Schneider Electric: пандемия изменила подходы к кибербезопасности крупных компаний

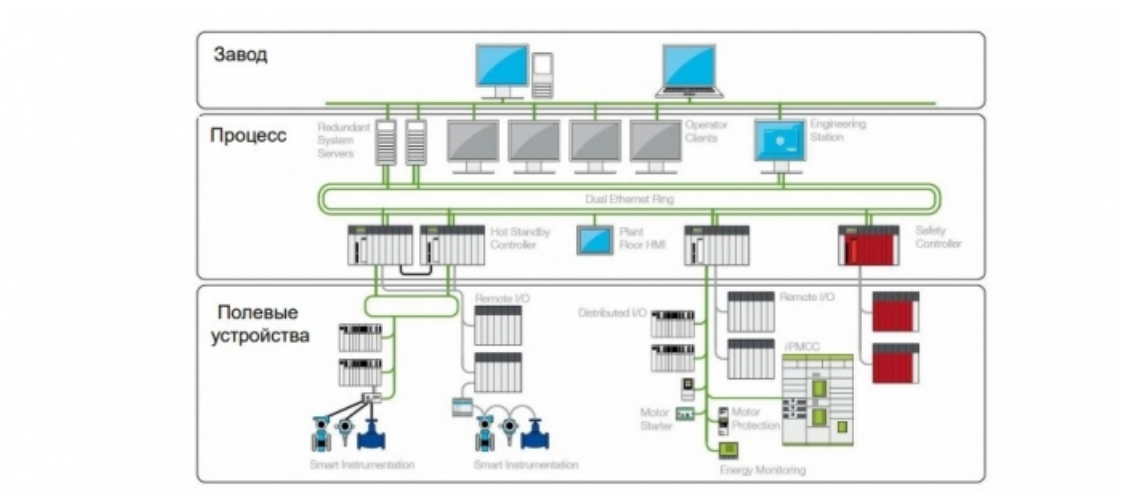
Проблемы кибербезопасности в современном мире, где информационные технологии проникли уже практически во все сферы деятельности человека, давно вышли на первый план. Однако, зачастую акцент в кибербезопасности принято делать на защищенность телекоммуникационных и корпоративный сетей, а также устройств, которые к этим сетям подключены. И это было справедливо до тех пор, пока злоумышленники не обратили свой взор на крупные производственные предприятия. За последние годы количество атак на ключевые отрасли государств увеличилось и ответ на эту угрозу в комплексном подходе к кибербезопасности и совместной работе регулирующих органов, бизнеса и вендоров аппаратных решений и программного обеспечения. О том, как обеспечить кибербезопасность промышленных объектов и критической инфраструктуры, мы поговорили с техническим консультантом по кибербезопасности Schneider Electric Андреем Ивановым.

В одном из недавних вебинаров Вы затрагивали тему кибербезопасности автоматизированных систем управления технологическим процессом (АСУ ТП) на предприятиях. Можете вкратце пояснить, что такое АСУ ТП?

Если говорить сухим языком определений, то АСУ ТП - это группа решений технических и программных средств, предназначенных для автоматизации управления технологическим оборудованием на промышленных предприятиях. АСУ ТП применяются для технологических процессов, то есть на производстве. Это может быть любое производство от нефтегазовой отрасли до сборочного производства и пищевой промышленности.

В целом, АСУ ТП делится на три уровня - это полевые устройства, управление процессом и какие-то заводские системы, к которым АСУ ТП может подключаться и обмениваться с ними данными.

Полевые устройства состоят из различных датчиков и сенсоров, которые измеряют физические характеристики какого-либо процесса, преобразуют эту информацию в цифровую и передают в систему управления. Датчики обеспечивают контроль температуры, давления, расхода. В состав полевых устройств также входят различные исполнительные устройства - клапана, задвижки, насосы, электродвигатели, управление электродвигателем.



На уровне процесса появляются технические средства, которые могут обрабатывать эту информацию. То есть, это логические программируемые контроллеры, которые могут обрабатывать информацию (ПЛК) и элементы системы АСУ ТП, которые используют компьютер. Сюда входят как персональные ПК операторов, так и различное серверное оборудование для хранения и обработки данных.

