РЕШЕНИЯ CISCO SYSTEMS ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ ТРАНСПОРТА

События 11 сентября 2001 года в США ясно показали, что безопасность является в современной транспортной отрасли задачей номер один. Поэтому одной из стратегических целей Транспортной стратегии Российской Федерации до 2020 года, разработанной Министерством транспорта, является повышение комплексной безопасности и устойчивости транспортной системы России. При этом термин «комплексность» подразумевает решение не только вопросов антитеррористической направленности и физической безопасности. Нельзя забыть и о безопасности современных информационных технологиях, повышающих эффективность и конкурентоспособность транспортной системы России.

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ НА ТРАНСПОРТЕ

Своевременное получение информации о транспортной системе (будь-то аэропорт, железная дорога, морской порт или любые другие ее участки) является важным фактором, обеспечивающим выработку оптимального решения по управлению и обслуживанию транспортом. Современные информационные технологии позволяют решить эту задачу и в любой момент времени иметь информацию о местоположении транспортного средства и его состоянии. Особенно важную роль эти технологии должны играть при принятии решений в экстремальных и аварийных ситуациях.

Все большее число транспортных предприятий переходят на использование современных информационных систем, автоматизирующих многие процессы управления и контроля самолетами, кораблями, поездами и автомобилями. Однако недооценка вопросов информационной безопасности при внедрении таких систем может привести к серьезному экономическому (например, вследствие простоев транспорта по причине выхода из строя системы управления товаро- или пассажиропотоком или вследствие утечки информации о перевозимых грузах) или иному ущербу (например, потеря репутации, иски со стороны пострадавших сторон и т.д.).

СБОИ ВОЗМОЖНЫ

Летом 2004 года в Великобритании в результате сбоя в работе диспетчерских компьютеров нарушено воздушное движение. По словам представителя компании British Airways, сбой в работе ПК в главном центре Национальной службы управления воздушным движением в г. Суонвик на юге Англии произошел в 6 часов утра по местному времени. В результате в нескольких аэропортах были отменены все внутренние и международные рейсы.

Компания Cisco Systems помогает решить большинство возникающих в области информационной безопасности задач, начиная от проектирования среды передачи данных в защищенном исполнении и заканчивая внедрением средств обнаружения и предотвращения несанкционированных действий, происходящих как изнутри транспортной системы, так и направленные на нее снаружи.

CISCO SELF-DEFENDING NETWORK

Компания Cisco Systems, в отличие от других поставщиков, предлагает своим заказчикам не точечные продукты для защиты отдельных участков информационной системы, решающей задачи железнодорожного, морского, автомобильного и авиационного транспорта, а комплексное решение, интегрируемое в инфраструктуру предприятия для обеспечения информационной безопасности бизнеса на всех уровнях.

Self-Defending Network (SDN) – стратегия компании Cisco Systems, нацеленная на защиту бизнес-процессов в условиях растущей угрозы со стороны вредоносных программ и злоумышленников, воздействующих на бизнес-процессы транспортного предприятия изнутри и извне.

Учитывая скорость распространения современных угроз, например червей и вирусов, средства защиты компании Cisco Systems строятся на основе проактивного подхода, заключающегося в предвосхищении угроз, а не в борьбе с их последствиями. В основе SDN лежит интеграция механизмов безопасности в сетевую инфраструктуру, в которой все ее элементы – от персонального компьютера до сетевого оборудования, участвуют в процессе обеспечения защищенности, устойчивости и непрерывности бизнеса.

Стратегия Self-Defending Network заключается в автоматизации процесса обеспечения информационной безопасности за счет обнаружения угроз, реагирования соответственно уровню критичности, изолирования зараженных или взломанных узлов, и реконфигурации сетевых устройств с целью предотвращения повторных атак. При этом решения, входящие в Self-Defending Network одинаково эффективно защищают и распределенную инфраструктуру транспортного предприятия, и его корпоративную сеть.

