Автор: Артур Скальский © Babr24.com НАУКА И ТЕХНИКА , МИР 2502 18.07.2006, 17:40 282

Cisco Systems повышает безопасность мобильных операторов

Ежегодно тратя около 300 млн долларов на исследования и разработки в области информационной безопасности, компания Cisco Systems® помогает операторам мобильной связи защищать свои сети и абонентов от атак и угроз, число которых возрастает с каждым днем.

Всего лишь десять лет назад атаки типа "отказ в обслуживании" (DoS), сетевые черви и вирусы никак не затрагивали интересы мобильных операторов и пользователей, поскольку сети мобильной связи были изолированы от вычислительных сетей. Они подключались к жестко контролируемой инфраструктуре ТфОП и ОКС7 и предназначались для доставки только одной услуги - мобильной передачи голоса.

За последние годы, однако, мобильные сети претерпели множество важных изменений. На смену традиционным магистралям TDM и ATM пришли сети IP, которые отличаются более высокой скоростью, гибкостью и эффективностью. Сегодня передача голоса стала одной из сотен услуг, предоставляемых мобильным абонентам. Это значит, что ныне сети мобильной связи подключаются не только к сетям ТфОП и ОКС7. Широко распространились прямые подключения к Интернету, роуминг, корпоративные подключения, информационные услуги и хостинг приложений. В результате мобильные сети стали самыми доступными в мире. Мобильные же устройства, некогда поддерживавшие только голосовую связь, достигли поразительного уровня сложности. Сегодня они поддерживают мультимедийные сообщения, доступ в Интернет, сетевые игры, офисные приложения и виртуальные частные сети. Но все эти перемены не идут ни в какое сравнение с тем, что сулят абонентам мобильные сети третьего поколения (3G), которые принесут богатую функциональность и услуги Интернета всем мобильным пользователям в самых удаленных районах мира.

Сети и услуги 3G повысят качество жизни абонентов и откроют перед операторами новые рынки и источники дохода. В то же время они откроют дорогу новым угрозам и рискам. Так, например, доступ в Интернет, роуминг, связь с заказчиками и партнерами - все это крайне необходимо для доставки новых услуг, но этими же каналами могут воспользоваться злоумышленники для взлома корпоративных систем, проведения атак DDoS и распространения вредоносных программ. Все более мощные мобильные устройства 3G с широкой функциональностью тоже создают проблемы, поскольку могут выступать в качестве источников и объектов атак.

Многие устройства ЗП, по сути, представляют собой миниатюрные компьютеры. С появлением ПК-карт 3G миллионы ноутбуков также подключились к сетям 3G и стали использовать их для получения широкополосных услуг.

Защита мобильных устройств 3G от атак, а также защита мобильных сетей и абонентов от зараженных и атакующих устройств представляет собой сложную задачу, особенно в ситуации, когда оператор не имеет полного контроля над возможностями и конфигурацией устройств. Особую проблему создает появление одноранговых приложений (peer-to-peer applications), которые делают устройства 3G активным источником трафика, способного заполнить ограниченные сетевые ресурсы и воспретить доступ к сети для прибыльных абонентов.

Борьба с этими и прочими рисками имеет огромное значение для операторов, которым нужна постоянная доступность услуг, удовлетворенность абонентов, высокая надежность, безопасность и защита личных данных. Для этого, по словам Брайана Догерти (Brian Daugherty), специалиста по безопасности Cisco Systems, необходимы "управление, мониторинг и смягчение рисков". Для этого, в свою очередь, нужно:

• Разработки и внедрение правил управления сетевым доступом и использованием сетевых ресурсов при одновременном повышении уровня защиты сетевой и сервисной инфраструктуры от атак.

• Активный мониторинг сети и поведения абонентов, чтобы обеспечить соблюдение правил и своевременно выявлять события, которые могут повлиять на доставку мобильных услуг.

• Быстрое реагирование на атаки с помощью динамического набора устройств, инструментальных средств и стратегий.

Чтобы помочь операторам, компания Cisco Systems разработала широкий набор систем безопасности, которые можно использовать в мобильных сетевых инфраструктурах GSM, CDMA, Wi-Fi и двухрежимных инфраструктурах (Dual-Mode). Мобильные операторы могут использовать средства безопасности Cisco для защиты IP-инфраструктуры и сетевой периферии, для соблюдения установленных правил и защиты критически важных серверов и услуг от сетевых вирусов и червей.

