Безопасность промышленных предприятий в опасном мире кибератак

ЗАО "ВСП Лтд"

Показаны точки уязвимости АСУТП в результате возможных кибератак. Представлена стратегия "глубинной защиты" как средство обеспечения безопасной и надежной среды для функционирования АСУТП.

Ключевые слова: кибератака, вирус, брандмауэр, патч.

В разговорах о "компьютерной безопасности" или "кибератаках", нам представляются вирусы в электронной почте или хакеры, которые пытаются проникнуть в корпоративные сети или на Web-сайт. Эти проблемы, хотя и носят опасный характер, оставаясь в пределах Internet, кажутся далекими от производственных процессов. Мы не допускаем мысли о том, что может случиться, если какие-либо вирусы или хакеры могут проникнуть в критически важные системы управления производством, службы авиадиспетчерского контроля или нефтеперерабатывающих предприятий (НПЗ).

Недавний случай с компьютерным "червем" Stuxnet (http://www.tofinosecurity.com/stuxnet-central), заставил нас посмотреть на проблему по-другому. Stuxnet представляет собой компьютерный "червь", специально разработанный для поражения ТП, в которых используются системные продукты Siemens WinCC и PCS7 и STEP7. Что послужило причиной для создания этого вируса, и против кого он был направлен, окончательно не установлено, однако достоверно доказано, что вирус был создан с целью поражения производственного объекта.

Даже в том случае, отдельно взятое производство не является целью атаки, производственный процесс может существенно пострадать от сопутствующих потерь, вызванных обычными ИТ вирусами. В2003 г.операторы буровой вышки на Аляске ощутили на себе такой урок. Сначала они заметили, что периодически теряется связь между компьютерными терминалами и серверами SCADA, подключенными к буровым участкам. Затем стало очевидным, что периодически выходит из строя связь с контроллерами на буровых. Проблема развивалась быстро.Система управления стала работать настолько нестабильно, что могло вызвать возможнуюостановкуработывсей смены. Персонал доложил, что АСУТП подверглась массированной вирусной атаке – на пяти операторских ПК было запущено приложение, создающеебольшой трафик, которыйблокировалвсе маршрутизаторы и коммутаторы в сети автоматизированного управления.

Компьютеры, вызвавшие нарушения, были отключены от системы, сама система управления была выведена из корпоративной сети, и таким образом проблему удалось локализовать. Производство и буровые операции удалось вывести из-под удара с минимальными потерями. Непосредственный прямой ущерб был ограничен потерей данных по аварийным событиям в течение нескольких часов. Затраты на персонал по поддержке ИТоказались существенными, так как выяснение причин и устранение их последствий в системе управления заняло несколько недель.

В компании понимали, что в большой степени им просто повезло: во время происшествия основная система распределенного управления работала на базе специализированногоинтерфейса, и таким образом оказалась в безопасности. Однако в планах развития предприятия предполагалось заменить систему собственной разработкисо специализированным интерфейсом на стандартное решение, базирующееся наEthernet, так что в будущем ситуация могла бы сложиться намного хуже.

Анализ ситуации показал, что на системе был установлен хороший брандмауэр, но каким-то образом вирус его обошел. Возможно, присутствовала ошибка в конфигурации брандмауэра, может быть причиной явился зараженный портативный компьютер, который подключили к сети (несколькими месяцами позже такая же ситуация произошла в Луизиане на НПЗ). Возможно, виновником был модем дозвона.

Можно никогда не узнать, как вирус попал в систему, но факт состоит в том, что, однажды попав туда, вирус находит легкую цель и может реально причинить много вреда. Коммутаторы, отделяющие АСУ от корпоративной сети не были рассчитаны на защиту системы управления от вирусов – они были предназначены для ограничения передачи информации и упрощения администрирования сети; незащищенные компьютеры только ждали момента инфицирования.

ИТ безопасность не равнозначна безопасности системы управления

Независимо от того, каким образом вирус попал внутрь, существует ряд основных причин, предопределивших этот случай. Во-первых, на многих предприятиях обычно полагаются на ИТ специалистов в плане обеспечения безопасности систем, включая сюда и сферу АСУТП. Специалисты по ИТ отлично владеют способами обеспечения безопасности систем, которые им близки, таких как серверы под ОС Windows, различные БД и т.п. К сожалению, ИТ специалисты на многих больших предприятиях не всегда владеют в достаточной степени знаниями и пониманием АСУТП.

Например, многие АСУТП построены на базе специальных ОС и приложений, таких как VxWorks или SIMATIC™ STEP 7. Последние существенно отличаются от офисных решений. Это означает, что многие из проверенных решений по защите информационных систем не будут функционировать корректно или в процессе работы будут создавать помехи для АСУТП.

