КИБЕРБЕЗОПАСНОСТЬ ПРОМЫШЛЕННОЙ АВТОМАТИЗАЦИИ

АНДРЕЙ ЧЕРТКОВ
andrei.chertkov@schneider-electric.com

Новый виток развития средств промышленной автоматизации существенно обострил проблему обеспечения кибербезопасности предприятий. В ряде отраслей собственники производств только начинают осознавать значимость этой проблемы и масштаб возможных потерь. Однако эксперты убеждены, что в ближайшем будущем рост числа кибератак заставит пользователей систем автоматизации более взвешенно и комплексно подходить к вопросам защиты своих активов от этой категории рисков.

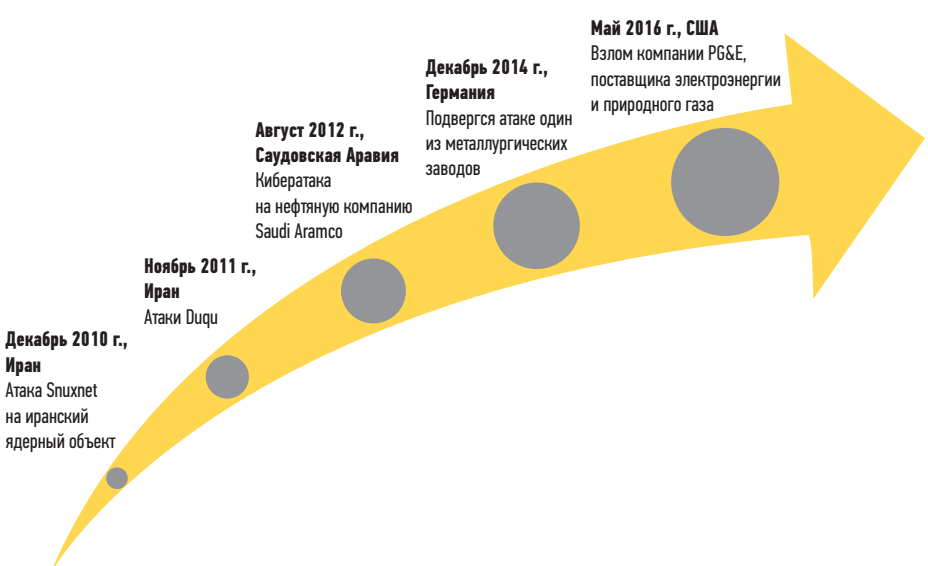
РОСТ УГРОЗ НЕ ВПОЛНЕ ОСОЗНАЕТСЯ

Киберугрозы — явление не новое, но за последнее десятилетие значимость связанных с ними рисков многократно возросла. Дело в том, что раньше автоматизированные системы управления технологическими процессами (АСУ ТП) были физически отделены от локальных вычислительных сетей и Интернета. В современном мире требования к АСУ ТП изменились: они больше не могут оставаться изолированными от внешнего мира. Также важно отметить возрастающую роль решений автоматизации в рамках концепции промышленного «Интернета вещей» (Industrial Internet of Things, IIoT). Эта тенденция заставляет абсолютно по-новому взглянуть на проблему обеспечения кибернетической безопасности в промышленной среде.

Сегодня руководству компаний важно в режиме онлайн контролировать множество показателей технологических процессов, управлять эффективностью производства и обеспечивать коллективную работу через сети, в том числе для территориально удаленных сотрудников. В процессе освоения «Интернета вещей» к промышленным сетям в той или иной мере должны получить доступ третьи компании, к примеру, поставщики оборудования — с целью контроля над его состоянием. Все эти новые возможности АСУ существенно упрощают многие процессы и радикально сказываются на рентабельности, однако при этом создают новые риски для операционной деятельности, связанные с киберугрозами.

Мотивы кибератак многообразны: это получение финансовой выгоды, желание нанести ущерб конкурентам, оказать политическое давление. Порой атаки совершаются по личным мотивам недовольными сотрудниками или подрядчиками. Вне зависимости от причин ущерб от несанкционированного вторжения в АСУ ТП оказывается очень весомым. Это не только внеплановые остановки производства и поломки оборудования, но и серьезные репутационные потери, утечка конфиденциальной информации, угроза жизни и здоровью людей, рост риска аварий и даже техногенных катастроф.

