Информационная безопасность в управлении промышленными объектами

Н.А. Захаров (Журнал "Автоматизация в промышленности")

Рассматривается имеющаяся статистика по учету компьютерных атак в области промышленных ИТ. Показаны потери, к которым приводят компьютерные атаки на производстве. Рассматриваются пути проникновения внешних воздействий в системы управления. Указываются меры борьбы с компьютерными атаками, которые разрабатывают в Управлении национальной безопасности (NSA) США. Рассматривается программно-технический комплекс компании Verano (США) – Industrial Defender, предназначенный для контроля и защиты инфраструктуры критически важной системы управления от внешних и внутренних угроз.

В сегодняшней обстановке расширяющихся угроз безопасности ИТ, включающих троянские программы, вирусы, червей, DoS-атаки и даже кибертерроризм, компании, эксплуатирующие критически важную инфраструктуру, сталкиваются с неизбежной необходимостью адекватного обеспечения безопасности систем управления и сетей с целью снижения риска и избежания разрушительных последствий таких, как потеря критически важных данных, перебои в работе, отключения электроэнергии и угроза общественной безопасности. Традиционные решения для предприятий не укомплектованы средствами обеспечения безопасности АСУТП, блокирующими несанкционированный доступ к оборудованию, работающему в сетях управления промышленными объектами. Трагические события 11 сентября 2001 г. требуют пересмотра сложившегося подхода к различным аспектам безопасности, включая информационную безопасность систем управления объектами промышленности и инфраструктуры.

Многие организации с неохотой сообщают об инцидентах, связанных с безопасностью. Они часто отрицают само существование риска компьютерных атак. Например, существует точка зрения, что нет риска атак по сети на SCADA-системы, используемые в водоснабжении, поскольку в каждой инсталляции они индивидуально сконфигурированы, поэтому для их взлома требуются дополнительные специфические знания.

Наряду с этим задокументированы такие инциденты в области информационных технологий, как проникновение червя Slammer на атомную электростанцию в г. Огайо (США) и несколько других предприятий энергетики, атака по беспроводным линиям связи на SCADA-систему очистных сооружений в г. Квинсленде (Австралия). Очевидно, слияние общепринятых информационных технологий таких, как Ethernet, Windows и Web-службы с технологиями управления в промышленности устранило сомнительный барьер "безопасности из-за непрозрачности".

Промышленные системы управления, очевидно, сталкиваются с некоторой степенью риска, которую следует оценить, хотя это и непросто. Нельзя игнорировать риск, но при этом нет возможности платить бесконечную цену за идеальную защиту. Разумный деловой подход требует баланса между ценой за меры по устранению риска с потенциальной стоимостью ущерба от возможного события. Это требует понимания составляющих риска для промышленного предприятия. Кроме того, необходимо постоянно отслеживать эти составляющие риска, чтобы обнаружить их изменения. Для достижения технической и экономической эффективности такой подход должен адаптироваться к изменениям видов угроз, точек уязвимости систем и выбора потенциальных для атаки целей. К сожалению, эти составляющие быстро меняются и требуют постоянного внимания.

Технологический университет Британской Колумбии (Канада) поддерживает БД инцидентов в области безопасности ИТ в промышленности, предназначенную для учета событий, непосредственно влияющих на системы управления и ТП. Регистрируются как случайные инциденты, так и умышленные действия такие, как попытки взлома извне, DoS-атаки и заражения вирусами/червями.

Данные собираются из открытых источников и конфиденциальных сообщений компаний-участников, желающих иметь доступ к БД. Каждое событие анализируется и затем оценивается в соответствии с надежностью информации.