Более того, задачи по обеспечению ИТ безопасности отличаются от приоритетов АСУТП. ИТменеджер

по безопасности видит свою задачу, прежде всего, в обеспечении конфиденциальности, тогдакак для руководителя производства первоочередной и приоритетной целью является безопасность человека и объекта управления. Разная постановка задачи перерастает в огромную разницу в реализуемой практике безопасности. Например, использование стандартной процедуры блокирования при помощи пароля просто неприемлемо для большинства операторских станций в диспетчерской – здесь операторский доступ по умолчанию предпочтительнее, чем просто блокировка, что противоречит ИТ представлениям. Представьте, что во время аварийной ситуации на НПЗ оператор в панике ошибочно три раза вводит неправильный пароль, в результате чего блокируется любой доступ в течение ближайших 10 минут. Блокировка по паролю представляется правильным подходом для защиты ИТ серверов, но однозначно не подходит для работы в диспетчерской нефтяной компании или завода.

Не будем утверждать, что решения по информационной безопасности непригодны для промышленных предприятий. Напротив, опыт крупных нефтяных компаний показывает, что 90% всех стратегий и технологий ИТ безопасности хорошо работают в области промышленных систем управления. Решение вопроса лежит в четком понимании требований промышленных технологий и их отличия от офисных технологий с последующим правильным применением модификаций ИТ в сфере АСУТП. Для этого требуется тесное сотрудничество ИТ специалистов с инженерами АСУ, а не слепое копирование процедур ИТ защиты.

Помните о Линии Мажино

Другим виновником описываемого инцидента, случившегося на Аляске, явился сам подход к концепции безопасности, который основывался на так называемой "модели бастиона". По аналогии со знаменитой системой укреплений, которая должна была защитить французскую армию от немецкой в начале Второй Мировой войны, модель бастиона основана на идее укрытия всех ключевых ресурсов за единой монолитной стеной – решением по обеспечению безопасности. В данном случае под бастионом понимался один межсетевой экран (брандмауэр) между производственной сетью и Internet.

К сожалению, нефтяная компания обнаружила, что при реализации модели бастиона возникают предпосылки к отказу в одной точке, чего неизбежно. По закону Мэрфи можно либо избежать отказа, либо отказ обязательно произойдет в этой точке. И когда эта ситуация наступает, производство остается абсолютно незащищенным.

Многие компании также полагают, что угрозы безопасности возникают за пределами предприятия, а пути проникновения носителей угрозы очевидны, и с ними можно справиться при помощи одного экрана защиты. Вся концепция безопасности этих компаний строится на установке одного брандмауэра между производственной сетью и сетью управления и предполагается, что такой брандмауэр будет наилучшим защитным фильтром, предотвращающим проникновение в систему управления любого вредоносного элемента. Однако при зарождении проблемы изнутри межсетевой экран не приносит большой пользы.

Internet - это модель нашей жизни. Она делает добро, объединяя людей, и страшное зло, заражая вирусами миллионы компьютеров.

Г. Александров

Много дорог ведет в систему управления

Чтобы понять, почему модель бастиона не выдержала атаки, можно в качестве примера рассмотреть вирус SlammerWorm и изучить, как он воздействал на системы управления со времени своего создания в 2003 г. Согласно отчетам Информационного архива нарушений промышленной безопасности (RISI) (США) только один этот вирус отвечает за большую часть зарегистрированных нарушений в производственных процессах, чем какой-либо иной источник. В числе его "достижений" – поражение SCADA и нарушение энергоснабжения, инфицирование системы отображения параметров безопасности (SPDS) на предприятии атомной энергетики и прерывание операций по добыче нефти в Мексиканском заливе.

Особенно интересным является тот факт, что вирус Slammerworm использовал, по крайней мере, пять различных путей для проникновения в систему управления своей жертвы. В одном случае он проник в систему управления нефтяной компании через обслуживающий портативный компьютер, который использовался сотрудником дома (и был инфицирован), а затем был перенесен на предприятие. В другом случае – через модем дозвона вирус повредил интерфейсное устройство, которое применялось для дистанционной поддержки управления. В третьем случае вирус проник напрямую через плохо сконфигурированный брандмауэр. Во всех этих примерах межсетевые экраны были установлены, однако вирус либо обошел их, либо нашел уязвимые места в самих брандмауэрах.