РИС. 1. ▼ Крупнейшие кибератаки на промышленные сети в 2010–2016 гг.



Количество кибератак на промышленные сети неуклонно растет (рис. 1). Так, по данным ICS-CERT (United States Computer Emergency Readiness Team — Американская группа реагирования на чрезвычайные ситуации в киберпространстве), с 2006 по 2012 г. количество киберинцидентов увеличилось на 782%. В 2014 г. было зарегистрировано 245 случаев кибератак на промышленных объектах, а в 2015 г. — уже 295. При этом очевидно, что многие атаки остались вне поля зрения аналитиков. По данным международной консалтинговой корпорации PwC, средний ущерб от инцидента в сфере информационной безопасности в России в 2015 г. составил $5,3 млн, что на 47% выше, чем годом ранее.

Безусловно, все большее распространение киберугроз заставляет собственников промышленных активов искать надежные способы защитить свои сети, а поставщиков решений в сфере АСУ ТП — продумывать комплексные программы минимизации рисков в сфере кибербезопасности.

В отраслях с критически важной инфраструктурой (к примеру, в энергетике, нефтегазовой и атомной промышленности) производства уже

сегодня готовы инвестировать средства в повышение защищенности своих активов. Однако в других отраслях многие пользователи либо не знают о риске кибератак, либо не спешат внедрять на своих предприятиях решения, необходимые для обеспечения безопасности (рис. 2). Ухудшает ситуацию то, что окупаемость инвестиций в кибербезопасность трудно посчитать. В результате многие производственные компании сегодня заняли выжидательную позицию, изменить которую сможет только появление обязательных регулирующих норм или прецедент кибератаки.

ФАКТОРЫ РИСКА

В промышленности объектами киберугроз могут становиться распределенные системы управления (РСУ), программируемые логические контроллеры (ПЛК), системы сбора данных и управления (системы SCADA) и элементы человеко-машинного интерфейса (HMI).

При грамотной оценке ситуации и тесном сотрудничестве с поставщиком решений в области автоматизации большинство уязвимостей, имеющихся в промышленных сетях, реально устранить. Факторы риска вполне можно надежно контролировать, главное, чтобы у персонала промышленного предприятия хватало желания и квалификации, чтобы этим заниматься.

На сегодня один из ключевых факторов уязвимости — общая низкая культура процессов обеспечения кибербезопасности. На многих предприятиях не проводится оценка ключевых рисков и не обеспечивается безопасное управление операциями, включая базовое управление паролями. Отсутствует комплексный аудит, не гарантируется согласованное и эффективное соблюдение политик безопасности, а также недооцениваются доступные инструменты контроля и обнаружения угроз. Даже в современном мире весьма распространенными проблемами остаются недостаточный контроль физического доступа на территорию и халатное отношение к процедурам авторизации и аутентификации при входе в корпоративные и промышленные сети (к примеру, слишком легкие, редко изменяемые пароли).

Программно-аппаратными лазейками для злоумышленников могут становиться незащищенные каналы удаленного доступа, неадекватные межсетевые экраны или неправильно выстроенная архитектура сети, в том числе отсутствие сегментации. Иногда в системах встречаются незащищенные удаленные терминалы, компьютеры, USB-порты, мобильные и периферийные устройства, а также специфические виды устройств человеко-машинного интерфейса.

Постепенный переход к использованию коммерческих ИТ-решений, несомненно, несет коммерческую выгоду и упрощает эксплуатацию и интеграцию систем. Но при этом системы управления оказываются более уязвимыми перед вредоносным программным обеспечением (ПО) и угрозами безопасности, нацеленными именно на коммерческие системы.

Причинами возникновения уязвимостей могут служить разнообразные ошибки «человеческого фактора», в частности неверные действия проектировщика или инсталлятора при конфигурации и установке системы. Негативно сказываются на безопасности неадекватные планы сопровождения и модернизации АСУ ТП, недостаточный уровень квалификации персонала, отвечающего за их внедрение и обслуживание. Производственный сектор гордится высококвалифицированными специалистами по системам автоматизации, однако такая экспертиза в конкретных продуктах и решениях далеко не всегда означает адекватную экспертизу в промышленных ИТ-сетях. Этот пробел ослабляет способность организации разрабатывать всесторонние стратегии защиты и предотвращения угроз.