ЗАЩИТА КОРПОРАТИВНОЙ СЕТИ И ИНФРАСТРУКТУРЫ ТРАНСПОРТНОГО ПРЕДПРИЯТИЯ

Защита информационной сети предприятия и ее инфраструктуры в рамках стратегии Self-Defending Network достигается за счет правильного применения совокупности трех основных элементов:

Защита от вторжений (Threat Defense). Наиболее эффективная защита бизнес-ресурсов предприятий транспортной отрасли от злоумышленников и вредоносных программ достигается только в случае эшелонированной обороны, распределенной по всей сети (включая и ее периметр, и ее внутренние сегменты), а не сосредоточенной в одной точке. Стратегия Threat Defense System интегрирует различные защитные механизмы в маршрутизаторы и коммутаторы, предлагает выделенные защитные устройства для разграничения доступа (Cisco Pix Firewall и Cisco ASA 5500 Series), отражения атак и контроля Web-контента (Cisco IPS 4200 и Cisco Content Engine), а также позволяет защищать конечные устройства, такие как сервера и рабочие станции от широкого спектра угроз (Cisco Security Agent).

ХАКЕРЫ ВТОРГАЮТСЯ В СИСТЕМЫ УПРАВЛЕНИЯ ТРАНСПОРТОМ

В 2000 году Управление гражданской авиации Великобритании выпустило предупреждение относительно новой угрозы для пассажиров воздушных судов, исходящей от хакеров: преступные хулиганы вторгаются в переговоры авиадиспетчеров и пилотов, посылая ложные команды или поддельные экстренные вызовы. Число инцидентов неправомочного использования радиочастот, принадлежащих службам управления авиаперевозок Великобритании, растет год от года.

Защищенное взаимодействие (Secure Connectivity). Распределенность транспортной системы требует обеспечения защиты данных, передаваемых по открытым каналам связи (например, через Интернет). Сохранение конфиденциальности и целостности данных являются обязательным элементом современных бизнес-приложений. Это требование достигается за счет стратегии Cisco Secure Connectivity System, которая, используя механизмы аутентификации и скрытия передаваемой информации, одинаково эффективно защищает данные (например, от системы управления предприятием или от Web-сервера), голос (например, от IP-телефонии) и видео (например, от камер видеонаблюдения или

в рамках видеоконференции), передаваемые как по проводным, так и по беспроводным соединениям. Составной частью Secure Connectivity System являются такие технологии, как IPSec, SSL, SSH, GRE и MPLS.

Идентификация и управление доверием (Identity & Trust Management System). Прежде чем пользователь, приложение или устройство получит доступ к необходимым ресурсам, он должен быть опознан средствами защиты. Именно эту задачу на сетевом уровне решают технологии и средства входящие в стратегию Identity & Trust Management System – Cisco Secure Access Control Server (ACS), Cisco Secure User Registration Tool, 802.1x, Network Admission Control (NAC). Стратегия Trust and Identity Solution распространяется на все элементы информационной сети транспортного предприятия – коммутаторы и маршрутизаторы, ПК и IP-телефоны, беспроводные точки доступа и клиенты и т.д.

СИТУАЦИОННЫЙ ЦЕНТР ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Специалисты по безопасности должны иметь инструменты для проведения всестороннего анализа данных, получаемых от средств обеспечения информационной безопасности, разбросанных по всей транспортной системы – от масштабов одного аэропорта или морского порта и заканчивая всей железнодорожной системой страны.

Ситуационные центры по информационной безопасности (Cisco MARS), выпускаемые компанией Cisco Systems, позволяют не только выполнить задачу визуализацию уровня защищенности и сигналов тревоги от различных средств защиты (межсетевые экраны, системы обнаружения атак, средства защиты персональных компьютеров и серверов), но и блокируют обнаруженные внутренние и внешние нападения. Достоинство указанных решений в том, что они могут управлять не только защитными средствами, выпущенными компанией Cisco Systems, но и продуктами других производителей (ISS, Check Point, Juniper и т.д.).

ДИАГНОСТИКА СОСТОЯНИЯ ЗАЩИЩЕННОСТИ

Для повышения уровня защиты как среды передачи данных, так и корпоративной сети транспортного предприятия необходимо использование средств диагностирования состояния защищенности и прогнозирования его изменения. Для решения этой задачи компания Cisco Systems предлагает как уже упомянутый выше ситуационный центр по информационной безопасности, так и специальное решение (Security Auditor), предназначенное для дистанционной проверки оборудования и средств защиты и выработки рекомендаций по повышению уровня защищенности.

