ВОСЕМЬ СОВЕТОВ ПО ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ ICS

КИТ МАНДАХИТ (KEITH MANDACHIT)
ШОН КРЕАГЕР (SEAN CREAGER)
ДЖЕЙ СТАЙНМАН (JAY STEINMAN)
ПЕРЕВОД: ВЛАДИМИР РЕНТЮК

Реализация стратегии по обеспечению кибербезопасности как защиты от внутренних и внешних угроз — это ключевой шаг к общей безопасности промышленной системы управления (ICS). Приведенные в статье восемь простых советов помогут промышленным предприятиям уменьшить риск кибератак и их последствий.

В эпоху «умного» производства «Интернет вещей» (Internet of Things, IoT) и то, что мы называем четвертой промышленной революцией (Industrie 4.0), дают нам важные конкурентные преимущества, и для их полной реализации необходимо сетевое подключение в общую систему. Однако такое подключение несет в себе не только новые возможности, но и риски. Некоторые компании смотрят вперед и понимают все проблемы, связанные с кибербезопасностью, а другие не воспринимают это всерьез, пока не столкнутся с последствиями от внешней угрозы и вмешательством, нарушающим функционирование предприятия. Создание надежной стратегии для предотвращения кибератак требует целостного и многоуровневого подхода. Следуя ключевым советам, приведенным ниже, можно получить базу для разработки надежного плана защиты систем управления промышленными предприятиями (Industrial control systems, ICS)[1] от внешних и внутренних угроз, связанных с тем или иным вмешательством через компьютерные сети.

УГЛУБЛЕННЫЙ ПЛАН ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

«Углубленный план», который называют Defense-in-depth (буквально «глубокая оборона» или «эшелонированная защита»), — это термин, используемый для описания стратегии по обеспечению кибербезопасности ICS. Цель такого плана — достижение идеального состояния защиты за счет многоуровневых систем безопасности и контроля доступа. Чтобы его реализовать, следует начать с идентификации внутренних, внешних, физических и виртуальных угроз для конкретной системы управления. Необходимо оценить, насколько большой риск влечет за собой каждая угроза, и на основе этого выяснить, как наилучшим образом распределить бюджет для претворения в жизнь плана по кибербезопасности.

После проведения анализа можно составить комплексный план по смягчению этих рисков до приемлемого уровня, который, естественно, будет отличаться в зависимости от конкретного объекта. Далее следует понять, какой должна быть реакция на каждую потенциальную угрозу или вмешательство, если они станут реальностью. Не стоит забывать и про необходимость тщательно планировать мониторинг системы и оповещения, чтобы уведомлять пользователей о том, что нарушение происходит в данный момент времени или уже произошло.

СОВЕТ ПЕРВЫЙ: СЕГМЕНТАЦИЯ

Сегментация — одна из стратегий углубленной защиты, направленная на то, чтобы уменьшить размер ущерба, который может быть нанесен в случае какого-либо нарушения. В основе этого подхода лежит принцип разделения сети. Сегментация для предотвращения нежелательного доступа и ограничения уязвимости системы создает в рамках большей (общей) сети изолированные, автономные сети (сегменты, отсюда и название стратегии). Сегментацию можно реализовать физически, используя дополнительные аппаратные средства, такие как кабели и коммутаторы (рис.), но это трудоемкий и весьма дорогостоящий подход.

Как правило, изолированные сети создаются в более крупной системе с использованием виртуальных локальных сетей (virtual local area network, VLAN). Цель сегментации может быть очень простой (например, отделить производственную сеть от бизнес-сети) или более сложной — обеспечить отдельные сегменты для каждой производственной ячейки. Так, в фармацевтической промышленности каждая производственная ячейка или упаковочная линия могут быть сегментированы друг от друга. Если сетевые сегменты должны взаимодействовать, то дополнительную защиту может предоставить файервол (firewall) или брандмауэр. Файервол — это межсетевой экран, программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами. Файервол определяет, разрешено ли сетевому трафику проходить далее, и в противном случае его прохождение блокируется.

Если предприятие не локализовано, а разбросано по регионам, то каждый такой сегмент защищает всю систему от потенциально катастрофического отказа. Если же требуется дополнительное разделение, сегменты могут быть созданы уже на каждом заводе такого предприятия, например по отдельности для системы контроля, управления и визуализации.

[1] Согласно определению стандарта NIST SP 800-82 «Guide to Industrial Control Systems», ICS – это общее понятие, используемое для обозначения нескольких типов систем управления, включая системы диспетчерского управления и сбора данных (SCADA), распределенные системы управления (DCS) и др., которые можно встретить в промышленных секторах критически важных инфраструктур.

