Сети управления. Поддержка доступности сетей при кибератаке

Обзор

Сети управления и промышленные системы управления контролируют самые разные системы — от производства электроэнергии и автоматизации производственных линий до кондиционирования зданий и многих других процессов. При этом для них характерен ряд уникальных особенностей, в том, что касается обеспечения информационной безопасности. Cisco понимает это и помогает защитить сети управления до, во время и после атаки — без малейшего ущерба для их надежности.

Если говорить о кибербезопасности, сети управления подвержены тем же угрозам, что и другие корпоративные сети. Однако многие промышленные системы управления разрабатывались в ту эпоху, когда для защиты сетей управления было достаточно физически отделить («изолировать») их от корпоративных сетей. Предполагалось, что этого достаточно: если система подключена к такой сети управления, то задавать дополнительные разрешения для нее уже не требуется. Однако программный червь Stuxnet, способный вредить в изолированной сети управления, показал, что изоляция как метод кибербезопасности больше не эффективна.

Здесь важно учитывать, что если решение по кибербезопасности защищает корпоративную сеть, это еще не значит, что оно подходит для сети управления. У тех, кто администрирует эти сети, разные приоритеты. ИТ-специалисты, как правило, следят за конфиденциальностью, целостностью и доступностью систем — именно в таком порядке. Однако от сетей управления в первую очередь требуется доступность, а потом уже целостность и конфиденциальность, ведь сбой в таких сетях ставит под угрозу жизни людей и безопасность окружающей среды. Вот почему первостепенное значение имеют доступность и надежность.

Еще один момент — простота использования. Довольно часто кибербезопасность является лишь одной из множества функций, за которые отвечают специалисты по операционным технологиям (ОТ). Поэтому им требуются интуитивно понятные решения по кибербезопасности с минимальными требованиями в части управления.

Полный цикл атаки и глубокая оборона

Многие годы предполагалось, что главное — защитить периметр сети, чтобы злоумышленники не могли проникнуть внутрь. Тому, что происходило внутри предприятия, уделялось совсем мало внимания, и многим организациям такой подход сослужил плохую службу. Как бы ни эффективна была хорошая, мощная стена, она защищает лишь от определенных видов атак. Достаточно просто оставить дверь открытой (намеренно или случайно), как самые мощные стены становятся бесполезными.

Именно поэтому парадигма сегодня изменилась. Рано или поздно злоумышленник проникнет в сеть, поэтому необходимы методы глубокой обороны, чтобы минимизировать ущерб. Данный подход включает в себя многоуровневую и мультитехнологическую стратегию защиты объектов организации, которые наиболее важны с точки зрения бесперебойного снабжения, непрерывности производства и анализа рисков.

Еще одной важной вехой в представлениях о безопасности является осознание того факта, что кибербезопасность — это не разовая мера от случая к случаю. Ее скорее следует рассматривать как непрерывный, постоянно развивающийся процесс. Поэтому стратегия компании Cisco строится по принципу полного цикла атаки.

Полный цикл можно разделить на три этапа: до, во время и после атаки, — каждый из которых состоит из ряда отдельных операций. К примеру, когда злоумышленник исследует сеть и планирует вторжение, это этап «до атаки», а когда он уже проник в сеть и уничтожает данные — это «во время атаки». Но многие забывают о третьем этапе, «после атаки», когда злоумышленники могут прятаться в течение нескольких дней, недель или месяцев, пока не завершат свою миссию и не создадут плацдарм для последующих вторжений. Если мы не хотим повторения неприятной ситуации, противодействие атаке не может ограничиваться лишь обнаружением и блокированием. Постоянный анализ после атаки критически важен для минимизации ущерба и подготовки к отражению следующей атаки. Чтобы защитить сеть на всех этапах атаки, Cisco обеспечивает непрерывную проверку, мониторинг и реагирование, а также анализ событий и трафика, что помогает выявить текущие тенденции и методы проникновения.

Кибербезопасность сетей управления

До атаки

Пословица «кто предупрежден, тот вооружен» является ключевым принципом в стратегии Cisco. Группа информационной безопасности и аналитики Cisco Talos ежегодно анализирует миллионы вредоносных приложений и регулярно обновляет правила, обеспечивая готовность своих заказчиков к отражению новых угроз. Наша библиотека правил включает в себя специальный контент по промышленным системам управления для распространенных промышленных протоколов. Заказчики или поставщики могут создавать собственный контент и импортировать его в нашу библиотеку правил. Сделать это можно как с помощью наших продуктов, так и в решении Snort® с открытым исходным кодом. Такая гибкость позволяет легко обмениваться контентом в рамках сообщества, не требуя от каждого заказчика создания собственного контента с нуля.