Порой между ИТ-департаментом и департаментом промышленных систем управления нет достаточного уровня взаимопонимания в силу разных приоритетов. Так, специалисты по АСУ ТП нередко настороженно относятся к внедрению дополнительных мер кибербезопасности. Обновление операционных систем, ПО и средств антивирусной защиты представляется им как потенциальная угроза непрерывности технологического процесса. Справедливости ради заметим, что при неквалифицированном выполнении таких операций угроза может стать вполне реальной.

Серьезным препятствием для повышения уровня кибербезопасности предприятий является и неопределенность в правовом поле, отсутствие требований, закрепленных на законодательном уровне, а также недостаточно развитый уровень стандартизации в сфере защиты от киберугроз.

ПЛАН ЗАЩИТЫ ОТ КИБЕРАТАК

Для предотвращения киберугроз предприятиям необходимо наладить партнерские отношения с поставщиками решений, понимающими специфические характеристики промышленных сетей и уделяющими большое внимание вопросам безопасности. Ответственные

РИС. 2. ▼ Количество кибератак в разных отраслях промышленности в 2016 г., по данным Kaspersky Lab ICS CERT

поставщики средств автоматизации стремятся встраивать средства безопасности во все продукты и сервисы как на стадии разработки, так и на протяжении их жизненного цикла. Такие поставщики помогают заказчикам развернуть многоуровневую систему глубокой защиты средств АСУ ТП, используя для этого комплексный план поэтапного снижения рисков.

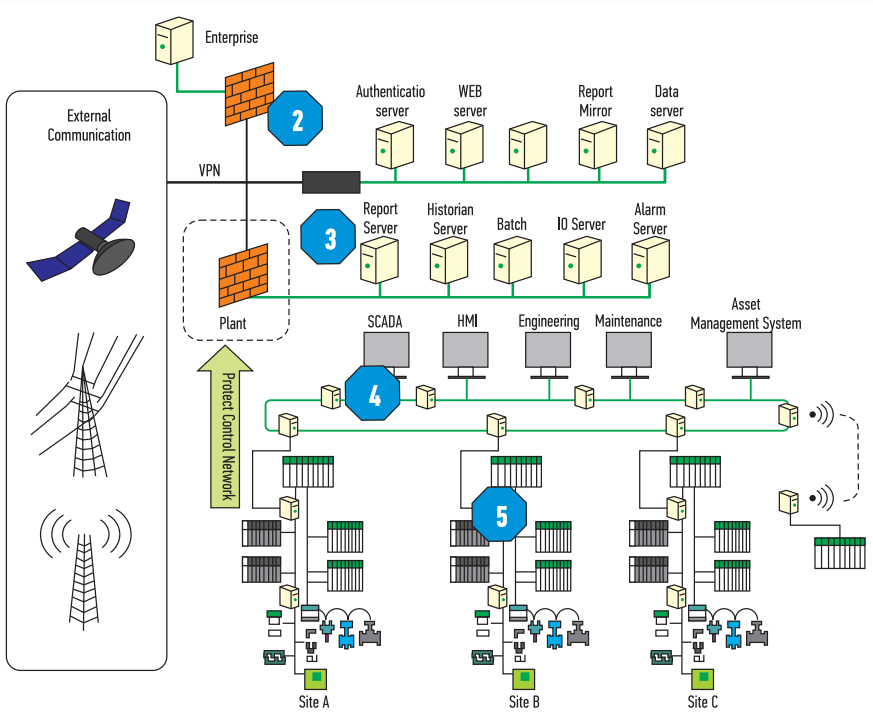
В частности, компания Schneider Electric рекомендует промышленным предприятиям использовать подход Defense-in-Depth. Эта гибридная стратегия многоуровневой защиты реализует комплексный подход к безопасности в масштабе всего промышленного предприятия.