СОВЕТ ВТОРОЙ: ДЕМИЛИТАРИЗОВАННАЯ ЗОНА

Частным случаем сегментации является так называемая демилитаризованная зона (demilitarized zone, DMZ)[2] между промышленными и производственными системами компании, ее бизнес- и ИТ-сетями или Интернетом. Хотя такой подход не всегда можно реализовать в системах управления, такие демилитаризованные зоны крайне важны для определенных ситуаций. Правильно спроектированная демилитаризованная зона не позволяет трафику проходить через нее в сеть ICS из бизнес-сети или Интернета. В такой системе в качестве посредников для связи внутри зоны выступают серверы или специально назначенные устройства.

СОВЕТ ТРЕТИЙ: РЕГУЛЯРНОЕ РЕЗЕРВНОЕ КОПИРОВАНИЕ И СВОЕВРЕМЕННЫЕ ОБНОВЛЕНИЯ

В целях усиления кибербезопасности крайне важно обеспечить регулярное резервное копирование системы. Для этого необходимо создавать образы всех жестких дисков, резервных виртуальных машин и сохранять конфигурации и программы на специальном устройстве, например с сетевым подключением (network attached storage, NAS). Для дополнительной защиты резервные копии должны быть дублированы на другое устройство за пределами заводской площадки. Независимо от того, насколько эффективна защита системы, она никогда не будет 100%-ной. А резервные копии являются ключом к быстрому и безболезненному восстановлению системы после ее падения. Также следует обновлять системы, используя версии с последними исправлениями, и любые компьютеры, на которых запущены не поддерживаемые извне операционные системы. Для таких устаревших платформ часто публикуется информация о проблемах уязвимости, хотя сами патчи (вставки в программу с целью ее исправления или изменения для улучшения функциональности) через производителя больше не предлагаются.

СОВЕТ ЧЕТВЕРТЫЙ: ПРОГРАММНО-АППАРАТНЫЙ КОМПЛЕКС СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

Некоторые производители выпускают специальные продукты для обеспечения кибербезопасности, ориентированные именно на системы управления. Средства безопасности в виде файерволов имеют специализированное аппаратное и программное обеспечение, соответствующее требованиям ICS. Эти инструменты позволяют задавать правила, определяющие, каким устройствам разрешено связываться с системой и какие порты и протоколы они могут использовать. При этом файервол блокирует связь с существующими устройствами для обеспечения надлежащего потока трафика. Кроме того, такой файервол распознает, передано ли сообщение так, как это предполагается, или нет. Если нет, то трафик блокируется. В дополнение к блокировке трафика могут быть установлены уведомления или соответствующие сигналы тревоги.

СОВЕТ ПЯТЫЙ: РАЗВИТИЕ НАДЛЕЖАЩЕЙ КОРПОРАТИВНОЙ КУЛЬТУРЫ

Решение проблем, связанных с киберугрозами, сочетает в себе не только здравый смысл и регламентный подход, но и наличие определенных знаний. Многие нарушения происходят изнутри и часто непреднамеренно, без злого умысла, что подчеркивает необходимость привлечения персонала предприятия к процессу обеспечения кибербезопасности и проявления должной бдительности. Рекомендуется создать план непрерывного обучения и организовать подготовку будущих сотрудников. Также сотрудникам следует ознакомиться с общей методикой социальной инженерии. Социальная инженерия — это искусство манипулирования людьми, добывание идентификационной, финансовой и прочей ценной информации в ходе общения с человеком путем обмана или злоупотребления доверием. Персонал должен уметь распознавать атаки и угрозы, например, от фишинговых[3] писем или телефонных звонков, которые, как представляется, исходят из вполне легальных источников и направлены на то, чтобы обмануть людей и получить от них доступ к интересующей злоумышленника информации. Следует научить их, на что обращать внимание, на что не кликать мышкой и как избежать других типичных ловушек.

СОВЕТ ШЕСТОЙ: ОГРАНИЧЕННЫЙ ДОСТУП И УНИКАЛЬНЫЕ ПАРОЛИ

Стратегия least-privileges (минимальная привилегия, или ограничение полномочий) позволяет предоставлять сотрудникам доступ только к тому, что им нужно для выполнения своих непосредственных обязанностей. Также необходимо заставить пользовате-