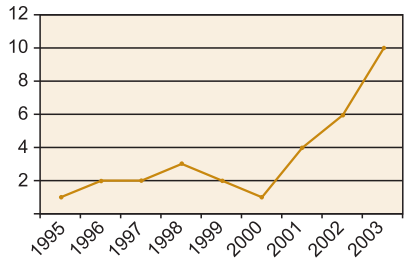
На сегодня проанализировано и занесено в БД 41 событие, еще 11 инцидентов ожидают расследования. Из них семь отмечены как ложные, а 34 оставлены для статистического анализа. На рис. 1 показан тренд событий в период с 1995-2003 гг. Видно резкое увеличение возникновения событий около 2001 г. Это означает или фактическое возрастание числа атак, или является результатом более пристального внимания к сбору данных. Данные от других исследователей и опыт систематизации обычных криминальных инцидентов в бизнесе свидетельствует о том, что потерпевшие организации сообщают об одном из 10 случаев. Если этот процент сообщений применить к преступлениям в области ИТ, в настоящее время должно происходить, по меньшей мере, 100 инцидентов в год.

В 1982-2000 гг. произошли 13 инцидентов, которые делятся примерно поровну на случайные, имеющие внутренние причины и внешние, при этом только треть событий возникли вовне компании. Случайности, неправильные действия сотрудников и недовольные сотрудники создавали большинство проблем. Это хорошо коррелируется с цифрами, которые в это время сообщали исследователи в области безопасности в традиционных ИТ.

В период 2001-2003 гг. вызванные извне инциденты насчитывали около 70% от общего числа. В мире ИТ наблюдается аналогичная тенденция. Консалтинговая компания Deloitte & Touche Ross обследовала 80 финансовых компаний из списка Fortune 500 в рамках своего глобального исследования в области безопасности в 2003 г. Установлено, что 90% брешей в защите компаний пробито извне, а не произошли по вине недобросовестных сотрудников.

Что объясняет изменение угрозы за такое короткое время? С промышленными системами управления связаны несколько возможностей. Опасность автоматических атак червями, начиная с Code Red в июле 2001 г. (Code Red был не первым почтовым червем, но он оказался первым, имевшим существенное проникновение в промышленные системы) означает, что многие проникновения стали ненаправленными и автоматизированными. Системы управления оказываются скорее случайными целями, а не выбранными осознанно.

ОС и приложения общего применения (Windows 2000, Linux, SQL сервер, Explorer, и т.д.) сейчас преобладают в ЧМИ, инженерных станциях и архивах данных. Они часто поставляются с ядром, написанном на кодах для бизнес-приложений, поэтому они уязвимы для обычных ИТ атак и вирусов. Сложности в установке патчей на промышленные системы усугубляют проблему.



Инциденты в период 1995-2003 гг.

Увеличивающееся число соединений между критически важными системами создало взаимозависимости, которых ранее просто не было. Инцидент с червем Slammer, описанный Североамериканским советом по надежности в электроэнергетике, свидетельствует о том, что Internet может косвенно воздействовать на системы, которые его вообще не используют. В этом случае энергосистема использовала ретрансляцию кадров для своей SCADA-сети, считая транспортную систему безопасной. К несчастью, провайдер ретрансляции кадров использовал общую систему асинхронной передачи в своей сетевой магистрали для различных служб, включая коммерческий трафик Internet (наряду с трафиком SCADA). Ресурсы пропускной способности были переполнены червем, что заблокировало трафик SCADA к подстанциям.

Источники угрозы перемещаются изнутри вовне независимо от причины, и это следует принимать во внимание в процессе оценки риска. Правительственные исследования угроз критически важной инфраструктуры предоставляют превосходную отправную точку для аналитиков риска.

Если угрозы все более становятся внешними, возникает вопрос о путях проникновения. Очевидным путем являются подключения к Internet, но это не единственный путь. Например, зарегистрировано не менее четырех путей проникновения червя Slammer в системы управления:

- в компьютер системы управления и системы отображения параметров безопасности АЭС Davis-Besse – через арендованную линию T1;
- в SCADA-систему электроснабжения – через виртуальную частную сеть;
- в систему управления в нефтепереработке – через лаптоп;
- в ЧМИ бумагоделательной машины – через модем.