Defense-in-Depth была разработана для оборонных целей Агентством национальной безопасности США, однако впоследствии оказалась применимой и для гражданских отраслей. По мнению ряда экспертов, в будущем данная концепция станет стандартом обеспечения безопасности в промышленной среде.

Подход Defense-in-Depth предполагает шесть ключевых компонентов (рис. 3):

1. Разработка плана по обеспечению безопасности: описание процедур оценки рисков и их минимизации, а также методов аварийного восстановления.
2. Отделение сетей промышленной автоматизации от других сетей путем создания буферных зон, способных защитить промышленную систему от запросов и сообщений из корпоративной сети.
3. Защита периметра от несанкционированного доступа, включающая межсетевые экраны, средства аутентификации, авторизации, VPN (виртуальные частные сети) и антивирусное ПО.
4. Сегментация сети, позволяющая ограничить распространение потенциальной угрозы одним сегментом. Для разделения сети на подсети и ограничения передачи трафика между сегментами используются коммутаторы и VLAN (группа хостов с общим набором требований, которые взаимодействуют между собой независимо от их физического местонахождения).
5. Усиление защиты устройств: управление паролями, определение профилей пользователей и деактивация неиспользуемых сервисов.
6. Регулярный мониторинг и обновление: постоянное наблюдение за активностью операторов и сетевыми коммуникациями, а также своевременное обновление программного и микропрограммного обеспечения.

РИС. 3. ▼ Ключевые компоненты Defense-in-Depth



ПОШАГОВЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ КИБЕРБЕЗОПАСНОСТИ

Хотя подход Defense-in-Depth приветствует создание и реализацию исчерпывающего плана защиты, будет неверным полагать, что переход к этой концепции осуществляется по принципу «всё или ничего». На самом деле, для достижения быстрых результатов с минимальными затратами клиенты могут придерживаться пошагового подхода. Для этого необходимо следующее:

- идентифицировать пробел в системе обеспечения безопасности, который может привести к наиболее серьезным для предприятия последствиям;
- выявить конкретные производственные зоны, с которыми эти последствия связаны;
- описать наиболее серьезные уязвимости в данной области;
- минимизировать или устранить эти уязвимости.

Обеспечив безопасность наиболее критической зоны, компания может перейти к устранению уязвимостей в другой области. Такой сфокусированный пошаговый подход позволит избежать необходимости менять всю систему сразу и избавит от связанного с этой задачей «аналитического ступора». Он не только гарантирует, что немедленно будут устранены проблемы, ведущие к серьезным последствиям для деятельности предприятия, но и позволит не распылять силы и средства, то есть добиться максимального результата от инвестиций. Тем не менее поэтапная тактика не должна приводить к потере целостной картины.

Также важно помнить, что обеспечение кибернетической безопасности — это процесс, а не единовременное решение. Поэтому неоспоримым преимуществом поставщика средств автоматизации должно быть наличие у него комплексного пакета решений и услуг. Такой пакет может включать:

- услуги по оценке рисков и проектированию систем автоматизации, помогающие клиентам идентифицировать наибольшие риски, определять фокусные области для снижения этих рисков и применять элементы сетевой архитектуры, необходимые для минимизации рисков, связанных с кибернетическими угрозами;

- текущую поддержку по мониторингу, управлению и защите систем автоматизации с целью оперативной изоляции возникающих угроз;
- рекомендации в форме референсных архитектур, помогающие клиентам применять к своим системам подход Defense-in-Depth;
- предложение полного набора средств и инструментов для непосредственного решения задач по обеспечению кибернетической безопасности с учетом перспективы.