На уровне завода мы видим уже классические информационные системы. Это в чистом виде информационные компьютерные технологии, которые используют данные с нижних уровней для их обработки и принятия решений на производстве.

На самом деле, полевых устройств в виде чисто технических решений, очень много. Сейчас на рынке есть огромное количество разнообразных датчиков и сенсоров. То же самое касается и программных продуктов, которые, в основном, задействованы на втором и первом уровнях.

Раньше, когда компьютеры были большими и не были персональными, системы АСУ ТП строились с использованием релейной логики. Такие системы занимали целые помещения и управляли техническими процессорами.

Следующим этапом стало появление интегральных микросхем, а вместе с ними появились программируемые логические контроллеры. Первый ПЛК появился 1968 году. ПЛК занимает гораздо меньше места, чем линейная логика, и самое главное: для изменения логики работы, его достаточно было перепрограммировать.

Здесь нужно понимать что программирование контроллеров и разработка веб-сайтов - это принципиально разные вещи. Для того, чтобы запрограммировать контроллер, нужно владеть другими языками программирования и знать особенности технологии производства. При их программировании используются прикладные протоколы для обмена данными между элементами АСУ ТП - это специфичные промышленные протоколы. Один из них - это протокол MudBus, которые появился достаточно давно - в 1978 году.

Следующим шагом в развитии АСУ ТП было появление в них компьютерных или информационных технологий. С появлением ПК, стали появляться и первые хакеры. Встала в полный рост проблема кражи информации, которая содержится в компьютерах. Так появилось понятие "информационная безопасность". Впервые его описали в 1978 году.

С развитием технологий произошло взаимопроникновение IT и OT (операционные технологии - это технологии управления производством и технологическим процессом). Как раз эти технологии используются в АСУ ТП. Взаимное проникновение как раз и произошло потому, что в АСУ ТП стали использовать информационные технологии.

То есть, с появлением и распространением интернета угроза для крупных предприятий стала выше? Какими способами злоумышленник может добраться до АСУ ТП?

Как правило, системы АСУ ТП не изолированы. Они соединены с системами управления предприятием, которые, в свою очередь, имеют соединение с корпоративной сетью. Ну а корпоративная сеть имеет выход в интернет.

Во-вторых, есть такое понятие как внутренний нарушитель. То есть, можно подкупить / запугать / шантажировать сотрудника, который имеет доступ к АСУ ТП. Его можно заставить принести на работу флешку и прицепить ее к ПК, который входит в состав АСУ ТП.

Если на сегодняшний день почитать отчеты с описанием производимых атак, то можно увидеть, что 40% приходится на серверы управления технологическим процессами. То есть, это те самые атаки на АСУ ТП. Интерес к ним с каждым годом все больше. Согласно данным "Касперского", целевых атак на промышленные компании становится все больше. Причем, в основном, это атаки, так называемых, вымогателей.

Какие меры для защиты сейчас применяются?

Первый международный стандарт кибербезопасности АСУ ТП был разработан в 90-х годах прошлого века. Согласно ему, средства защиты делятся на четыре группы. Их так много потому, что на сегодняшний день какого-то универсального средства защиты из коробки, приобретя которое можно закрыть все бреши в кибербезопасности, попросту нет. На сегодня это должен быть комплекс решений с одной стороны, а с другой - система защиты должна быть построены по многоуровневому принципу. Даже если взломщик сможет преодолеть один уровень, то другой уровень должен его остановить или задержать до того, как можно будет предпринять шаги по его нейтрализации.

Из чего состоит комплексное решение?

Оно состоит из нескольких важных частей. Первое - это контроль управления доступом. Как физическим доступом к техническим средствам, так и доступом к программным средствам. Защита конечных узлов - антивирусы, управление подключаемыми устройствами. Контроль флешек, например. Также необходимо обеспечить наличие средств обнаружения атак и средств реагирование на атаки. Сюда входит, например, резервное копирование. Оно позволяет восстановить работу системы в самых критических случаях - даже, когда атака оказалась успешной.

Поскольку АСУ ТП состоит из технических и программных средств, то кроме, так называемых, наложенных средств защиты (антивирусы, мониторинг и прочее), существуют еще и встроенные. Речь идет о функционале безопасности, который присутствует на борту технических средств АСУ ТП (контроллеров и прочего). Производители АСУ ТП об этом тоже думают и встраивают системы защиты в свои устройства.