Основным источником внутренних инцидентов являются сети, предназначенные для бизнеса. Для внешних событий большинство точек проникновения дает Internet, но свой вклад также вносят модемные соединения, виртуальные частные сети, беспроводные системы. Отсюда следует очевидный вывод, что современная SCADA-система или АСУ имеют несколько вероятных точек проникновения. Фокусировка на одной точке проникновения (например, брандмауэр Internet) может привести к пропуску других потенциальных точек нападения.

Оценка последствий ИТ атак в промышленности не сводится к простому присвоению инциденту финансовой величины. Хотя имеются очевидные и легко обсчитываемые потери (продукции, повреждение оборудования и другие, последствия которых могут быть не столь очевидными). Ущерб репутации может оказаться более существенным, чем цена простоя производства. Инциденты, касающиеся здоровья, безопасности или ущерба окружающей среде, могут серьезно повредить имиджу бренда компании. Даже эффекты, ведущие к незначительному нарушению нормативов, могут поставить под угрозу репутацию компании или ее лицензию на право работы.

Для большинства занесенных в БД событий участники не смогли (или не захотели) предоставить подробности финансовых последствий, связанных с ИТ атаками в промышленности: менее третьей части сообщений содержат такие оценки. Хотя выборка невелика, кажется существенным, что около половины организаций, детализировавших финансовые последствия, сообщили, что убытки превысили 1 млн. долл. США.

Примечательна природа эффекта атак. 41% пострадавших предприятий сообщили о потерях продукции, в то время, как 29% сообщили о потере возможности наблюдать за оборудованием или управлять им. К счастью, о травмировании персонала сообщений минимум – всего один неподтвержденный (и, возможно, ненадежный) отчет, включающий смертельный случай. В общем, зарегистрированные события ясно показывают, что наиболее вероятные последствия ИТ атаки в промышленности касаются потери наблюдаемости или управляемости процесса.

Заблокированное управление процессом или системой возлагает повышенные ожидания на резервные системы защиты. Традиционно эти системы независимы от основной системы управления и, поэтому, заслуживают доверия. Однако эти системы защиты все больше используют стандартные ИТ (такие, как TCP/IP) и обычно подключаются в некоторой точке к главной системе управления; это увеличивает потенциальный риск отказа общего узла основной и защитной систем. При проектировании

Больше всех рискует тот, кто не рискует.
А.И. Бунин

как основной системы управления, так и системы защиты следует учитывать системные риски ИТ атак. Хакерское сообщество становится все более компетентным в SCADA и системах управления и начинает рассматривать их в качестве более привлекательных целей, чем Internet-сайты.

На конференции в г. Ванкувер в мае 2003 г. рассматривался вопрос осуществления атак на встроенные ОС, используемые в маршрутизаторах, принтерах и сотовых телефонах. Эти же встроенные системы находят использование в современных SCADA-системах и оборудовании АСУ. Все это вместе ясно свидетельствует о том, что хакерское сообщество обладает интересом к нападению на системы управления и соответствующей квалификацией.

Для реализации защиты промышленной системы требуется, по меньшей мере, четыре шага. На уровне проектирования системы рекомендуется в большем объеме использовать защиту внутренней зоны и средства обнаружения проникновения. Компаниям также может потребоваться заново оценить защиту границы в целом, не ограничиваясь очевидными подключениями такими, как связь с бизнес-процессами. Один брандмауэр между сетью офиса и сетью системы управления может пропустить многие проникновения и не обеспечивает безопасности, если злоумышленник получил доступ к сети системы управления.

Со стороны изготовителей систем управления, SCADA и технических средств автоматики требуется проектирование и тестирование с позиций надежного обеспечения безопасности перед развертыванием в поле. Требуется обновление протоколов с включением в них функций защиты: многие устройства в настоящее время уязвимы даже для простейших атак и не имеют никаких механизмов аутентификации/авторизации для предотвращения управления злоумышленником.

Отсутствие адаптации к изменяющимся угрозам и уязвимостям делает мир управления все более подверженным ИТ атакам. Результатом может оказаться потеря репутации, ущерб окружающей среде, потеря продукции и денег и даже травмирование людей.