Например, в портфеле Schneider Electric есть специальное решение по обеспечению кибернетической безопасности для АСУ ТП — Foxboro Evo, использующее необходимые аппаратные и программные средства для обеспечения защиты на уровне сети управления технологическими процессами и на уровне внешних информационных сетей. Это решение включает в себя применение соответствующих сетевых экранов, проверенных архитектур построения АСУ ТП, встроенную защиту контроллеров от коммуникационных атак, а также комплексный инструментарий для защиты от кибернетических угроз, в который входят следующие компоненты:

- Антивирусное сканирование и обновление файлов антивирусных данных. Это позволяет обнаружить и предотвратить кибератаку и удалить вредоносное ПО, включая системные и компьютерные вирусы и «черви», троянские программы, шпионское и рекламное ПО. Обнаружение и предотвращение угроз на ранней стадии позволяет свести к минимуму возможность повреждения оборудования, входящего в состав системы, и повышает безопасность ведения технологического процесса.
- Подсистема обнаружения несанкционированного вторжения. Эта подсистема отслеживает внешние или внутренние нарушения системной политики безопасности. Она блокирует известные атаки и защищает против несанкционированного просмотра, копирования, изменения и удаления информации и соответствующих системных и сетевых ресурсов и приложений, получающих и хранящих информацию.
- Унифицированная платформа управления безопасностью дает возможность пользователям централизованно отслеживать и управлять работой различных продуктов безопасности.
- Подсистема предотвращения потери данных идентифицирует, отслеживает и защищает конфиденциальные данные (которые находятся в использовании, перемещении, хранении), применяя контекстуальный анализ на предмет безопасности. Также обеспечивается контроль доступа к аппаратным портам, таким как различные типы дисководов, включая CD/DVD или USB-порты рабочих станций системы управления и серверов.
- Сервис администрирования доменных сетей и учетных записей пользователей. Этот сервис производит аутентификацию и авторизацию всех пользователей и компьютеров в доменной сети, а также присваивает и применяет политики безопасности для всех компьютеров и пользователей, производит установку и обновление ПО.
- Процедура повышения «прочности» операционной системы.
- Применение политик «белых» списков используемого ПО для исключения возможности установки и запуска запрещенного, неопознанного или нерекомендуемого к применению ПО.
- Инструментарий для оценки состояния станций и серверов.
- Подсистема резервного хранения и восстановления станций и серверов.
- Подсистема парольной защиты, которая обеспечивает изменение паролей для входа в систему, в том числе на периодической основе, создание индивидуальных паролей пользователей с различным уровнем доступа, блокирование пароля после нескольких неудачных попыток входа в систему, безопасный механизм для сброса пароля и имени пользователя, поддержка в пароле цифро-буквенных и символьных знаков, защита файла с паролями, отслеживание создания, удаления и модификации учетных записей пользователей, отслеживание входа/выхода пользователей и изменений в конфигурации.

Нужно также принимать во внимание, что кибербезопасность тесно связана с безопасностью предприятия в более широком смысле. Наилучшим вариантом станет сотрудничество с поставщиком, предлагающим не только решения по автоматизации технологических процессов и управлению предприятием, но и системы обеспечения физической безопасности, включая системы контроля доступа, видеонаблюдения, противопожарной защиты. В этом случае план по уменьшению уязвимости предприятия будет цельным и комплексным.

ОБЪЕДИНЕНИЕ УСИЛИЙ В БОРЬБЕ С КИБЕРПРЕСТУПНОСТЬЮ

Сегодня большинство промышленных предприятий только начинает осознавать масштаб рисков, связанных с киберугрозами. Тем не менее, по наблюдениям экспертов, уже сегодня видна положительная динамика: компании все чаще задумываются над тем, как защитить свои активы от киберпреступности, которую следует рассматривать в качестве основного препятствия на пути к новому этапу в развитии систем промышленной автоматизации.

Вероятно, в ближайшее время на международном и российском уровне будут разработаны нормативные требования по обеспечению кибернетической безопасности для АСУ ТП. Необходимо выработать единую терминологию, правила сертификации продуктов и стандарты (возможно, таким стандартом мог бы стать IEC 62443 8). В первую очередь они должны коснуться предприятий с критически значимой инфраструктурой.

В любом случае, каждая производственная компания может уже сегодня, не дожидаясь выработки стандартов и законодательных мер, задуматься о собственной защищенности от кибератак. Такой ответственный подход позволит уже сейчас начать пользоваться всеми преимуществами современных открытых АСУ ТП. Со своей стороны, поставщики промышленных систем управления, рассматривающие безопасность как основу своего предложения по автоматизации, станут надежными союзниками в этом вопросе. ●