Здесь для нас, как для вендора АСУ ТП, все начинается с цикла безопасной разработки. Он подразумевает, что мы должны использовать проверенные безопасные компоненты - это касается как аппаратной части устройства, так и программного обеспечения.

Как должны быть организованы на предприятии все меры кибербезопасности, чтобы максимально снизить угрозу?

Сеть АСУ ТП должна быть отделена от корпоративной сети через межсетевой экран. При этом, сама сеть АСУ ТП должна быть сегментирована, а средства защиты должны быть выделены в отдельный сегмент.

В целом, средства защиты АСУ ТП можно разделить на три уровня. Первое - это защита узлов, которые используют для своей работы компьютеры. Для этого применяется антивирусное ПО, контролируется запуск приложений и их целостность. То есть, даже если нарушитель или сотрудник сможет установить вредоносное ПО на компьютер, то средства защиты не позволят запустить это приложение.

Следующий уровень - это защита сетей. Сетевой трафик тоже нужно мониторить и выявлять несанкционированную деятельность. Третий уровень - защита самих элементов АСУ ТП - это использование встроенного функционала который предлагает вендор.

Насколько эта структура типична для российских предприятий?

Она типична для крупных предприятий в той или иной степени. В целом, это классическая пирамида построения управлением предприятием. Для малых предприятий такая структура тоже достаточно типична, потому что в той или иной мере, функционал в системах присутствует.

Многие объекты энергетики, например, подстанции, до сих пор имеют аналоговое управление. Казалось бы, хорошо: что не оцифровано, то нельзя и взломать. Но всё же: как защищать такие объекты?

Там есть свои специфические меры защиты. Естественно, на "аналог" антивирус не поставить, но это не отменяет защиту периметра, защиту на уровне физического доступа к этим системам управления и так далее. Если же та или иная мера не может быть применена, должны быть разработаны компенсирующие меры. Такие задачи решаются и для таких систем есть свои меры защиты. Плюс

Минэнерго выпускает свои дополнительные требования к объектам энергетики.

Насколько внимательно малый и средний бизнес относится к обеспечению кибербезопасности своих предприятий, или пока этим озабочены преимущественно крупные компании?

По своему опыту скажу, что средний бизнес либо начал что-то делать в этом направлении, либо задумался об этом, потому что у нас запросы о кибербезопасности появляются от все более мелких компаний.

Какие новые риски, на ваш взгляд, появятся с распространением в системах АСУТП мобильных устройств IoT и мобильных сетей передачи данных? Как вы в целом оцениваете перспективу операторов сотовой связи на рынке АСУТП (услуги на базе LoRa, NBIOT, 4/5G)?

Мы пока не сталкивались с операторами связи, как с поставщиками средств защиты. А вот появление мобильных устройств в сетях АСУ ТП - тема отдельная и очень интересная, потому как эти устройства используются все чаще. На самом деле, мобильные устройства в сети создают большие риски и каждая компания сейчас работает с этой угрозой по-своему.

Как пандемия отразилась на кибербезопасности?

Самым прямым образом. Многих работников перевели на удаленную работу, из-за этого многим работодателям понадобилось организовывать удаленный доступ. Теперь требования по безопасности удаленного доступа даже прописали в нормативах.

До 1 января 2024 года объекты КИИ должны перейти на использование отечественного ПО, до 1 января 2025-го - начать использовать преимущественно отечественное оборудование. На ваш взгляд, насколько это реальная задача и можно ли говорить о том, что к этим срокам российские разработчики и производители обеспечат рынок достаточно качественным софтом и железом, в том числе, с точки зрения кибербезопасности?

С точки зрения кибербезопасности он уже обеспечен, если говорить о программных средствах.Есть решения по мониторингу и предотвращению атак. С аппаратным обеспечением ситуация пока хуже. Те же российские межсетевые экраны уже есть, но пока начального уровня. Если требуется высокая производительность и высокая пропускная способность, то таких решений почти нет. Что касается прикладного ПО, то во-первых сроки были определены после диалога с разработчиками, которые обещали успеть. Кроме того, в приказе Минцифры речь идет о преимущественном использовании российского ПО. Полного запрета на иностранное ПО не вводится лишь до появления иностранного аналога.