Защита данных в Industrial Ethernet: мифы и решения

Компания «Шнейдер Электрик»

Сформулированы рекомендации от компании Schneider Electric по использованию оборудования, оснащенного средой передачи данных Industrial Ethernet.

Ключевые слова: Industrial Ethernet, Internet, передача данных, системы защиты, широковещательные пакеты, тестирование, механизмы контроля доступа.

В 2007 г. атомная электростанция Browns Ferry отключилась из-за зацикливания пакетов данных в сети Ethernet. Сервер работал в сети управления предприятием и обменивался данными с контроллерами ТП с целью мониторинга и диагностики. Видимо, сервер, предназначенный для синхронизации систем управления, записал в контроллеры значения сброса (нули), что вызвало отключение системы. В прессе сообщалось и о проблемах из-за неправильного подключения кабеля Ethernet. В результате неправильного подключения кабеля возникло сетевое кольцо Ethernet, вызвавшее «лавину» широковещательных пакетов, которая прервала работу ответственных конечных устройств.

Могло ли применение более совершенной защиты сети, например, более совершенного брандмауэра или системы обнаружения несанкционированного доступа (Intrusion Detection System — IDS) предотвратить эти сбои? Маловероятно. Эти системы защиты спроектированы так, что работая на уровне шлюза или конечного устройства, они не могут быть эффективными, если проблемы создаются доверенными системами из других сетей или вызваны сбоями внутри локальной сети.

Системы внешней защиты предназначены для отражения атак из Internet. Эти же отказы были внутренними, созданными локально. К таким проблемам может привести, например, плохо протестированная обновленная версия доверенной SCADA-системы, которая имеет право записывать информацию в контроллеры, или неверно подключенный кабель Ethernet, вызвавший зацикливание пакетов данных.

Однако богатый опыт и передовые технологии компании Schneider Electric способны смягчить и даже предотвратить возникновение таких проблем у клиентов. Согласно статистике, большинство случаев неправильного функционирования, приводящего к таким проблемам, гораздо чаще обусловлено не посторонними хакерами, а другими причинами. Это может быть: персонал клиента; системные интеграторы, не работающие с компанией Schneider Electric и не знакомые с изделиями компании; неправильно функционирующие системы сторонних поставщиков комплектного оборудования (OEM).

Основное отличие от прежних промышленных сетей заключается в том, что Ethernet имеет возможность подключения к сети Internet, что редко было возможно в прежних системах. По этой причине отказы в производственных процессах, использующих Ethernet, сразу же связывают с Internet-хакерством. Исследования показали, что >80 % производственных отказов происходят по внутренним причинам, а не являются результатом внешней угрозы.

Как компания Schneider Electric помогает своим клиентам, использующим Industrial Ethernet, избежать подобных сюрпризов, причина которых лежит внутри, а не снаружи?

Тестирование всех систем, имеющих право записывать информацию в ПЛК

• Современные информационные сети являются гетерогенными: в них используются изделия различных поставщиков комплектного оборудования, которые функционируют на базе одной универсальной технологии — Modbus TCP и Ethernet. Однако не все поставщики тестируют устройства и драйверы в соответствии со строгими стандартами компании Schneider Electric. Следовательно, поскольку Modbus является открытым стандартом и позволяет любому поставщику предлагать изделия на ее основе, нужно убедиться, что клиент использует только устройства и системные драйверы, сертифицированные организацией Modbus-IDA; это поможет избежать проблем при передаче данных по сети.

• Важно объяснить клиентам, что плохо протестированная система может вызвать проблемы в любой промышленной сети, а не только в Ethernet и Modbus TCP. Неправильно функционирующая или плохо протестированная система, как в описанном случае, доказывает, что тестирование перед вводом в действие необходимо даже после внесения незначительных изменений. В настоящее время при использовании Ethernet проектирование и тестирование так же важны, как и в прежних промышленных сетях. SCADA или иная система диспетчерского управления, способная записывать информацию в контроллеры, должна быть протестирована, чтобы исключить возможность ее непредсказуемого поведения. При обновлении, настройке или изменении конфигурации любой платформы, не относящейся к компании Schneider Electric, нужно убедиться, что перед вводом в действие она была протестирована в производственной среде.

• Нужно обеспечить присутствие представителя поставщика оборудования, ответственного за развертывание или ввод в эксплуатацию систем, не относящихся к компании Schneider Electric, которые могут повлиять на ПЛК компании Schneider Electric, так как имеют к ним доступ с правом записи.

• Убедиться, что во всех устройствах, разработанных не в компании Schneider Electric и имеющих доступ с правом записи к ПЛК Schneider Electric, предусмотрены механизмы контроля доступа, такие как защита паролем.

Использование изделий Schneider ConneXium помогает избежать проблем, связанных с неверным подключением кабелей

При установке, обновлении и техническом обслуживании сети информация о ее фактической топологии может оказаться неверной или устаревшей. В результате может случайно возникнуть кабельная петля, способная вызвать «широковещательную лавину» и повлиять на работу конечных устройств.

Кроме того, неправильное функционирование систем сторонних поставщиков может создать трафик, способный нарушить работу любых автоматизированных систем, а не только систем компании Schneider. Имеет смысл обеспечить условия, при которых, например, сетевой адаптер на неисправном ПК не мог бы генерировать избыточный трафик широковещательной рассылки или искаженные пакеты, нарушающие работу средств автоматизации.

• Настоять на использовании коммутаторов ConneXium компании Schneider Electric и разрешить работу протокола Rapid Spanning Tree Protocol (RSTP). Протокол RSTP коммутаторов ConneXium отключает случайно возникшую кабельную петлю в течение 1 секунды. Это позволяет предотвратить зацикливание пакетов данных при неверном соединении, причиной которого может стать устаревшая документация, неверная маркировка кабелей или неверная архитектура. Коммутаторы ConneXium с протоколом RSTP решают проблему подобных случайных ошибок, прежде чем она станет проблемой клиентов.

• Использовать функцию ограничения частоты широковещательной рассылки в коммутаторах, чтобы ограничить избыточный и потенциально опасный объем трафика широковещательных сообщений и защитить ответственные конечные устройства. Для каждого приложения, возможно, придется задать собственный предел частоты широковещательной рассылки.

• Предложить клиенту протестировать все новые модели ПК, серверы, ОС, сетевые интерфейсные платы и обновления драйверов, прежде чем вводить их в эксплуатацию в промышленной сети Ethernet.

• Предложить клиенту, чтобы все посетители использовали только разрешенные клиентом ПК и ноутбуки, чтобы конфигурация их личных ПК не приводила к конфликтам и не нарушала работу сети клиента.

Дополнительные меры, связанные с инфраструктурой коммутаторов ConneXium

• Ограничение доступа к MAC- и IP-адресам для предотвращения подключения неавторизованного ПК к контроллерам в сети Ethernet.

• Блокировка неиспользуемых портов коммутаторов Ethernet для предотвращения любого подключения к ним, за исключением авторизованного и разрешенного администратором.

• Правильная маркировка гнезд Ethernet-портов, документирование устройств и архитектуры для предотвращения неправильной коммутации устройств во время технического обслуживания.

• Обучение персонала работе с инструментальными средствами программирования для предотвращения непреднамеренной остановки контроллеров.

• Обучение обслуживающего персонала правильным методам соединений и основам эксплуатации Ethernet.

• Маркировка устройств с указанием IP-адресов для предотвращения ошибочного подключения контроллеров во время технического обслуживания.

• Обсуждения с коллегами порядка технического обслуживания и обновления для координации плановых остановов и отключений контроллеров.

• Согласование с представителями системных интеграторов порядка останова работы для обслуживания или ввода в эксплуатацию.

Обслуживание сетей клиентов

Перед обслуживанием сетей клиентов полезно получить точное представление о подключенных устройствах и топологии сети. Не следует предполагать, что имеющаяся в комплекте поставки документация является актуальной.

Средства диагностики промышленной сети Ethernet, такие как коммутаторы ConneXview, способны точно указать, как именно соединены между собой устройства. Это защитит пользователей от выбора неверного порта коммутатора при подсоединении или отсоединении устройства.

Коммутатор ConneXview является также ценным инструментом системных интеграторов и специалистов по обслуживанию сети клиента. ConneXview способен точно описать топологию сети и подключенные устройства вне зависимости от того, что говорится в документации клиента. Документы по сети могут оказаться устаревшими.

Функции контроля доступа в ПО Messaging and FactoryCast Web Configuration среды Unity компании Schneider Electric может ограничивать список устройств, которым разрешено обмениваться данными с ПЛК через Ethernet, чтобы предотвратить неавторизованное чтение или запись информации в контроллер со стороны устройства. Следует изучить функционирование инструментов, предусмотренных в аппаратных и программных продуктах с целью предотвращения неавторизованного доступа к конечным устройствам компании Schneider Electric.

Контактный телефон (495) 777-99-90.
Http:// www.schneider-electric.com