Чтобы использовать накопленные данные, для начала необходимо понять, какой объект нужно защитить, и где он находится. В случае сетей управления здесь все не так просто, как может показаться. Большинство промышленных систем управления предназначены для выполнения конкретных задач и работают с проприетарными операционными системами, которые располагают небольшим объемом процессорной мощности и памяти. Таким образом, даже самые элементарные методы обнаружения, такие как сканирование портов, могут привести к сбою промышленных систем управления. Cisco может пассивно профилировать сетей управления без вмешательства в них. Иными словами, сканирование не загружает сети управления и не увеличивает задержку связи между системами. Затем можно составить белые списки моделей поведения и обмена данными и проверять только подозрительный трафик, а «чистый» обмен данными будет осуществляться в обычном для сетей управления порядке.

В последние несколько лет многие системы управления перешли на коммерческие операционные системы, включая Microsoft Windows XP. Особенно это касается систем с интерфейсом «человек-машина» и серверов архивных данных. Использование коммерческих операционных систем выгодно производителям. Им не нужно тратить свои усилия на разработку собственных операционных систем. При этом для владельцев предприятий сохраняется возможность повышенной совместимости с оборудованием поставщиков. Однако такие системы управления особенно уязвимы, поскольку исходный код ОС очень сложный. Зависимость от них сама по себе представляет угрозу. Хотя поставщики коммерческих ОС регулярно выпускают исправления для своих средств защиты, исправление систем в сети управления — совсем не то же самое, что исправление систем в ИТ-сети. Оно занимает больше времени и требует тщательной проверки для обеспечения надежности. Cisco предоставляет средства управления компенсирующего характера, уделяя особое внимание защите этих систем, пока они не исправлены и уязвимы.

Во время атаки

Спецслужбы могут зондировать корпоративные сети в поисках доступа к сети управления. Смартфон подключается к системе управления при зарядке аккумулятора, и вредоносное ПО попадает в сеть. Новое устройство на подстанции начинает обмениваться данными с системой управления, которая, в свою очередь, начинает обмен данными с другими системами, чего не происходило ранее. Юные хакеры находят системы, которые по недосмотру подключились к Интернету, и пытаются осуществить атаку, чтобы взять их под свой контроль.

Атаки могут быть как быстрыми и грубыми, так и медленными и тихими. Они могут осуществляться напрямую или через ничего не подозревающего посредника. Атаки угрожают физической безопасности так же, как и надежности работы сети.

Cisco отслеживает периметр вашей сети и внутреннюю сеть на предмет атак, подозрительных действий, нарушения прав доступа, совершенного вредоносного ПО и прочих угроз посредством единой аппаратной платформы. Устройства могут быть исполнены в виде аппаратных средств или виртуальных устройств. Кроме того, есть возможность проверять оконечные и мобильные устройства на предмет сложного вредоносного ПО. Набор реализуемых возможностей определяется исходя из собственных требований, бюджета и сроков. При этом не требуется дополнительное оборудование и сохраняется возможность постепенного развития инфраструктуры. Если обнаруживается что-то подозрительное, решения Cisco могут либо реагировать в режиме оповещения, либо автоматически принимать меры по сдерживанию угрозы. Выбор за вами. Вы также можете регулировать правила реагирования для того или иного сегмента сети, чтобы действия в отношении ответственных сегментов требовали подтверждения со стороны человека перед их выполнением. Все действия, связанные с контролем, отчетностью и управлением, выполняются через единую центральную консоль.

После атаки

Как уже было сказано выше, невозможно заранее спланировать встречу с врагом. Реальность такова, что тактика злоумышленников быстро меняется, и поэтому средства защиты от них должны развиваться так же быстро. То, что кажется безобидным сегодня, завтра может оказаться хитроумно замаскированной атакой. Как защитить уязвимые места, которые еще не известны? Подход Cisco ориентирован на защиту от угроз; он подразумевает непрерывный анализ данных о событиях и сетях, а также выявление подозрительных и шаблонных действий. Если они обнаруживаются, наши средства обеспечения безопасности определяют источник и объем угрозы, сдерживают ее и нейтрализуют вредоносное ПО. С помощью такой совершенной технологии можно обновлять средства защиты, минимизируя вероятность повторного заражения.

Вывод

Изолирование систем больше не гарантирует защиту от вторжения. Повышенная взаимосвязанность систем, обеспечивающая производственную эффективность для сетей управления, вместе с тем усугубляет уязвимость и дает больший простор для вредоносных действий. Хотя эти угрозы и подобны тем, с которыми сталкиваются корпоративные ИТ-сети, но сети управления имеют свои уникальные особенности, и потому решения в области кибербезопасности не являются панацеей от всех бед. В компании Cisco это понимают. Наш расширенный портфель решений в области кибербезопасности поможет защитить ваши сети до, во время и после атаки без ущерба для их надежности.

Штаб-квартира в США
Cisco Systems, Inc.
Сан-Хосе (Калифорния)

Штаб-квартира в Азиатско-Тихоокеанском регионе
Cisco Systems (USA) Pte. Ltd.
Сингапур

Штаб-квартира в Европе
Cisco Systems International BV, Амстердам,
Нидерланды

Компания Cisco насчитывает более 200 офисов и представительств по всему миру. Адреса, номера телефонов и факсов приведены на веб-сайте Cisco по адресу **www.cisco.com/go/offices**.

Отпечатано в США 11/14