В США реализуется программа защиты критически важной инфраструктуры, целью которой является повышение к 2007 г. безопасности компьютерных систем, управляющих производством в критически важных отраслях промышленности, включая электроэнергетику, водоснабжение, химию, фармацевтику, металлургию, нефтяную, газовую, горнодобывающую, целлюлозно-бумажную промышленность и производство товаров длительного пользования путем:

1. определения и применения стандартов информационной безопасности;

2. разработки руководств по внедрению мер информационной безопасности и оказания помощи нуждающимся в ней;

3. разработки лабораторных и полевых методик тестирования продуктов и приложений информационной безопасности в области управления в промышленности.

Компьютерные системы, управляющие промышленным производством и распределением, были спроектированы, в первую очередь, чтобы удовлетворять требованиям к производительности, надежности, безопасности и гибкости. Сейчас эти системы все больше приобретают способность к удаленному доступу. Промышленность начала принимать во внимание, что открытость придает серьезную уязвимость используемым ОС. Одной из серьезных проблем, требующих немедленного реагирования, является отсутствие методик специфицирования и проверки характеристик безопасности компонентов систем управления и сетей. На решение этой проблемы нацелены Общие критерии оценки ИТ безопасности, разработанные Национальным институтом стандартов и технологий (NIST) и Управлением национальной безопасности (NSA) США.

Чтобы разработать требования ИТ безопасности для систем управления в промышленности, NIST возглавляет Форум по требованиям к безопасности в управлении процессами (Process Control Security Requirements Forum – PCSRF), рабочую группу, состоящую из поставщиков и пользователей АСУТП. В PCSRF участвуют Институт исследований в области электроэнергетики (Electric Power Research Institute – EPRI), Общество приборов, систем и автоматизации (Instrumentation Systems and Automation Society – ISA), Sandia Labs и другие лаборатории Министерства энергетики, Американская газовая ассоциация (AGA), Институт газовых технологий (Institute for Gas Technology – IGT), Ассоциация городских служб водоснабжения (Association of Metropolitan Water Agencies – AMWA), Открытая группа Института инженеров по электротехнике и электронике (Institute for Electronic and Electrical Engineers – IEEE), Национальный технологический центр (National Center for Manufacturing Sciences – NCMS) и отдельные компании. В рамках PCSRF предпринимаются следующие шаги:

- разработка требований информационной безопасности в управлении ТП для существующих в настоящее время архитектур компьютерных систем управления, включая анализ угроз и уязвимостей;
- разработка требований информационной безопасности на языке и в формате, понятном пользователям и поставщикам АСУТП;
- трансляция требований информационной безопасности в общепринятые критерии. Профили защиты, определенные международным стандартом ISO 15408, общие критерии оценки безопасности информационных технологий могут быть использованы для тестирования и оценки компьютерных продуктов и систем управления аккредитованными лабораториями информационной безопасности.

Фирма Verano (www.verano.com, г. Мансфилд, шт. Массачусетс, США) представляет продукт Industrial Defender, предназначенный для контроля и защиты инфраструктуры критически важной системы управления от внешних и внутренних угроз и обеспечения надежной безопасной

среды функционирования оборудования. Это законченное решение, состоящее из устройства защиты периметра, предназначенного для блокировки потенциально вредоносного трафика, системы мониторинга безопасности для обнаружения и обработки событий, касающихся безопасности, и полный набор служб для планирования и проведения защитных мероприятий.

Industrial Defender – это всеобъемлющее интегрированное многоуровневое программно-техническое средство организации безопасности. Изготовитель позиционирует его как единственное доступное сегодня решение, удовлетворяющее уникальным потребностям критически важных производств и управляющих сетей. Данный продукт функционирует в среде RedHat с расширением SELinux Industrial Defender, в РВ обеспечивает постоянный контроль, обнаружение угроз, информирование и защиту систем управления через простой дружественный пользовательский интерфейс.

Упомянутое выше защитное устройство Guard полностью интегрировано с Industrial Defender и доступно через единый операторский интерфейс. Впервые безопасность системы управления и сети оказалась в руках инженера АСУТП, а не отдела ИТ.