ЗАЩИТА ИНТЕГРИРОВАННОЙ СЕТИ

Одной из сложностей обеспечения эффективного управления транспортом является разрозненность систем, отсутствие которой снижает не только эффективность управления транспортными потоками, но и оперативность реагирования на возникающие проблемы.

КОМПЬЮТЕРНЫЙ ЧЕРВЬ ОТМЕНИЛ ВЫЛЕТЫ САМОЛЕТОВ

В январе 2003 года компьютерный червь SQL Slammer нарушил работу систему управления полетами американской авиакомпании Continental Airlines, что привело к задержке и отмене некоторых рейсов.

Компания Cisco Systems помогает решить эту задачу путем объединения всех сервисов (включая IP-телефонию, видеокамеры наблюдения, данные от систем управления предприятием, сигналы тревоги от средств информационной безопасности и т.п.) в рамках единой и защищенной инфраструктуры. Такая интеграция позволяет не только снизить затраты на создание и обслуживание сети передачи данных, голоса и видео, но и создать эффективно масштабируемое и управляемое решение для воздушного и железнодорожного, морского и внутреннего водного, автомобильного и городского электрического (включая метрополитен), а также промышленного транспорта.

ЗАКЛЮЧЕНИЕ

«*В Транспортной стратегии Российской Федерации также предусмотрены меры, направленные на повышение безопасности движения на железнодорожном транспорте, безопасности полетов воздушных судов, безопасности морского судоходства и судоходства на внутренних водных путях. Они дополняется комплексом мер по выполнению важнейшей и злободневной задачи нового времени - обеспечению антитеррористической защищенности и устойчивости транспортной системы.*

Помимо повышения уровня безопасности, совершенствование технического уровня транспортных средств, применение современных перевозочных, управленческих и информационных технологий является одним из ключевых условий повышения эффективности и конкурентоспособности транспортной системы России»[1].

Компания Cisco Systems, признанный лидер в области сетевых решений и информационной безопасности, позволяет эффективно реализовать меры, предусмотренные Транспортной стратегией России. При этом решения, используемые для защиты перевозочных, управленческих и информационных технологий, уже не первый год занимают лидирующие позиции не только на мировом рынке, но также и в России и странах СНГ. Такое положение было бы невозможно без исследований и разработок, на которые ежегодно компания Cisco Systems тратит свыше 300 миллионов долларов.

Учитывая, что транспортные предприятия относятся к критичным национальным инфраструктурам и их информационные системы подлежат обязательной защите с помощью сертифицированных решений, компания Cisco Systems регулярно проводит соответствующие работы в Федеральной службе по техническому и экспортному контролю (бывшая Государственная техническая комиссия при Президенте России). На начало 2005 года, решения компании Cisco имели свыше 120 сертификатов по российским требованиям информационной безопасности, что существенно превышает число сертификатов, полученных какой-либо другой компанией (российской или зарубежной), работающей на рынке информационной безопасности.

ДОПОЛНИТЕЛЬНАЯ ИНФОРМАЦИЯ

Решения Cisco Systems по информационной безопасности

http://www.cisco.com/go/security

Решения Cisco Systems для предприятий транспортной отрасли

http://www.cisco.com/en/US/strategy/transportation/index.html

[1] Из доклада Министра транспорта И.Е. Левитина на заседании Правительства Российской Федерации 28 апреля 2005 года «Транспортная стратегия Российской Федерации».

Cisco Systems
Россия, 113054 Москва
бизнес центр “Риверсайд Тауэрз”
Космодамианская наб., 52
Стр. 1, 4-й этаж
Тел.: +7 (095) 961 14 10
Факс: +7 (095) 961 14 69
Internet: www.cisco.ru
www.cisco.com

Cisco Systems
Казахстан, 480099 Алматы
бизнес центр “Самал 2”
Ул. О. Жолдасбекова, 97
блок А2, этаж 14
Тел.: +7 (3272) 58 46 58
Факс: +7 (3272) 58 46 60
Internet: www.cisco.ru
www.cisco.com

Cisco Systems
Украина, 252004 Киев
бизнес центр “Горайзон Тауэрз”
Ул. Шовковична, 42-44, этаж 9
Тел.: (044) 490 36 00
Факс: (044) 490 56 66
Internet: www.cisco.ua
www.cisco.com

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on **Cisco Connection Online Web site at http://www.cisco.com/ http://www.cisco.ru/**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe