрометированными полномочиями;
- хакеры нацелены на все классы пользователей, включая привилегированных пользователей;
- традиционная безопасность на основе периметра недостаточна;
- основа безопасности находится в области контекстных политик.

Эта стратегия хорошо сочетается со все большим рассредоточением периметра ICS, который пользуется преимуществами открытой связи, и поэтому ему пойдет на пользу, если им займутся специалисты по безопасности предприятия.

В связи с тем что 63% подтвержденных нарушений данных связаны со слабыми, дефолтными (установленными по умолчанию) или украденными паролями [8], управление учетными данными занимает одно из первых мест в списке киберугроз для ICS. Возможность физического доступа через украденные или потерянные мобильные устройства также обусловливает необходимость в эффективном управлении учетными данными.

Промышленные сети обеспечивают первый уровень защиты с помощью брандмауэров, виртуальных частных сетей (VPN) и коммутаторов. Поставщик платформы ICS должен шифровать конфигурационные

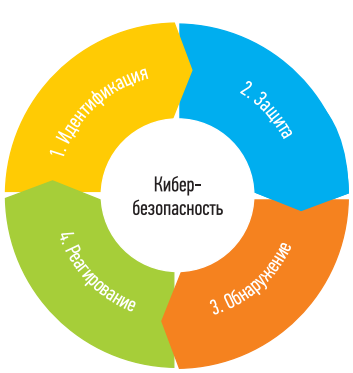

РИС. ◀ Основы кибербезопасности по NIST

файлы, обеспечивать мониторинг необычных попыток подключения, использовать защищенные протоколы, такие как HTTPS, и предоставлять расширенные права пользователя, интегрированные с Microsoft Active Directory. Благодаря этим возможностям платформа ICS может вписаться в мир управления идентификацией как его устойчивая часть. Применяя Active Directory в качестве основного репозитария такого управления, для всех приложений пользователя ICS можно использовать один вход.

В управлении мобильным персоналом краеугольным камнем являются контекстные политики. Права, требующиеся операторам, варьируются в зависимости от их рабочей зоны, а сервер мобильных устройств ICS обеспечивает применение соответствующих жестких контекстных политик, управляя доступом к ресурсам, основанным на географической основе и при этом синхронизируясь с активным каталогом.

Еще один важный момент в решении данной проблемы связан с невозможностью управлять выведенными за рамки системы пользователями и выполнять отключение их учетных записей. Например, у подрядчика, нанятого для работы на объекте, есть возможность иметь временную учетную запись, которая остается открытой и может использоваться в случае, если подрядчику когда-нибудь будет необходимо вернуться на объект. В связи с этим может возникнуть определенная сложность, потому что, когда есть «острова идентичности», трудно распознать, находится ли он (подрядчик) на объекте или вне его. Централизованное управление идентификацией устраняет проблемы с потерянными учетными записями, избавляет от необходимости использования корневых паролей и от упомянутых «островов идентичности». Это значительно упрощает управление и интеграцию учетных данных в соответствии с корпоративными политиками.

ОБНАРУЖЕНИЕ ПОДОЗРИТЕЛЬНОГО ПОВЕДЕНИЯ

С четкой инвентаризацией активов и базовыми шаблонами, отражающими поведение сети и приложений в штатном режиме, система мониторинга промышленной сети будет готова идентифицировать ненормальное состояние системы. Если базовые шаблоны сравниваются в реальном времени с текущим функционированием ICS, то система может генерировать сигналы тревоги и быстро реагировать на угрозу установленного компромиссного поведения.

Существует еще один важный аспект обнаружения ненормальной работы системы, который связан с тенденцией к увеличению мобильности. Управление мобильными устройствами, или MDM (Mobile Device Management), используется предприятиями для развертывания своих политик путем предоставления соответствующих прав своему персоналу. Примером может быть политика отключения камеры устройства на рабочем месте, разрешающая ее включение при выходе за его пределы.

Лучшие в своем классе решения для систем управления обеспечены защитой, позволяющей устройству реагировать на угрозы даже при отключении от сети. Такие системы быстро обнаруживают несанкционированно подключенные и взломанные устройства, а также атаки типа «человек посередине» (тип интернет-атак, при которых злоумышленник перехватывает канал связи, получая полный доступ к передаваемой информации), т. н. состояния тихого взлома и потерянные или украденные устройства и сетевые атаки [9].

МИНИМИЗАЦИЯ УЩЕРБА И ОБЕСПЕЧЕНИЕ ВОССТАНОВЛЕНИЯ СИСТЕМЫ

Для мобильного устройства автоматический ответ на ненормальное поведение включает в себя блокировку или стирание информации устройства, его перезагрузку в безопасное состояние или отключение доступа к сети. Лучшие в своем классе системы также уведомляют о таком инциденте персонал службы безопасности.

При этом крайне важно обеспечить надежное управление в области контроля и сохранения версий программного обеспечения. Это необходимо для того, чтобы после инцидента и его устранения можно было восстановить систему в ранее созданной безопасной контрольной точке. Управление версиями, развернутое на защищенном сервере, помогает поддерживать целостность конфигурации системы и обеспечивает отслеживание любых изменений, внесенных в файлы конфигурации.

К сожалению, восстановление системы до предыдущей версии может, в зависимости от того, где хранятся операционные данные, привести к потере исторических данных. Резервированные контроллеры, сети, исторические серверы и коммуникационные серверы уже давно стали отличительной чертой лучших в своем классе решений SCADA. Этого, однако, недостаточно для предотвращения последствий от киберугроз, которые могут скомпрометировать и первичные, и резервные элементы системы.

Для снижения риска потери данных в системе могут использоваться виртуальные машины, или VM (Virtual Machine), выступающие как хосты ICS. Развертывание на виртуальной машине услуги послеаварийного восстановления в качестве сервиса DRaaS (Disaster Recovery as a Service) позволяет сократить время восстановления системы до 15 минут [7]. Но, поскольку время между вторжением и его обнаружением все равно остается значительным [8], это все еще может привести к потере данных.

На основе всего сказанного можно сделать вывод, что в эпоху «Интернета вещей» самым надежным вариантом защиты от несанкционированного воздействия на системы SCADA и их наилучшей защитой от взломщиков является развитое управление учетными данными. ⬣

ЛИТЕРАТУРА

1. Centre for the Protection of National Infrastructure. Securing the Move to IP-Based SCADA/PLC Networks. London: Centre for the Protection of National Infrastructure. 2011.
2. Centrify Overview and Company Strategy. 2016.
3. National Nuclear Security Administration. NNSA to conduct Aerial Radiation Assessment Survey over Boston area, March 31, 2016 // National Nuclear Security Administration Press Release.
4. Nugent E., Hoske M.T. SCADA cyber security. Control Engineering. July 2015.
5. Nugent E., Bailliencourt P., Kaltenbacher A. The Architecture of the SCADA Mobility Infrastructure. July 28, 2015. www.automation.com.
6. Robles R. J., Kim T.H. Architecture for SCADA with Mobile Remote Components // Proceedings of the 12th WSEAS International Conference on Automatic Control, Modelling and Simulation. 2010. 346.
7. The Always On Enterprise. 2016 // Veeam.
8. Verizon. 2016 Data Breach Investigations Report. 2016.
9. Mobile cybersecurity for remote workforces. 2016 // ViaSat.