Linux наследует многие концепции, включая безопасность и контроль доступа, от ОС Unix, имеющей большую историю применения в критически важных приложениях. Linux работает на ПК широкого применения, но обеспечивает живучесть и устойчивость, необходимые наиболее требовательным приложениям. Linux по своей природе менее уязвима для вирусов и иного злонамеренного кода, который может атаковать домашние компьютеры. Базовая структура ОС усложняет вставку и исполнение такого кода, в то время как система разрешений минимизирует потенциальный ущерб. В Linux также легко реализуется отключение ненужных служб, чтобы избежать их уязвимостей. Большинством дистрибьюторов Linux поставляется дополнительное ПО для защиты файлов паролями, создания виртуальных частных сетей и встраивания программных брандмауэров.

Как и их коммерческие собратья, стандартные дистрибутивы Linux используют средства избирательного контроля доступа. NSA улучшила Linux, создав одну из наиболее передовых, среди доступных в данный момент, систему безопасности: Security Enhanced Linux (или SELinux), которая разработана, чтобы удовлетворить жестким требованиям NSA, предъявляемым к безопасным ОС. Она поставляется в виде модуля к дистрибутиву Red Hat 7.3.

SELinux – это единственная ОС, которая может обеспечить высокую степень внутренней защиты и изоляции для критических приложений. Фирма Verano адаптирует эту технологию в качестве основы своего семейства продуктов Industrial Defender, поскольку органически присущая ей способность защищать приложения и информацию на уровне ОС обеспечивает последний рубеж обороны.

Устройство защиты периметра для применения в промышленности Industrial Defender™ Guard, обеспечивает безопасность систем управления. Оно ориентировано, в первую очередь, на применение в производстве и распределении электроэнергии, водоочистке, переработке отходов и на транспорте. Industrial Defender Guard также имеет функцию динамической блокировки (подана заявка на патент), ориентирующуюся на уровни угрозы безопасности, определяемые Министерством внутренней безопасности (Department of Homeland Security – DHS) США. При повышении уровня угрозы Industrial Defender Guard предоставляет простые средства для быстрой изоляции промышленного оборудования на основе предопределенных правил, динамически изменяя доступ к управлению для защиты критически важных систем.

Устройство Industrial Defender Guard спроектировано для установки в существующие системы в точке подключения внешней сети, обеспечивая блокировку неавторизованных пользователей и вредоносного содержимого. Архитектура на основе специализированных интегральных схем обеспечивает противодействие вторжениям, антивирусное сканирование по сети, фильтрацию содержимого и функции шлюза виртуальной частной сети.

Основные функции Industrial Defender Guard:

- блокировка доступа неавторизованных пользователей к сети на производстве, инспектирование в РВ трафика Web, E-mail и FTP при помощи брандмауэр, построенного на основе специализированных интегральных схем;
- сетевая антивирусная фильтрация защищает уязвимые системы управления, которые не могут использовать офисные антивирусные продукты;
- распознавание и уничтожение вредоносного трафика до того, как он достигнет критически важных систем, средствами встроенной системы противодействия вторжениям;
- поддержание виртуальных частных сетей для установки безопасных зашифрованных связей с удаленными пользователями;
- обеспечение быстрой надежной реакции в периоды повышенной угрозы при помощи менеджера правил с функцией немедленной блокировки;
- полная интеграция с Industrial Defender обеспечивает контроль и управление средствами одного дружественного операторского интерфейса.

Основанная в 1996 г. компания Verano, Inc. является сегодня ведущим поставщиком решений в области безопасности для промышленных объектов. Она поставляет свои системы для более, чем 220 предприятий энергетики, коммунального хозяйства, транспорта и промышленности. Число инсталляций систем Industrial Defender в мире превышает 2200.

Захаров Николай Анатольевич *– канд. техн. наук, член редакционного совета журнала "Автоматизация в промышленности". Контактный телефон (095) 980-73-80.*

При подготовке обзора использовались следующие источники: ethernet.industrial-networking.com, www.mel.nist.gov, www.verano.com