Вирус Slammer является всего лишь одним из примеров – анализ 175 случаев нарушения безопасности в отношении систем управления в период 2002-2010 гг. говорит о том, что около половины вирусных атак извне приходится на вторичные пути проникновения, такие как соединения дозвона, беспроводные системы и мобильные устройства. Во всех этих случаях брандмауэр выполнил свою функцию, а стратегия защиты дала сбой.

В некоторых случаях брандмауэр пропускает через себя атаки и вирусы. Это обычно является не слабостью самого брандмауэра, а скорее вызвано его конфигурацией. Обычный брандмауэр требует значительного опыта при его разработке, вводе в эксплуатацию и поддержании. Сложность этой задачи часто

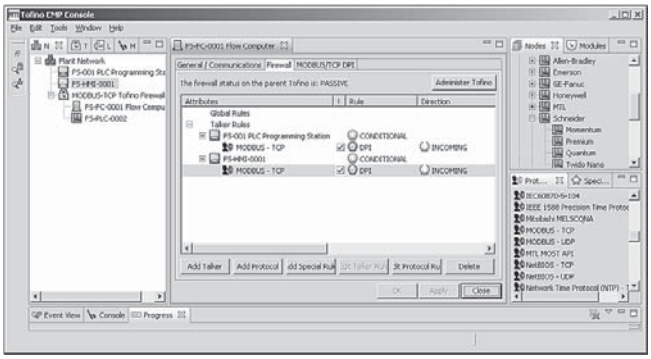

Рис. 1

недооценивается. В классической работе 2004 г., посвященной ошибкам при конфигурации брандмауэра, доктор Авишай Вул указал на то, что многие брандмауэры в крупных корпорациях обладают слабо составленным набором правил и подвержены атакам. Он дал определение 12 серьезным конфигурационным ошибкам и затем провел анализ конфигураций брандмауэров в 37 крупных корпорациях. В среднем было выявлено по семь серьезных ошибок на каждый брандмауэр, в некоторых случаях число ошибок достигало 12 ед.

Если эту статистику распространять на защищаемые брандмауэрами производственные системы, неудивительно, что кибератаки в конце концов достигают систем управления в случае установки только брандмауэра.

Может возникнуть мысль о том, что брандмауэр бесполезный инструмент, но это утверждение далеко от истины. Брандмауэр не является слабой технологией, фактически – это прекрасный элемент в наборе защитных инструментов. Но промышленность вместо применения всего арсенала инструментов, использует всего лишь одно защитное средство.

Мягкие и вполне съедобные внутри

Проникший через основной межсетевой экран вирус, или хакер, или простая небрежность персонала могут вызвать ситуацию, когда система управления станет легкой добычей. На предприятиях установлено множество компьютеров, работающих под ОС Windows, а антивирусное ПО скорее исключение, чем правило. Например, в результате аудита безопасности на крупном НПЗ в 2006 г. было обнаружено, что только 55% компьютеров с ОС Windows 2000/XPв диспетчерской имеют патчи, предотвращающие бластерные инфекции, и еще меньше (38%) имеют установленные патчи для защиты от вируса Sasser. И это несмотря на то, что оба патча были одобрены поставщиком системы управления во время аудита. Даже малоопытный хакер мог бы проникнуть в такую систему управления в течение нескольких часов.

ПЛК или распределенные системы управления (РСУ) являются еще более легкими мишенями, чем ПК. В исследованиях CERN, Европейской лаборатории физики высоких энергий, 25 промышленных устройств управления были протестированы при помощи стандартных программных инструментов ИТ защиты (Nessus и Netwox), свободный доступ к которым может получить любой начинающий хакер. Почти треть устройств не прошла тестирование большей частью из-за отказов по связи, полного отказа системы или незащищенных сервисных функций. Эти результаты не были так уж и удивительны – в большинстве ПЛК и РСУ не используются механизмы авторизации, целостности данных или конфиденциальности, и устройство может полностью контролироваться любым лицом, способным "перебрасывать информацию" на него. Кроме того, сложно обновлять ПО этих устройств или загружать в них дополнительные средства защиты.

Построение безопасной системы управления № 1 – Определение зон защиты

Каким образом предприятие может защитить жизненно важную систему управления? Прежде всего, необходимо осознать, что любая надежная стратегия защиты военная, физическая или кибернетическая должна быть основана на концепции "Глубинной защиты". Эффективная защита создается путем определения границ с последующим наслоением многочисленных решений защиты так, что, если одно из них обходится, другие решения обеспечивают защиту. Принцип – не полагаться чрезмерно на какую-то одну технологию также лежит в основе стратегии.

Современные промышленные стандарты, такие как ANSI/ISA-99 и IEC 62433 трактуют эту технологию, как модель защиты "зон и информационных каналов".