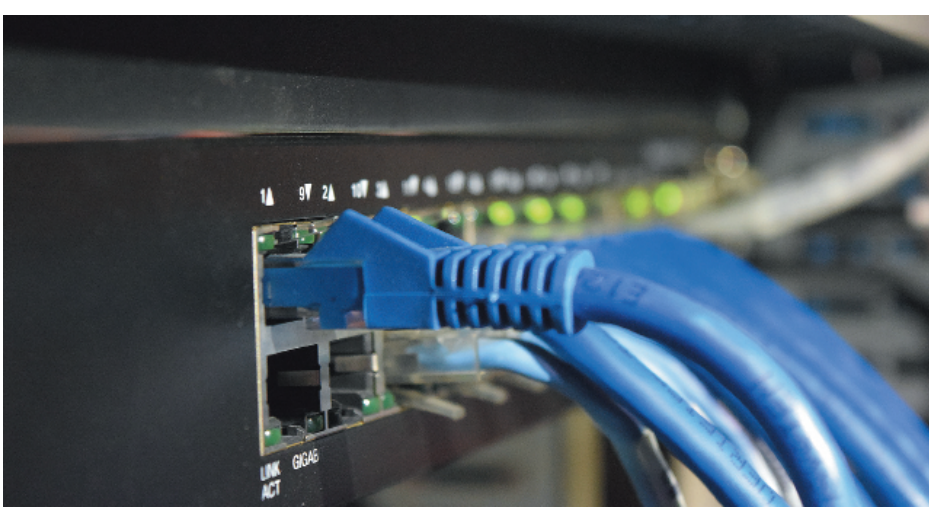

РИС. ▼ Сетевой коммутатор играет важную роль в промышленной системе управления, но это всего лишь один из аспектов многоуровневой архитектуры кибербезопасности

[2] Демилитаризованная зона — операционная среда между внутренним и внешним сетевыми экранами, в которой дислоцируются ПО и аппаратные средства, обеспечивающие доступ к приложениям экстрасети и предотвращающие прямое обращение к внутренней корпоративной сети.

[3] Фишинг — это преступная деятельность интернет-мошенников, действующих под видом благонадежных компаний и юридических лиц с целью незаконного получения секретной информации, например паролей и логинов.

лей использовать уникальные пароли и никогда не оставлять систему с паролем, установленным по умолчанию. Кроме того, пользователи не должны хранить пароли рядом с оборудованием или в другом доступном для неуполномоченного персонала месте. Следует добавить в систему, если это возможно, двухфакторную аутентификацию с использованием таких технологий, как непрерывно изменяющийся код, биометрия и т. д. Такая аутентификация должна быть обязательной для всех устройств, предоставляющих удаленный доступ к внутренней системе управления предприятием.

СОВЕТ СЕДЬМОЙ: ФИЗИЧЕСКАЯ ЗАЩИТА

Надлежащие меры по обеспечению физической безопасности часто игнорируются, однако пренебрегать ими не стоит. Организацию физической защиты от несанкционированного доступа рекомендуется начинать непосредственно с входа в объект. Необходимо определить, как для критически важных инфраструктурных систем, таких как серверы и пункты диспетчерского управления и сбора данных (supervisory control and data acquisition, SCADA), эффективнее использовать охранные системы, системы контроля доступа, огражденные периметры и заблокированные двери. Ключи на программируемых логических контроллерах, которые позволяют изменять программу, должны быть удалены, если они доступны, а блоки управления, чтобы предотвратить доступ к ним неавторизованных пользователей, заблокированы. Также следует отключить или заблокировать все USB-порты системы управления.

Не забывайте, что через доступные USB-порты в систему управления могут быть переданы и внедрены вирусы или могут быть украдены ценные данные. Сотрудники могут непреднамеренно поставить под угрозу безопасность объекта, просто заряжая через них мобильные телефоны.

СОВЕТ ВОСЬМОЙ: ОТНОШЕНИЯ С СИСТЕМНЫМИ ИНТЕГРАТОРАМИ

Еще одна пара глаз, которая знает системы автоматизации компании внутри и снаружи, не помешает — более того, это поистине бесценное достояние. Например, в прошлом году против компаний во всем мире была развернута целая серия угроз и последующих вымогательств. Доверенный системный интегратор может помочь в ходе или уже после кибератаки и обеспечить быстрое восстановление системы. Естественно, это возможно только в том случае, если системный интегратор обладает глубокими знаниями о приложениях, процессах и процедурах ICS клиента, а также имеет полную документацию по ее программному обеспечению, включая недавние резервные копии.

Что касается реализации стратегии по обеспечению углубленной кибербезопасности, то она не обязательно должна быть дорогостоящей и трудоемкой. Нужно помнить, что несколько средств защиты значительно повысят уровень безопасности для ICS. При этом свою роль также может сыграть системный администратор. Поэтому при разработке и установке желаемого типа технологий кибербезопасности системные интеграторы систем управления должны работать в тесной связке с ИТ-отделом заказчика. Кроме того, они могут помочь и в проведении обучения или, если это потребуется, выступить в качестве советчика. ⬣