Системы безопасности Cisco включают:

• Network Foundation Protection (средства защиты сетевой основы) - набор инструментальных средств и функций, таких как Control Plane Policing и Management Plane Protection, который включается в операционную систему Cisco IOS® для надежной защиты маршрутизаторов и коммутаторов в операторской IP-сети.

• Cisco DDoS mitigation (система борьбы с атаками DDoS). Эта система строит базовые профили трафика и анализирует его с помощью "детекторов аномалий" (Anomaly Detectors). Если форма трафика отклоняется от базового профиля, данные передаются "сторожам" (Anomaly Guards), которые выделяют атакующий код, ликвидируют его и направляют "вылеченный" трафик в пункт назначения.

• Cisco Secure Packet Gateways (безопасные шлюзы Cisco для передачи пакетов). Эти шлюзы защищают периферию сетей беспроводного доступа (RAN) с помощью аутентификации пользователей, предоставления им санкционированного доступа к услугам и данным, постоянного мониторинга поведения абонентов и управления межсетевой передачей трафика.

• Cisco Subscriber-Aware Firewalls (межсетевые экраны Cisco, учитывающие особенности абонентов). Эти системы защищают стыки сетей с Интернетом и другими сетями с помощью идентификации всего входящего трафика.

• Cisco Service Control Engines (средства Cisco для управления сервисами). Эти средства предоставляют операторам функции управления на единой платформе. Они поддерживают "глубокий анализ" пакетов и генерируют подробные отчеты с описанием поведения абонентов, услуг и приложений.

• Cisco Incident Control System (ICS) - система управления инцидентами, созданная Cisco вместе с компанией Trend Micro для защиты сетей от червей и вирусов. ICS позволяет оператору создавать списки контроля доступа (ACL) и передавать сигнатуры атак системам безопасности через считанные минуты после начала атаки.

В системе безопасности Cisco трудно найти элемент, выполняющий всего лишь одну задачу. К примеру, система борьбы с атаками DDoS (Cisco DDoS Mitigation System) не только борется с этими атаками, но и выполняет функции мониторинга. "Мы понимаем, что не все наши средства нужны каждому оператору. С другой стороны, для существенного повышения уровня безопасности сетей и услуг можно использовать не весь набор, а лишь какую-то его часть, - считает Брайан Догерти. - Поэтому каждый оператор должен подобрать для себя те средства, которые в наибольшей степени отвечают его индивидуальным особенностям, и внедрить их, используя поэтапный подход".

Автор: Артур Скальский © Babr24.com НАУКА И ТЕХНИКА , МИР 2502 18.07.2006, 17:40 282
URL: https://babr24.com/?ADE=31455 Bytes: 6872 / 6872 Версия для печати

НАПИСАТЬ ГЛАВРЕДУ:

Телеграм: @babr24_link_bot
Эл.почта: newsbabr@gmail.com

ЗАКАЗАТЬ РАССЛЕДОВАНИЕ:

эл.почта: bratska.net.net@gmail.com

КОНТАКТЫ

Бурятия и Монголия: Станислав Цырь
Телеграм: @bur24_link_bot
эл.почта: bur.babr@gmail.com

Иркутск: Анастасия Суворова
Телеграм: @irk24_link_bot
эл.почта: irkbabr24@gmail.com

Красноярск: Ирина Манская
Телеграм: @kras24_link_bot
эл.почта: krasyar.babr@gmail.com

Новосибирск: Алина Обская
Телеграм: @nsk24_link_bot
эл.почта: nsk.babr@gmail.com

Томск: Николай Ушайкин
Телеграм: @tomsk24_link_bot
эл.почта: tomsk.babr@gmail.com

Прислать свою новость

ЗАКАЗАТЬ РАЗМЕЩЕНИЕ:

Рекламная группа "Экватор"
Телеграм: @babrobot_bot
эл.почта: eqquatoria@gmail.com

СТРАТЕГИЧЕСКОЕ СОТРУДНИЧЕСТВО:

эл.почта: babrmarket@gmail.com

Подробнее о размещении

Отказ от ответственности

Правила перепечаток

Соглашение о франчайзинге

Что такое Бабр24

Вакансии

Статистика сайта

Архив

Календарь

Зеркала сайта