Промышленный объект сначала делится на различные зоны защиты с учетом функций управления, типичных пользователей и потенциальных последствий отказов. Затем каналы защиты используются для связи между зонами с брандмауэрами или кодовыми устройствами, которые управляют каналами. Например, на НПЗ система безопасности (SIS) может быть в одной зоне, система управления – в другой зоне, архивные данные – в третьей зоне, а сеть ИТ – в четвертой зоне. Нарушения защиты в любой из этих систем могут привести к разным последствиям, поэтому имеет смысл рассмотреть каждую отдельно.

Разработка глубинной защиты для зоны начинается с определения четкого электронного периметра вокруг каждой зоны системы управления с последующим укреплением устройств внутри нее. Периметр защиты для зоны определяется правилами и технологией. Прежде всего, правило определяет, что относится к сети зоны, а что нет. Затем брандмауэр зоны работает как канал передачи данных между другими зонами и устройствами управления в пределах зоны.

Правильно разработанная и реализованная защита системы управления является критичным фактором. Замена настоящей защиты маршрутизаторами или коммутаторами не решает вопроса защиты и бе-

зопасности. Крайне важно, чтобы брандмауэр разрабатывался специально для промышленных систем, а не для офисных. В качестве примера можно привести брандмауэры, специально разработанные для работы с промышленными протоколами, такими как ModbusTCP или OPC (рис. 1).

Построение безопасной системы управления № 2 – укрепление системы управления

После обеспечения защиты электронного периметра зоны необходимо построить вторичные уровни защиты самих устройств системы управления. Для компонентов системы управления (таких как человеко-машинные интерфейсы и средства архивации), которые базируются на традиционных ОС, таких как Windows, можно воспользоваться проверенными ИТ стратегиями установки патчей и антивирусного контроля.

Рис. 2

Многие специалисты АСУ ошибочно полагают, что в рамках системы управления невозможно реализовать использование патчей и антивирусных программ. Безусловно, неразборчивый подход к применению этих программных средств неоправдан, однако безопасное внедрение патчей и антивирусных программ вполне возможно. Ряд ведущих производственных компаний продемонстрировали, что политика правильного применения патчей и антивирусных программ помогает сбалансировать требования к надежности системы и обеспечению ее безопасности. На сегодняшний день большинство поставщиков систем управления дают рекомендации по правильному применению патчей и антивирусных программ для своих систем управления. Поэтому в рамках системы управления резонно обеспечить технологические компьютеры хорошими программными инструментами защиты – патчами и антивирусным ПО.

Защищая самое ценное

К сожалению, для критических с точки зрения управления устройств, таких как ПЛК, мобильные терминалы в настоящее время патчи или антивирусные решения не разработаны. Вместо этого рекомендуется применение оборудования промышленной безопасности. Решения по безопасности основаны на использовании экономичных модулей безопасности, которые устанавливаются непосредственно перед каждым устройством управления (или группой устройств), нуждающемся в защите.

Оборудование промышленной безопасности обеспечивает локальную защиту важнейших устройств управления подобно тому, как персональные брандмауэры (например,Windows® Firewall) и антивирусное программы обеспечивают локальную защиту настольных компьютеров. При этом, если даже хакер или вирус смогут проникнуть через брандмауэр периметра, они столкнуться с множеством целевых защитных устройств элементов управления, которые им придется взломать, прежде чем они смогут причинить какой-либо ущерб.

Примером решения защиты данного типа является брандмауэр HoneywellModbusTCP и решение промышленной защиты устройствами Tofino™ (рис. 2). Первое представляет собой небольшой модуль, предварительно сконфигурированный для защиты контроллеров Honeywell от возможной вирусной атаки. Защита направлена на определенное промышленное устройство управления, что делает его простым для установки персоналом.

Также просто устанавливается и новое уникальное решение Tofino™от MTLInstruments и ByresSecurityInc., при этом не возникает сложностей в конфигурировании. Инженеры-наладчики устанавливают его между устройством управления и остальной сетью и подают питание. Конфигурирование, мониторинг и управление устройством может также обеспечиваться с центральной платформы управления, расположенной в любой точке корпоративной сети. Разработанное специально для защиты важнейших устройств управления, а не всей сети, это оборудование можно индивидуально конфигурировать в соответствии с требованиями по защите промышленных систем.

Таким образом, только комплексная защита, в которой устройства управления и системы, оснащаются индивидуальными и коллективными средствами безопасности, может обеспечить надежное функционирование производства.

Официальный дистрибьютор MTLInstruments на рынке России, СНГ и Украины – компания ЗАО "ВСП Лтд".

Http://www.vsp-co.org